В. Брауэр

ВВЕДЕНИЕ В ТЕОРИЮ КОНЕЧНЫХ АВТОМАТОВ

ВВЕДЕНИЕ В ТЕОРИЮ КОНЕЧНЫХ АВТОМАТОВ

AUTOMATEN-THEORIE

Eine Einführung in die Theorie endlicher Automaten

Von Dr. rer. nat. Wilfried Brauer
Professor an der Universität Hamburg

B. G. Teubner Stuttgart 1984

В. Брауэр

ВВЕДЕНИЕ В ТЕОРИЮ КОНЕЧНЫХ АВТОМАТОВ

Перевод с немецкого К. В. Рудакова
под редакцией чл.-корр. АН СССР
Ю. И. Журавлева

Москва «Радио и связь»
1987

ББК 32.815
Б 87
УДК 007.52

Брауэр В.

Б87 Введение в теорию конечных автоматов: Пер. с нем. — М.: Радио и связь, 1987. — 392 с.: ил.

В книге профессора Гамбургского университета описаны основные классические модели теории конечных автоматов (автоматы Мили и Мура) и более сложные модели (автоматы Рабина — Скотта, многоленточные автоматы, конечные преобразователи). Рассмотрены преобразования конечных автоматов и регулярные множества. Существенную часть книги составляют упражнения.

Для инженерно-технических работников, связанных с приложениями теории конечных автоматов, а также работающих в области информатики и вычислительной техники.

Б $\frac{1502000000\text{-}123}{046(01)\text{-}87}$ 53-87 ББК 32.815

Редакция переводной литературы

Производственное издание

ВИЛЬФРИД БРАУЭР

ВВЕДЕНИЕ В ТЕОРИЮ КОНЕЧНЫХ АВТОМАТОВ

Заведующая редакцией О. В. Толкачева. Редактор С. Т. Симонова Переплет художника Н. А. Пашуро. Художественный редактор Т. В. Бусарова. Технические редакторы Г. И. Колосова, Т. Н. Зыкина. Корректор Л. А. Буданцева

ИБ № 1401

Сдано в набор 5.08 86 Подписано в печать 16 02.87
Формат 60 × 90¹/₁₆ Бумага тип. № 2 Гарнитура литературная
Печать высокая Усл. печ. л. 24,5 Усл. кр.-отт. 24,5
Уч.-изд л. 27,23 Тираж 10 000 экз. Изд. № 21635
Зак. № 5260 Цена 2 р. 10 к.
Издательство «Радио и связь», 101000 Москва, Почтамт, а/я 693

Ордена Октябрьской Революции и ордена Трудового Красного Знамени МПО «Первая Образцовая типография имени А. А. Жданова» Союзполиграфпрома при Государственном комитете СССР по делам издательств, полиграфии и книжной торговли. 113054, Москва, Валовая, 28.

ПРЕДИСЛОВИЕ

Конечные автоматы и такие тесно связанные с ними конструкции, как, например, линейные грамматики и регулярные выражения, относятся к важнейшим основным понятиям информатики. Различные варианты конечных автоматов и близкие им математические объекты служат для описания и анализа технических устройств, различных систем и процессов, программ и алгоритмов. Многие сложные концепции теоретической информатики — и притом относящиеся не только к более общим моделям автоматов, таким как автоматы с магазинной памятью и машины Тьюринга, — были выработаны на базе теории конечных автоматов. Теория автоматов порождает ряд легко формулируемых, но далеко не тривиальных проблем. Они приводят к весьма сложным алгоритмам и отчасти проясняют причины, по которым необходимо систематическое развитие математического программирования и теории алгоритмов, сопровождаемое подробным анализом корректности и сложности. Теория конечных автоматов имеет многочисленные приложения в технической и практической информатике и составляет существенную часть теоретической информатики. Это делает знание основ теории автоматов необходимым каждому специалисту по информатике.

Данная книга дает начальные представления о важнейших классических основных моделях, концепциях, методах и результатах теории конечных автоматов.

Поскольку теория автоматов является одним из старейших разделов теоретической информатики, широко развитым во многих направлениях, возможны целый ряд подходов и изложение разных аспектов этой теории различными методами и с различными целями. В данной книге избран «средний путь» между чисто математическим и направленным только на приложения подходами.

Мы будем рассматривать конечные автоматы как абстрактные модели простейших устройств, обрабатывающих данные, обращая в основном внимание на входно-выходное поведение, т. е. на определяемое автоматом отображение или соответствие между входным и выходным множествами слов. При этом особое значение будет придаваться конструктивным и алгоритмическим аспектам проблемы.

Способ изложения ориентирован прежде всего на теорию формальных языков, однако не предполагается, что у читателя имеются какие-либо специальные познания в этой области. Кроме

того, от читателя не требуются особые познания в математике или в других разделах информатики, выходящие за пределы материала, который изучается на первом курсе студентами, специализирующимися в области информатики [1].

Используемые в книге математические понятия, обозначения и методы кратко описаны в гл. 1. Некоторые простые и обычные понятия, кроме того, поясняются в том месте текста, где они употребляются впервые, так что после введения к гл. 1 можно переходить к чтению гл. 2 и только при необходимости использовать гл. 1 для справок.

Каждая из гл. 2—8 относительно независима: в гл. 2—5 и 8 рассматриваются основные модели автоматов, в гл. 6 изучается некоторая специальная конструкция и в гл. 7 представлен иной подход к проблеме. Все эти главы начинаются одним или несколькими вводными примерами и завершаются наборами упражнений и разделами, содержащими обзор литературы к данной главе. Список литературы дан в конце книги. Вводные и ряд других примеров в тексте взяты из различных разделов информатики. Они должны, с одной стороны, мотивировать введение абстрактных понятий и конструкций и, с другой стороны, демонстрировать возможности их применения.

Все теоремы, леммы и следствия (за исключением теорем о соответствиях Поста и о полноте системы аксиом для рациональных равенств) сопровождаются полными доказательствами. Эти доказательства по мере возможности конструктивны и неформальны (скажем, в доказательствах не используются методы формальной логики).

В книге принята простая система терминов, которую автор пытался составить так, чтобы разумно сочетать как ставшие уже историей, так и современные точки зрения. Данная терминология возникла в результате рассмотрения различных и, отметим, часто противоречивых систем понятий, встречающихся в литературе. В некоторых случаях в обзорах литературы после соответствующих глав содержатся комментарии по этому поводу. Эти обзоры включены в книгу прежде всего для указания авторов излагаемых идей и результатов и, кроме того, в них цитируются некоторые дополнительные работы и многие учебники. В тексте книги специальных ссылок на литературу нет.

Многочисленные задания предназначены для упражнений и более глубокого изучения материала, а также и для дополнения основного содержания книги (особенно трудные задания помечены звездочкой). Они являются важнейшей составной частью книги и должны быть внимательно прочтены и обдуманы читателем, даже если их и не удается выполнить полностью.

---

[1] Все же для понимания некоторых конструкций желательно знакомство читателя с проблематикой вычислимости, см., например, книги Роджерс Х. Теория рекурсивных функций и эффективная вычислимость: Пер. с англ. — М.: Мир, 1972. — 624 с. и Катленд Н. Вычислимость. Введение в теорию рекурсивных функций: Пер. с англ. — М.: Мир, 1983. — 256 с. — *Прим. перев.*

В соответствии с принятой в книге точкой зрения, в ней не представлены многие разделы теории автоматов. В частности, не рассматриваются вопросы, связанные с технической реализацией конечных автоматов (такие, как теория контактных схем и переключательных схем с памятью, теория разложения автоматов, теория линейных автоматов и т. д.). Также не изучается широкий круг сложных проблем, относящихся к теории формальных языков и теории сложности (например, не рассматриваются более общие модели автоматов такие, как машины Тьюринга, автоматы с магазинной памятью, пакетные автоматы, древовидные автоматы). Наконец, в книге не представлены сложные, преимущественно чисто математические теории (такие, как алгебраическая теория решеток, теории стохастических и топологических автоматов, теория рациональных степенных рядов, алгебраическая теория кодирования и т. д.).

Я выражаю глубокую благодарность проф. Г. Хольцу и д-ру П. Шпулеру за их предложение написать эту книгу и за проявленное ими при этом терпение. Доктор К. Й. Ланге основательно проработал многие варианты рукописи, сделав при этом ряд ценных предложений и внеся ряд поправок. Специалист по информатике К. Буттлер крайне тщательно прочитал окончательную редакцию текста и сделал при этом несколько предложений для дальнейшего его улучшения. Кроме того, он составил списки терминов и обозначений. Двум последним я особенно признателен. Я также благодарен всем, с кем работал, в том числе и ряду студентов, за стимулирующие обсуждения и критику. За выдержку и аккуратность, проявленные при подготовке рукописи, я крайне признателен моей секретарше А. Цильц. Но более всего я благодарен моей жене за ее сотрудничество и помощь. То, что она дала мне целый ряд советов в отношении дидактики, методики и стилистики, выполнила рисунки, отпечатала многие варианты рукописи и прочитала корректуру, является лишь малой частью ее вклада. Я смог работать над этой книгой, не ограничивая преподавательской и научной деятельности, только благодаря тому, что моя жена взяла на себя многие из моих разнообразных обязанностей и освободила меня от многих нагрузок. И при этом она с пониманием относилась к тому, что я и без того небольшое свободное время посвящал в основном этой рукописи. Без дружеской помощи эта книга не была бы написана.

В. Брауэр

ГЛАВА 1.

ОСНОВНЫЕ МАТЕМАТИЧЕСКИЕ ПОНЯТИЯ

ВВЕДЕНИЕ

Рассматриваемые в книге модели автоматов являются абстрактными описаниями технических устройств, социально-экономических, биологических и других динамических систем или описаниями программ, алгоритмов и вычислительных процессов. В основе таких моделей лежит предположение о том, что эти «автоматы» работают дискретным образом: находятся перед и после каждого шага в совершенно определенном состоянии и за каждый шаг воспринимают некий «вход» или порождают некий «выход». Предполагается также, что каждый автомат может иметь только одно из конечного множества состояний и что его входы и выходы могут быть описаны символами из некоторого конечного алфавита. То, что происходит с автоматом за отдельный шаг, будет описываться с помощью отображений или соответствий.

Таким образом, нам понадобятся сведения с множествах, отображениях, соответствиях (многозначных отображениях), отношениях и графах. Эти сведения не выходят за пределы материала, изучаемого на первом курсе и даже в средней школе. Они содержатся в разд. 1.1—1.3.

При изучении конечного автомата интересны не только его поведение за отдельный шаг, обработка конкретного входа и порождение конкретного выхода, но и поведение на протяжении длительных промежутков времени. Для формального описания такого поведения нам будут нужны сведения о конечных последовательностях отображений конечного множества в себя. Это означает, что нам понадобятся понятия полугруппы и моноида, приведенные в разд. 1.4 (определения этих понятий не будут повторяться в последующих главах).

Поскольку у читателя не предполагается наличие особых математических знаний и навыков, в разд. 1.5 дается обзор основных необходимых для дальнейшего изложения методов доказательств.

Утверждения, приведенные в разд. 1.1—1.5 без доказательств, могут быть проверены читателем на базе вводимых определений посредством простых выкладок. Во многих же случаях даются наброски доказательств или указания.

Формальная логика в книге непосредственно использоваться не будет, логические связки и кванторы будут записываться сло-

вами. В то же время предполагается, что читатель имеет представление об алгоритмах и проблематике вычислимости и разрешимости. Поэтому такие понятия, как эффективная конструкция, эффективная вычислимость и т. п., будут использоваться без дальнейших пояснений. Скажем только, что мы считаем некоторую проблему разрешимой (неразрешимой), если существует (не существует) решающий ее алгоритм. Пример неразрешимой проблемы в первый раз появится в гл. 8, а неэффективная конструкция будет описана в гл. 5 (теорема 5.5.7).

Для понимания некоторых примеров и соответствующих методов желательно, чтобы читатель имел определенные познания в области практического программирования и в теории языков программирования. Следует также иметь в виду, что для некоторых сложных алгоритмов необходимы доказательства корректности и оценки времени работы и объема памяти.

1.1. МНОЖЕСТВА

Далее понадобятся только представления наивной теории множеств в смысле Г. Кантора: «Под множеством мы понимаем собрание определенных отличных друг от друга объектов (реальных или воображаемых), называемых элементами множества, в их общности». Поскольку мы начинаем с конечных множеств и формируем бесконечные множества на базе конечных с использованием вполне определенных операций, нам не приходится опасаться появления возможных в наивной теории множеств антиномий. При желании можно считать, что все рассматриваемые множества являются подмножествами некоторого универсума, за пределы которого не выводят все используемые операции.

ТЕОРЕТИКО-МНОЖЕСТВЕННЫЕ ОБОЗНАЧЕНИЯ

Будем обозначать *множества* прописными латинскими буквами типа M, M', M_1, *множества множеств* — прописными рукописными буквами типа $\mathcal{M}$, $\mathcal{R}$, а *элементы* множеств — строчными латинскими буквами типа m, m' m_1.

$m \in M$ означает высказывание «m *является элементом множества* M»; в этом случае мы также говорим «m принадлежит множеству M »или« из M» и т. п.

$m \notin M$ означает отрицание высказывания $m \in M$, т. е. высказывание «m не принадлежит M».

$M_1 \subseteq M_2$ означает высказывание «каждый элемент множества M_1 является также элементом множества M_2», в этом случае мы также пишем «M_1 *является подмножеством множества* M_2» или «имеет место включение $M_1 \subseteq M_2$».

$M_1 = M_2$ означает высказывание «$M_1 \subseteq M_2$ и $M_2 \subseteq M_1$», в этом случае мы также говорим «*множества* M_1 и M_2 *равны*».

$M_1 \neq M_2$ является отрицанием высказывания $M_1 = M_2$.

$M_1 \subset M_2$ эквивалентно высказыванию «$M_1 \subset M_2$ и $M_1 \neq M_2$», в этом случае мы также говорим «M_1 *является собственным подмножеством множества* M_2».

$|M|$ для конечного множества M есть *число элементов этого множества.*

$\varnothing$ означает единственное множество, не содержащее элементов. Отсюда вытекает, что для любого множества M выполняется включение $\varnothing \subseteq M$ и, если для некоторого множества M верно, что $M \subseteq \varnothing$, то $M = \varnothing$.

СПЕЦИАЛЬНЫЕ МНОЖЕСТВА

Мы считаем, что определены следующие множества: множество *натуральных чисел* 1, 2, 3, ..., обозначаемое $\mathbf{N}$; множество *неотрицательных целых чисел* 0, 1, 2, ..., обозначаемое $\mathbf{N}_0$; множество целых чисел ..., —2, —1, 0, 1, 2, ..., обозначаемое $\mathbf{Z}$. Считаем также, что на этих множествах определены арифметические операции и отношения $\leqslant$ (меньше или равно) и $<$ (строго меньше). Кроме того, полагаем известными понятия простого числа, четного числа, нечетного числа и т. д.

ПОСТРОЕНИЕ НОВЫХ МНОЖЕСТВ

Множества могут быть построены следующими способами.

1. *Перечислением всех элементов.*

Примеры. $X = \{a, b\}$; $Y = \{1\}$; $Z = \{1, 2, \ldots, 8\}$; $M_n = \{m_1, m^2, \ldots, m_n\}$, где $n \in \mathbf{N}$ (поэтому при $n = 0$ имеем $M_0 = \varnothing$).

Из определения равенства множеств вытекает, например, что $\{x, y\} = \{y, x\}$.

2. Заданием *характеристического свойства,* выделяющего элементы данного множества среди элементов указанного или указанных других множеств.

Примеры. $\mathbf{N} = \{n \mid n \in \mathbf{Z},\ n > 0\}$; $\{m \mid m \neq m\} = \varnothing$;

$\{m \mid$ существует $n \in \mathbf{N}$ такое, что $m = n^2\}$ — множество всех квадратов натуральных чисел.

3. *Описанием порождающей процедуры* с указанием множества (или множеств), которое пробегает параметр (или параметры) этой процедуры.

Примеры.

Множество всех квадратов натуральных чисел может быть также задано как $\{n^2 \mid n \in \mathbf{N}\}$;

$\{\{m, n\} \mid m \in \mathbf{N}$ и $n \in \mathbf{N}\}$ — множество всех двухэлементных подмножеств множества натуральных чисел;

$\{8x_1 + 14x_2 + 32x_3 \mid x_1,\ x_2,\ x_3 \in \mathbf{Z}\}$ — множество четных чисел.

БУЛЕВЫ ОПЕРАЦИИ

С помощью задания характеристических свойств можно определить специальные операции над множествами, позволяющие строить новые множества, — так называемые *булевы операции.* Пусть M и M' — множества.

Объединением множеств M и M' называется множество

$$M \cup M' = \{m \mid m \in M \text{ или } m \in M'\}.$$

Пересечением множеств M и M' называется множество

$$M \cap M' = \{m \mid m \in M \text{ и } m \in M'\}.$$

M и M' называются *дизъюнктными*, если $M \cap M' = \varnothing$.

Разностью множеств M и M' называется множество

$$M - M' = \{m \mid m \in M \text{ и } m \notin M'\}.$$

Симметрической разностью множеств M и M' называется множество

$$M \oplus M' = (M - M') \cup (M' - M).$$

Если $M' \subseteq M$, то разность $M - M'$ называется *дополнением* множества M' в множестве M.

Пример. $M \oplus M' = (M \cup M') - (M \cap M')$.

Такого рода равенства доказываются просто: нужно лишь показать, что каждый элемент множества, стоящего в одной части равенства, является также и элементом множества, стоящего в другой его части.

Доказательство. Первая часть утверждения, т. е. высказывание $M \oplus M' \subseteq (M \cup M') - (M \cap M')$ верно, поскольку очевидно, что $M \oplus M' \subseteq M \cup M'$ и каждый элемент, входящий и в M, и в M', не входит ни в $M - M'$, ни в $M' - M$. В то же время каждый элемент, принадлежащий множеству, стоящему в правой части доказываемого равенства, входит в M или в M', но не входит в $M \cap M'$, т. е. принадлежит M, но не M' или, наоборот, M', но не M, т. е. входит в $M \oplus M'$.

Если M и M' — конечные множества, то выполняются следующие равенства:

$$|M \cup M'| = |M| + |M'| - |M \cap M'|,$$
$$|M - M'| = |M| - |M \cap M'|,$$
$$|M \oplus M'| = |M - M'| + |M' - M| = |M| + |M'| - 2|M \cap M'|.$$

БУЛЕАН, БУЛЕВЫ АЛГЕБРЫ ПОДМНОЖЕСТВ ДАННОГО МНОЖЕСТВА

Для каждого множества M определен булеан $\mathscr{P}(M)$ — множество всех подмножеств множества M, т. е. $\mathscr{P}(M) = \{M' \mid M' \subseteq M\}$.

В частности $\mathscr{P}(M)$ содержит в качестве элементов $\varnothing$ и M, так что любое множество может рассматриваться как элемент некоторого (другого) множества.

Если множество M конечно, причем $|M| = n$, то выполняется равенство $|\mathscr{P}(M)| = 2^n$ (см. разд. 1.5).

Для каждого множества M булеан $\mathscr{P}(M)$ *замкнут относительно булевых операций*, т. е. для всяких двух элементов M_1 и M_2 булеана $\mathscr{P}(M)$ множества $M_1 \cup M_2$, $M_1 \cap M_2$ и $M_1 - M_2$ (а потому и $M_1 \oplus M_2$) являются элементами $\mathscr{P}(M)$.

Для булевых операций на $\mathscr{P}(M)$ справедливы, в частности, следующие законы, которые легко проверить указанным выше способом:

$$M \cup \varnothing = M,\ M - \varnothing = M,\ M \cap \varnothing = \varnothing,\ \varnothing - M = \varnothing,\ M \cup (M - M') = M;$$

$M \cup M = M$, $M \cap M = M$ (закон идемпотентности);

$M \cup N = N \cup M$, $M \cap N = N \cap M$ (закон коммутативности);

$$\left.\begin{aligned} M \cup (N \cap P) &= (M \cup N) \cap (M \cup P) \\ M \cap (N \cup P) &= (M \cap N) \cup (M \cap P) \end{aligned}\right\}$$ (закон дистрибутивности);

$(M \cup N) \cup P = M \cup (N \cup P)$, $(M \cap N) \cap P = M \cap (N \cap P)$ (закон ассоциативности);

$M \cap (M \cup N) = M$, $M \cup (M \cap N) = M$ (закон поглощения);

$$\left.\begin{aligned} M - (N \cup P) &= (M - N) \cap (M - P) \\ M - (N \cap P) &= (M - N) \cup (M - P) \end{aligned}\right\}$$ (законы Моргана)

Булеан $\mathscr{P}(M)$ вместе с булевыми операциями на нем образуют так называемую *булеву алгебру*. Каждое подмножество $\mathscr{T}$ булеана $\mathscr{P}(M)$, замкнутое относительно булевых операций, содержит как множество (например, $\varnothing$), являющееся подмножеством каждого множества из $\mathscr{T}$, так и множество (например, M), содержащее в качестве подмножества каждое множество из $\mathscr{T}$. Таким образом, $\mathscr{T}$ также оказывается булевой алгеброй.

ОБЪЕДИНЕНИЯ И ПЕРЕСЕЧЕНИЯ ПРОИЗВОЛЬНЫХ СЕМЕЙСТВ МНОЖЕСТВ

Благодаря свойству ассоциативности объединения и пересечения произвольных семейств множеств могут быть описаны без использования скобок.

Пусть $n \in \mathbf{N}$ и пусть $M_1, M_2, \ldots, M_n$ — множества. Положим

$M_1 \cup M_2 \cup \ldots \cup M_n = \cup\{M_i \mid 1 \leqslant i \leqslant n\} = \{m \mid$ существует i, где $1 \leqslant i \leqslant n$, такое, что $m \in M_i\}$.

$M_1 \cap M_2 \cap \ldots \cap M_n = \cap\{M_i \mid 1 \leqslant i \leqslant n\} = \{m \mid$ для каждого i, где $1 \leqslant i \leqslant n$, выполнено $m \in M_i\}$.

Эти определения могут быть обобщены на случай, когда множества M_i заданы как элементы некоторого семейства множеств $\mathscr{M}$ и требуется выполнение некоторого дополнительного условия B:

$\cup\{M \mid M \in \mathscr{M}$ и M удовлетворяет условию B$\} = \{m \mid$ существует $M \in \mathscr{M}$ такое, что для M выполнено условие B и $m \in M\}$.

Определение для пересечений аналогично вышеприведенному.

Пример. $\cup\{M \mid M \in \mathscr{P}(\mathbf{Z})$ и $M \cap \mathbf{N}_0 = \varnothing\}$ — множество всех отрицательных целых чисел.

Вместо $\cup\{M_i \mid i \in \mathbf{N}\}$ используется также запись $\bigcup_{i=1}^{\infty} M_i$ и аналогичная запись для пересечений.

ПАРЫ, n-КИ, ПОСЛЕДОВАТЕЛЬНОСТИ, ДЕКАРТОВЫ ПРОИЗВЕДЕНИЯ

Дальнейшие возможности построения новых множеств из заданных основаны на понятии (упорядоченных) пар и, более обще, (упорядоченных) n-ок.

Пусть $x_1, x_2, \ldots, x_n$ (при некотором $n \in \mathbf{N}$) — n не обязательно различных объектов (т. е. элементов некоторого множества или множеств). Тогда определен объект $(x_1, x_2, \ldots, x_n)$, называемый n-кой; x_i называется i-й компонентой этой n-ки.

Если x_i (при $1 \leqslant i \leqslant n$) попарно различны, то объект $(x_{i_1}, x_{i_2}, \ldots, x_{i_n})$, где $1 \leqslant i_j \leqslant n$, $i_j \neq i_k$ для $j \neq k$ и $1 \leqslant i, k \leqslant n$, отличен от объекта $(x_1, x_2, \ldots, x_n)$, если только существует q (где $1 \leqslant q \leqslant n$) такое, что $i_q \neq q$. Итак, n-ки упорядочены.

При $n=2$ n-ка называется *парой*, при $n=3$ — *тройкой*, при $n=4$ — *четверкой*, при $n=5$ — *пятеркой*, при $n=6$ — *шестеркой* и т. д.

Из сказанного, в частности, следует, что при $x \neq y$ пары (x, y) и (y, x) различны.

Можно рассматривать n-ки и как (конечные) *последовательности*. При этом n называется *длиной последовательности*.

Пусть $M_1, M_2, \ldots, M_n$ (при $n \geqslant 2$) — не обязательно различные множества. *Декартовым произведением* множеств M_i является множество $M_1 \times M_2 \times \ldots \times M_n = \{(m_1, m_2, \ldots, m_n) \mid m_i \in M_i$ при $i = 1, \ldots, n\}$.

Если одно из множеств M_i (при некотором i, где $1 \leqslant i \leqslant n$) пусто, то пусто и декартово произведение $M_1 \times M_2 \times \ldots \times M_n$.

Если $M_1 = M_2 = \ldots = M_n = M$, то $M^n = M_1 \times \ldots \times M_n$ называется n-й *декартовой степенью множества* M. При $n=0$ и $n=1$ по определению полагаем $M^0 = \{\varnothing\}$ и $M^1 = M$.

Пример. $\mathbf{Z}^2$ — множество всех пар целых чисел, т. е. всех координат целочисленных точек на евклидовой плоскости.

Существуют следующие правила:

$(M_1 \cup M_2) \times M_3 = M_1 \times M_3 \cup M_2 \times M_3$;

$(M_1 \cap M_2) \times M_3 = M_1 \times M_3 \cap M_2 \times M_3$;

$(M_1 - M_2) \times M_3 = M_1 \times M_3 - M_2 \times M_3$;

$T_1 \times M_2 \cap M_1 \times T_2 = T_1 \times T_2$, если $T_i \subseteq M_i$ при $i=1, 2$.

Важным подмножеством декартова произведения $M \times M$ является множество $\Delta_M = \{(m, m) \mid m \in M\}$, называемое *диагональю*.

ВЕКТОРЫ, МАТРИЦЫ

Часто n-ку называют (n-мерным или n-компонентным) *вектором* (или *вектор-строкой*). Если же компоненты n-ки записываются одна под другой по вертикали, то это образование называют *вектор-столбцом*.

n-ка m-мерных вектор-столбцов (при $m, n \in \mathbf{N}$) называется *m×n-матрицей*. Итак, *m×n*-матрица является прямоугольной схемой (или таблицей) содержащей m строк и n столбцов:

$$A = \| a_{ik} \| = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}.$$

a_{ik} называется *элементом* матрицы, n-ка i=x компонент вектор-столбцов ($1 \leqslant i \leqslant m$) в той же последовательности называется *строкой* матрицы. Мы будем рассматривать матрицы и как вектор-столбцы их строк.

В случае, когда m=n, n-ка (a_{11}, a_{22}, ..., a_{nn}) называется *главной диагональю* матрицы A.

УПРОЩЕННЫЕ ОБОЗНАЧЕНИЯ

В случаях, когда не могут возникнуть разночтения, будем опускать скобки, т. е. писать m вместо {m} и, в частности, $M \cup a$ вместо $M \cup \{a\}$, $M - a$ вместо $M - \{a\}$, $M \times a$ вместо $M \times \{a\}$ и т. д.

Далее, мы часто будем писать сокращенно: {m∈M | m удовлетворяет условию B} вместо {m | m∈$\mathcal{M}$ и m удовлетворяет условию B}.

При записи декартовых произведений и n-ок будем в большинстве случаев опускать внутренние скобки, т. е., замечая, что декартово произведение (соответственно операция образования n-ок) ассоциативно, записывать, например, $(M_1 \times M_2) \times M_3$ и $M_1 \times (M_2 \times M_3)$ как $M_1 \times M_2 \times M_3$.

1.2 СООТВЕТСТВИЯ И ОТОБРАЖЕНИЯ

СООТВЕТСТВИЯ

Пусть X и Y — множества.

Соответствием k *из* X *в* Y (или на Y) называется тройка k=(X, Y, K), где $K \subseteq X \times Y$. При этом K называется графиком соответствия k, что записывается следующим образом: gr k=K.

Множество D(k)={x∈X | существует y∈Y такое, что (x, y)∈gr k} называется *областью определения* соответствия k. Часто вместо D(k) пишут более коротко D_k.

Для каждого x из X положим: k(x)={y∈Y | (x, y)∈gr k}. Таким образом, имеем $D_k = \{x \in X \mid k(x) \neq \varnothing\}$.

Кроме того, для каждого подмножества X′ множества X положим $k(X') = \cup\{k(x) \mid x \in X'\}$.

Пример. Пусть P — множество всех простых чисел. Сопоставим каждому n∈**N** все его простые делители (простые числа, на которые делится n). Таким образом мы получаем соответствие t=(**N**, P, gr t), определяемое равенством t(n)={p∈P | p делит n}.

Если $X = X_1 \times \ldots \times X_n$, то, опуская скобки, мы вместо $k((x_1, \ldots, x_n))$ пишем $k(x_1, \ldots, x_n)$, и если $X_i' \subseteq X_i$ при i=1, ..., n, то полагаем $k(X_1', X_2', \ldots, X_n') = k(X_1' \times \ldots \times X_n')$.

ПОСТРОЕНИЕ НОВЫХ СООТВЕТСТВИЙ ИЗ ЗАДАННЫХ

Обратным соответствием для k является соответствие $k^{-1} = (Y, X, K^{-1})$, где $K^{-1} = \{(y, x) \in Y \times X \mid (x, y) \in K\}$. Отметим, что, вообще говоря, $k^{-1}(k(x)) \neq \{x\}$ и $k(k^{-1}(y)) \neq \{y\}$.

Пример. X={a, b}=Y, k=(X, Y, {(a, b), (b, b)}), $k^{-1}(k(a)) = k^{-1}(b) = \{a, b\}$, $k(k^{-1}(a)) = \varnothing$.

Если $T \subseteq X$, то соответствие $k' = k/\Gamma = (T, Y, \operatorname{gr} k \cap T \times Y)$ называется *ограничением* или *сужением* k на T, а k называется *расширением* или *продолжением* k'.

Пусть для $i = 1, 2$ заданы соответствия k_i из X_i в Y_i.

Включение $k_1 \subseteq k_2$ *по определению* выполняется тогда и только тогда, когда $X_1 \subseteq X_2$, $Y_1 \subseteq Y_2$ и $\operatorname{gr} k_1 \subseteq \operatorname{gr} k_2$.

Объединением соответствий k_1 и k_2 называется соответствие $k_1 \cup k_2 = (X_1 \cup X_2, Y_1 \cup Y_2, \operatorname{gr} k_1 \cup \operatorname{gr} k_2)$.

Равенство $k_1 = k_2$ по определению выполняется тогда и только тогда, когда $X_1 = X_2$, $Y_1 = Y_2$ и $\operatorname{gr} k_1 = \operatorname{gr} k_2$, т. е. когда выполняются оба включения $k_1 \subseteq k_2$ и $k_2 \subseteq k_1$.

Декартовым произведением соответствий k_1 и k_2 называется соответствие

$$k_1 \times k_2 = (X_1 \times X_2, Y_1 \times Y_2, \{((x_1, x_2)\ (y_1, y_2)) \mid (x_i, y_i) \in K_i$$

для $i = 1, 2\}$).

Если $X_2 = Y_1$, то *композицией соответствий* k_1 и k_2 *называется* соответствие $k_2 k_1 = (X_1, Y_2, K_1 \cdot K_2)$, где

$K_1 \cdot K_2 = \{(x, y) \in X_1 \times Y_2 |$ существует z такое, что $(x, z) \in K_1$ и $(z, y) \in K_2\}$.

Для каждого x_1 из X_1 справедливо равенство $k_2 k_1 (x_1) = k_2 (k_1 (x_1))$.

ОТОБРАЖЕНИЯ

Пусть $f = (X, Y, \operatorname{gr} f)$ — соответствие.

Соответствие f называется *отображением* из X в Y, если для каждого x из X выполнено равенство $|f(x)| = 1$, т. е. если каждое x из X встречается в ровно одной паре (x, y) в графике соответствия f. При этом также пишут $f : X \to Y$.

Легко видеть, что соответствие f является отображением тогда и только тогда, когда выполнены включения $\Delta_X \subseteq \operatorname{gr}(f^{-1} f)$ и $\operatorname{gr}(f f^{-1}) \subseteq \Delta_Y$.

f называется частичным отображением из X в Y, если $|f(x)| \leqslant 1$ для каждого $x \in X$, т. е. если имеет место включение $\operatorname{gr}(f f^{-1}) \subseteq \Delta_Y$. В этом случае мы также пишем $f : (X) \to Y$.

Частичное отображение является также и отображением, если $D_f = X$, т. е. если оно всюду определено или, что то же, если $\Delta_X \subseteq \operatorname{gr}(f^{-1} f)$.

Иногда отображения называют также *тотальными* или *всюду определенными,* чтобы отличать их от частичных отображений.

$f(x)$ называется *образом* элемента x множества X при отображении f. Соответственно $f(X')$ называется *образом* подмножества X' при отображении f. Вместо $f(x) = \{y\}$ часто используется запись $f(x) = y$.

$f^{-1}(y)$ [соответственно $f^{-1}(Y')$] называется *прообразом* элемента y множества Y [соответственно подмножества Y' множества Y] при отображении f.

Отображение f называется *сюръективным* (или *отображением на,* или *сюръекцией),* если $f(X)=Y$. f называется *инъективным* (или *однозначным,* или *обратимым,* или *инъекцией),* если f^{-1} является частичным отображением. f^{-1} в этом случае называется обратным к f (частичным) отображением. Отображение f называется *биективным* (или *биекцией*), если оно одновременно является и сюръективным, и инъективным.

Легко видеть, что f тогда и только тогда является инъективным (соответственно сюръективным, биективным), когда $f^{-1}(y)$ для каждого $y\in Y$ содержит не более (соответственно не менее, ровно) одного элемента.

Если отображение f сюръективно (инъективно), то выполняется равенство $f(f^{-1}(y))=y$ [соответственно равенство $f^{-1}(f(x))=x$].

Все введенные для соответствий понятия естественным образом переносятся и на случай (частичных) отображений. В частности, два (возможно, частичных) отображения $f_1=(X_1, Y_1, \operatorname{gr} f_1)$ и $f_2=(X_2, Y_2, \operatorname{gr} f_2)$ равны тогда и только тогда, когда они равны как соответствия. Поэтому данные отображения не равны даже в том случае, когда $\operatorname{gr} f_1=\operatorname{gr} f_2$, но $X_1\neq X_2$ или $Y_1\neq Y_2$.

Декартово произведение двух отображений является, очевидно, также отображением.

Композиция двух (частичных, инъективных, сюръективных, биективных) отображений также является (частичным, инъективным, сюръективным, биективным соответственно) отображением.

Вместо термина «отображение» часто используется термин *«функция».*

Отображение f конечного множества $\{m_1, \ldots, m_n\}$ в себя часто подставляют $2\times n$-матрицей

$$\begin{pmatrix} m_1 & m_2 & \ldots & m_n \\ f(m_1) & f(m_2) & \ldots & f(m_n) \end{pmatrix}.$$

Композиция отображений такого вида легко может быть определена по этим матрицам.

Если множество M конечно, то инъекция (или сюръекция) M в себя является также биекцией (см. разд. 1.5) и называется *подстановкой* множества M.

Пусть k — соответствие. На основе определения множества $k(X')$ для $X'\subseteq X$ соответствию k может быть сопоставлено отображение из $\mathcal{P}(X)$ в $\mathcal{P}(Y)$. Аналогичным образом отображение из $\mathcal{P}(Y)$ в $\mathcal{P}(X)$ может быть сопоставлено соответствию k^{-1}.

Пусть $f=(X, Y, \operatorname{gr} f)$ — отображение, и пусть $X', X''\subseteq X$ и $Y', Y''\subseteq Y$. Тогда выполняются следующие соотношения:

$$f(X'\cup X'')=f(X')\cup f(X'');$$

$f(X' \cap X'') \subseteq f(X') \cap f(X'')$ (равенство имеем при инъективном отображении f);

$f^{-1}(Y' \cup Y'') = f^{-1}(Y') \cup f^{-1}(Y'')$;

$f^{-1}(Y' \cap Y'') = f^{-1}(Y') \cap f^{-1}(Y'')$.

Кроме того, эквивалентны следующие три высказывания:
1) $f: X \to Y$ инъективно (сюръективно);
2) $f: \mathcal{P}(X) \to \mathcal{P}(Y)$ инъективно (сюръективно);
3) $f^{-1}: \mathcal{P}(Y) \to \mathcal{P}(X)$ сюръективно (инъективно).

СПЕЦИАЛЬНЫЕ ОТОБРАЖЕНИЯ

Если M′ является подмножеством множества M, то *характеристической функцией* M′ в M называется отображение $C^M_{M'}$:

$$C^M_{M'}: M \to \{0, 1\}, \quad C^M_{M'}(m) = \begin{cases} 1, \text{ если } m \in M', \\ 0 \text{ в противном случае.} \end{cases}$$

Пусть $M = M_1 \times \ldots \times M_n$ — декартово произведение. Тогда для каждого i из множества $\{1, \ldots, n\}$ определены отображения pr_i и $\underline{pr}_i$ (называемые *проекциями*):

$pr_i: M \to M_i$, $pr_i(m_1, \ldots, m_n) = m_i$;

$\underline{pr}_i: M \to M_1 \times \ldots \times M_{i-1} \times M_{i+1} \times \ldots \times M_n$,

$\underline{pr}_i(m_1, \ldots, m_n) = (m_1, \ldots, m_{i-1}, m_{i+1}, \ldots, m_n)$.

Пусть, далее, $1 \leqslant k \leqslant n$ и $1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n$. Тогда *проекция* $pr_{i_1, i_2, \ldots, i_k}: M \to M_{i_1} \times \ldots \times M_{i_k}$ определяется равенством $pr_{i_1, i_2, \ldots, i_k}(m_1, \ldots, m_n) = (m_{i_1}, m_{i_2}, \ldots, m_{i_k})$.

ДИАГРАММЫ

Для облегчения работы с отображениями применяются диаграммы. Пусть, например, даны функции $f_i = (X_i, X_{i+2}, gr f_i)$ при $i = 1, 2$ и $f_j' = (X_j, X_{j+1}, gr f_j')$ при $j = 1, 3$. Эта ситуация описывается диаграммой (прямоугольной) на рис. 1.2.1.

Эта диаграмма называется *коммутативной* тогда и только тогда, когда $f_3' f_1(x) = f_2 f_1'(x)$ для всех x из X_1.

Аналогичным образом определяется коммутативность треугольных диаграмм и т. д.

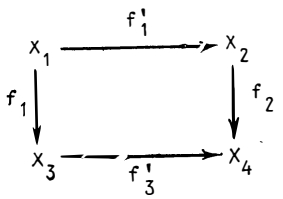


Рис 1 2.1

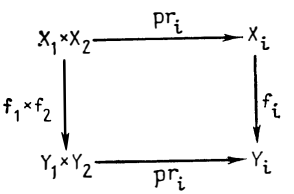


Рис. 1.2.2

Пример. Пусть определены отображения $f_i=(X_i, Y_i, \operatorname{gr} f_i)$ при $i=1, 2$. Тогда при $i=1$ и при $i=2$ коммутативна диаграмма, приведенная на рис. 1.2.2.

1.3. ОТНОШЕНИЯ И ГРАФЫ

ОТНОШЕНИЯ

Пусть M — множество. *Отношением на* M называется подмножество R множества $M\times M$ [1].

Если $(x, y)\in R$, то говорят, что x и y *находятся в отношении* R.

Пример. Пусть $M=\mathbf{N}$ и $R_{\leqslant}$ отношение $\leqslant$. Тогда $R_{\leqslant}=\{(i, j)\in \in \mathbf{N}^2 \mid i\leqslant j\}$.

Для отношений часто используется способ записи, при котором знак отношения ставится между элементами множества, т. е. вместо $(x, y)\in R$ пишется xRy.

Множество всех отношений на множестве M в точности равно $\mathscr{P}(M^2)$. Оно образует булеву алгебру относительно булевых операций с выделенными элементами $\varnothing$ (*нулевое отношение*) и M^2 (*тождественно истинное отношение*).

Отношения могут рассматриваться и как графики соответствий, что позволяет прямо перенести на них ряд понятий, в частности ввести понятия *обратного отношения* R^{-1} для данного R и *композиции отношений* $R\cdot R'$ для R и R'.

ОРИЕНТИРОВАННЫЕ ГРАФЫ, ПРЕДСТАВЛЕНИЕ ОРИЕНТИРОВАННЫХ ГРАФОВ ДИАГРАММАМИ И МАТРИЦАМИ

Отношение R на M может быть представлено так называемым ориентированным графом: *ориентированный граф* (или *орграф*) есть пара $G=(E, K)$, где E — множество *вершин* графа G, и $K\subseteq \subseteq E\times E$ — множество ориентированных *ребер* графа G. Ориентированный граф G может быть представлен диаграммой, причем вершины изображаются кружками, а ориентированные ребра — стрелками.

Диаграммы, представляющие орграфы, часто также называют графами.

Пример. Соответствующий отношению $\leqslant$ на $\mathbf{N}$ граф — это граф $(\mathbf{N}, R_{\leqslant})$. Часть этого графа показана на рис. 1.3.1.

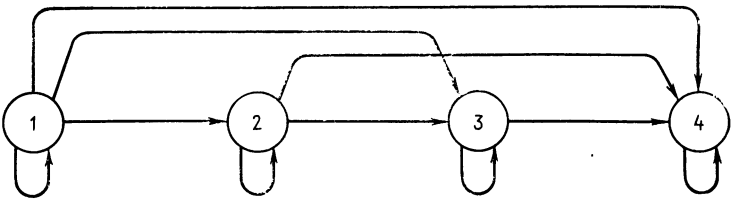


Рис. 1.3.1

[1] Автор понимает под отношениями только бинарные отношения, не оговаривая это дополнительно. — *Прим. перев.*

Так же как и для отношений, ориентированными графами и диаграммами могут быть представлены и графики соответствий (или отображений). Конечный ориентированный граф G (а потому и отношение на конечном множестве или соответствие между двумя конечными множествами) может быть задан матрицей следующим образом.

Пусть $G=(E, K)$, где $E=\{e_1, ..., e_n\}$. *Матрицей смежности* для графа G называется $n\times n$-матрица $M=(m_{ik})$, где

$$m_{ik}=\begin{cases}1, & \text{если } (e_i, e_k)\in K,\\ 0 & \text{в противном случае.}\end{cases}$$

В ориентированном графе $G=(E, K)$ (*направленным*) *путем длины* $k+1$ из e *в* e′ называется последовательность (e, e_1), $(e_1, e_2), ..., (e_k, e')$ ориентированных ребер из K.

ВЗВЕШЕННЫЕ ОРИЕНТИРОВАННЫЕ ГРАФЫ

Если на некотором множестве M определены несколько отношений (или соответствий) и эта ситуация должна быть представлена в графической форме, то относящиеся к различным отношениям ориентированные ребра должны быть по-разному помечены. Это приводит нас к следующему понятию.

Ориентированный граф со взвешенными ребрами (или просто *взвешенный орграф*) есть тройка $G=(E, X, K)$, где E — множество вершин, X — множество *весов ребер* и $K\subseteq E\times X\times E$ — множество *взвешенных ориентированных ребер* графа G.

Если $(e, x, e')\in K$, то говорят, что ребро (e. e′) имеет *вес* (*метку*) x. В этом случае на диаграмме ребро из e в e′ помечается символом x. В отличие от ранее определенных графов, в данном случае две вершины могут быть соединены несколькими ребрами, помеченными, разумеется, различным образом.

Пример. $M=\{3, 4, 6\}$. Для $t=1, 2, 3$ и $v=6, 12$ положим:

$R_t=\{(i, j)\in M^2 |$ наибольший общий делитель i и j равен t и $i<j\}$,

$R_v=\{(i, j)\in M^2 |$ наименьшее общее кратное i и j равно v и $i<j\}$.

Тогда взвешенным ориентированным графом, соответствующим пяти отношениям $R_1, R_2, R_3, R_6, R_{12}$, является граф $G(M\{1, 2, 3, 6, 12\}, \{(i, t, j) | (i, j)\in R_t\}\cup\{(i, v, j) | (i, j)\in R_v\})$ (рис. 1.3.2).

Аналогично вводится и еще одно обобщение понятия ориентированного графа: *ориентированный граф со взвешенными вершинами* есть упорядоченная четверка $G=(E, K, Y, b)$, где (E, K) — ориентированный граф, Y — множество *весов вершин*, b: $E\to Y$ — *отображение, сопоставляющее вершинам их веса.*

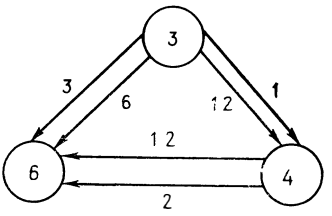


Рис. 1.3.2

СВОЙСТВА ОТНОШЕНИЙ

Отношение R на множестве M называется:

рефлексивным, если $\Delta_M \subseteq R$, т. е. если для всех x из M выполняется включение $(x, x) \in R$;

симметричным, если $R = R^{-1}$, т. е. если из $(x, y) \in R$ вытекает, что $(y, x) \in R$;

транзитивным, если $R \cdot R \subseteq R$, т. е. если из $(x, y) \in R$ и $(y, z) \in R$ вытекает, что $(x, z) \in R$;

отношением эквивалентности (эквивалентностью), если оно является одновременно рефлексивным, симметричным и транзитивным;

антисимметричным, если $R \cap R^{-1} \subseteq \Delta_M$, т. е. если из $(x, y) \in R$ и $(y, x) \in R$ вытекает, что $x = y$;

отношением частичного порядка (частичным порядком), если оно является рефлексным, антисимметричным и транзитивным;

отношением линейного порядка или просто отношением *порядка* (или *линейным порядком*), если оно является отношением частичного порядка и выполнено равенство $R \cup R^{1-} = M^2$, т. е. если для любых x и y из множества M выполняется либо $(x, y) \in R$, либо $(y, x) \in R$.

В ориентированных графах (диаграммах), представляющих транзитивные отношения, любые две вершины e и e′, соединенные некоторым путем, соединены также и ребром, т. е. для таких вершин $(e, e') \in R$.

ЗАМЫКАНИЯ ОТНОШЕНИЙ

Транзитивным (соответственно *рефлексивным и транзитивным*) *замыканием* R^+ (соответственно R^*) отношения R называется пересечение всех транзитивных (соответственно транзитивных и рефлексивных) отношений, содержащих R в качестве подмножества.

Выполнены равенства $R^* = \Delta_M \cup R^+$ и

$R^+ = \{(x, y) \in M^2 |$ в графе R существует путь из x в y$\}$.

Отметим, что R^+ является транзитивным отношением, а R^* — рефлексивным и транзитивным.

Если множество M конечно, то рефлексивное и транзитивное замыкание отношения R может быть получено с помощью так называемого *метода Варшалла* следующим образом.

Пусть $|M| = n$.

1. Полагаем $R_0 = \Delta_M$.

2. Для $i = 0, \ldots, n-1$ определяем

$R_{i+1} = R_i \cdot R = \{(x, y) |$ существует $z \in M$ такое, что $(x, z) \in R_i$ и $(z, y) \in R\}$.

3. Полагаем $R^* = R_0 \cup R_1 \cup \ldots \cup R_n$.

Доказательство корректности этого метода будет дано в разд. 1.5.

Пусть P — множество, $n \in \mathbf{N}$ и $k = (P^n, P, K)$ — соответствие.

Подмножество A множества P называется *замкнутым относительно соответствия* k, если $k(A, A, ..., A) \subseteq A$. Если, кроме того, P может быть задано эффективно и k эффективно вычислимо, то A называется *эффективно замкнутым* относительно k.

Пример. Пусть $P = \mathscr{P}(M)$ и k_b — соответствие из P^2 в P, которое каждым двум подмножествам U и V множества M сопоставляет три множества $U \cup V$, $U \cap V$ и $U - V$. Семейство A_e, содержащее $\varnothing$ и все конечные подмножества множества M, замкнуто относительно k_b.

Для каждого подмножества B множества P существует единственное наименьшее объемлющее B подмножество A множества P, замкнутое относительно соответствия k. Это подмножество называется *k-замыканием* B (или замыканием B относительно k). Отметим, что справедливо равенство

$$A = \bigcap \{A' \mid B \subseteq A' \text{ и } A' \text{ замкнуто относительно k}\},$$

так как если $B \subseteq A'' \subseteq P$ и A'' замкнуто относительно k, то $A \subseteq A''$.

Пример. Пусть $P = M^2$ и $k = (P^2, P, \{((x, y), (y, z), (x, z)) \mid x, y, z \in M\})$. Для любого отношения R на M в этом случае R^+ является замыканием R относительно k.

Однозначность k-замыканий используется при так называемых *индуктивных определениях*: чтобы задать некоторое множество M, элементы которого удовлетворяют данным условиям, полностью описывают некоторое подмножество T этого множества и определяют все множество M как замыкание T относительно некоторых операций.

Пример. Пусть $F_{1,2} = \{(1\ 1), (1, 2)\}$ и k_f — отображение из $\mathbf{N}^2 \times \mathbf{N}^2$ в $\mathbf{N}^2$, сопоставляющее парам (m, m') и $(m+1, m'')$ пару $(m+2, m'+m'')$. Если F есть k_f-замыкание $F_{1,2}$ и $f = (\mathbf{N}, \mathbf{N}, F)$, то $f(n)$ есть n-е число Фибоначчи.

УПОРЯДОЧЕННЫЕ МНОЖЕСТВА, РЕШЕТКИ

Упорядоченным множеством называется пара $(M, \leqslant)$, где $\leqslant$ — отношение частичного порядка на M (если x и y — элементы множества M, то вместо $(x, y) \in \leqslant$ используется запись $x \leqslant y$).

Пусть $T \subseteq M$, $t, t' \in T$, $m \in M$.

t называется *минимальным элементом* в T, если для любого $x \in T$ из $x \leqslant t$ вытекает, что $x = t$.

m называется *нижней гранью* для T, если для любого $x \in T$ выполнено $m \leqslant x$.

t' называется *наименьшим элементом* в T, если для всех x из T выполнено $t' \leqslant x$.

Аналогично определяются понятия максимального и наибольшего элементов в T и понятие верхней грани для T.

Каждое подмножество множества M [например, множество всех верхних (или нижних) граней некоторого подмножества T

множества M] имеет не более одного наименьшего (соответственно наибольшего) элемента, но может иметь много минимальных (или максимальных) элементов.

Упорядоченное множество называется *решеткой*, если каждое его конечное подмножество обладает наименьшей верхней и наибольшей нижней гранями.

Примеры. 1. $(\mathscr{P}(M), \subseteq)$ — решетка: $U \cup V$ является наименьшей верхней, а $U \cap V$ — наибольшей нижней гранью для $\{U, V\} \subseteq \subseteq \mathscr{P}(M)$.

2. **N** с отношением делимости | (где $i|j$, если i является делителем j) — решетка. Наибольшей нижней гранью для {i, j} оказывается наибольший общий делитель i и j, наименьшей верхней гранью для {i, j} — наименьшее общее кратное i и j.

ОТНОШЕНИЯ И КЛАССЫ ЭКВИВАЛЕНТНОСТИ

Пусть R — отношение эквивалентности на M.

Для $m \in M$ множество $[m] = \{m' \in M | (m, m') \in R\}$ называется *классом эквивалентности* m по модулю (относительно) R.

Любые два класса эквивалентности либо не пересекаются, либо совпадают. Действительно, если $x \in [m] \cap [m']$, то $(m, x) \in R$ и $(x, m') \in R$, а отсюда вследствие транзитивности отношения R вытекает, что $(m, m') \in R$.

Верно и обратное: каждое разбиение M на непустые дизъюнктные подмножества, объединение которых совпадает с M, определяет отношение эквивалентности R на M. Классы эквивалентности по этому отношению в точности совпадают с подмножествами, образующими исходное разбиение. Чтобы показать это, достаточно просто определить R следующим образом: $(m, m') \in R$ тогда и только тогда, когда m и m′ принадлежат одному подмножеству из заданного разбиения.

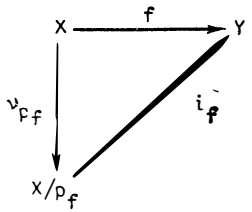


Рис. 1.3.3

Множество всех классов эквивалентности в M относительно R называется *фактор-множеством* M по R и обозначается M/R.

Отображение $\nu_R : M \to M/R$, определяемое соотношением $\nu_R(m) = [m]$ для каждого m из M, называется *естественным* или *каноническим* отображением. Каноническое отображение сюръективно.

Важную связь между отображениями и отношениями эквивалентности устанавливает следующая *теорема о разложении отображений*: отображение $f : X \to Y$ *индуцирует* на множестве X отношение эквивалентности $\rho_f = \{(x, x') | f(x) = f(x')\}$. Для ρ_f существует единственное инъективное отображение $i_f : X/\rho_f \to Y$ такое, что диаграмма на рис. 1.3.3 оказывается коммутативной, т. е. такое, что $i_f \nu_{\rho_f} = f$.

Если f сюръективно, то i_f — биекция.

Пример. Определим на $\mathbf{Z}\times\mathbf{N}$ отношение $\sim$ следующим образом: $(z, n)\sim(z', n')$ тогда и только тогда, когда $zn'=z'n$. Отношение $\sim$ является отношением эквивалентности. Пусть, далее, q — отображение из $\mathbf{Z}\times\mathbf{N}$ на множество $\mathbf{Q}$ рациональных чисел, определяемое равенством $q(z, n)=z/n$. Тогда $\rho_q=\sim$ и i_q является биекцией $\mathbf{Z}\times\mathbf{N}/\sim$ на $\mathbf{Q}$.

1.4. МОНОИДЫ И ГОМОМОРФИЗМЫ

ПОЛУГРУППЫ И МОНОИДЫ

Пусть M — множество и $\circ$ — отображение из $M\times M$ в M (для него используется способ записи, при котором знак отображения ставится между аргументами) такое, что для всех m_1, m_2, m_3 из M выполняется равенство $(m_1\circ m_2)\circ m_3=m_1\circ(m_2\circ m_3)$ (закон ассоциативности). Тогда пара $(M, \circ)$ называется *полугруппой*, а $\circ$ — *полугрупповой операцией* (или *умножением*) на M. Если ясно, о какой именно операции идет речь, то говорят просто о полугруппе M. При работе с полугруппами чаще всего используется «мультипликативная терминология», т. е. полугрупповая операция называется умножением и т. д.

Если в M содержится элемент e такой, что $e\circ m=m\circ e=m$ для всех m из M, то $(M, \circ)$ называется *моноидом*, а e — *нейтральным* (или *единичным*) *элементом* этого моноида. Моноид обладает единственным единичным элементом. Действительно, если $e'\in M$ и для всех m из M выполнено $e'\circ m=m\circ e'=m$, то, в частности, $e'=e'\circ e=e$.

Единичный элемент моноида M обозначается e_M.

Если множество M конечно, например $M=\{m_1, \ldots, m_n\}$, то моноид M может быть определен $n\times n$-матрицей $V=\|v_{ik}\|$, где $v_{ik}=m_i\circ m_k$, называемой *таблицей умножения*.

Примеры. 1. Множество всех соответствий (или всех отображений) некоторого множества в себя образует моноид относительно операции композиции отображений. Единичным элементом этого моноида является тождественное отображение.

2. $(\mathbf{N}, +)$ — полугруппа, $(\mathbf{N}_0, +)$ — моноид.

Для подмножеств U и V полугруппы M произведением U и V называется множество $U\circ V=\{u\circ v \mid u\in U, v\in V\}$. Введение такой операции умножения превращает $\mathscr{P}(M, \circ)$ в полугруппу (а если M — моноид, то и в моноид с единичным элементом $\{e_M\}$).

Далее будем считать, что $U^{i+1}=U^i\circ U^1$ при $i\in\mathbf{N}$ и $U^1=U$, а если M — моноид, то $U^0=\{e_M\}$.

ПОДПОЛУГРУППЫ И ПОДМОНОИДЫ

Подмножество U полугруппы M называется *подполугруппой* полугруппы M, если $U\circ U\subseteq U$. Если M — моноид, то подполугруппа моноида U такая, что $e_M\in U$, называется *подмоноидом* моноида M.

У моноидов могут быть подполугруппы, которые хотя и будут моноидами сами по себе, но не будут подмоноидами. В качестве

примера рассмотрим некоторое множество M, моноид A отображений M в себя, подмножество T множества M такое, что $|M-T| \geqslant 2$, фиксированный элемент m_0 из M—T и подполугруппу

$$A_T = \{f \in A \mid f(T) \subseteq T,\ f(m) = m_0 \text{ для } m \in M-T\}.$$

Тогда отображение f, определенное равенствами $f(t)=t$ для всех $t \in T$ и $f(m)=m_0$ для $m \in M-T$, хотя и будет единичным элементом для A_T, но не будет совпадать с Δ_M.

Для $X \subseteq M$ множество

$$X^+ = \bigcup_{i=1}^{\infty} X^i = \{x_1 \circ x_2 \circ \ldots \circ x_n \mid n \in \mathbf{N},\ x_i \in X \text{ для } i = 1, \ldots, n\}$$

является подполугруппой M. Если M — моноид, то $X^* = X^0 \cup X^+$ — подмоноид моноида M.

X^+ (соответственно X^*) называется *подполугруппой* (*подмоноидом*), *порожденной* (*порожденным*) *множеством* X. Она (он) является пересечением всех подполугрупп (подмоноидов) моноида M, содержащих X в качестве подмножества (т. е. X^+ оказывается замыканием множества X относительно операции произведения).

Если $M=X^+$ (или $M=X^*$ в случае, если M — моноид), то X называется *порождающей системой для* M. Например, если $M=(\mathbf{N}, +)$, то множество $\{1\}$ является порождающей системой. Полугруппа (или моноид) M называется *конечно-порожденной*, если она имеет конечную порождающую систему.

ГРУППЫ И ПОЛУКОЛЬЦА

Моноид $(M, \circ)$ называется группой, если для каждого принадлежащего множеству M элемента m в M существует элемент m^{-1} такой, что $m \circ m^{-1} = m^{-1} \circ m = e_M$. При этом элемент m^{-1} называется *обратным* для элемента m. Каждый элемент m из M имеет не более одного обратного элемента, как как из равенства $m' \circ m = e_M$ вытекает, что $m' = m' \circ e_M = m' \circ (m \circ m^{-1}) = (m' \circ m) \circ m^{-1} = e_M \circ m^{-1} = m^{-1}$.

Пример. Множество всех биекций некоторого множества на себя является группой.

Подмоноид группы называется *подгруппой*, если он вместе с каждым своим элементом содержит и его обратный элемент.

Пусть H — множество, на котором определены две операции (два отображения из $H \times H$ в H) причем $+$ (сложение) и $\circ$ (умножение) заданы таким образом, что

$(H, +)$ и $(H, \circ)$ — моноиды;

умножение дистрибутивно по отношению к сложению, т. е. выполнены равенства $h \circ (h_1 + h_2) = h \circ h_1 + h \circ h_2$ и $(h_1 + h_2) \circ h = h_1 \circ h + h_2 \circ h$ (для любых h, h_1 и h_2 из H);

для нейтрального элемента (*нулевого элемента*) 0 моноида $(H, +)$ и для любого h из H выполнены равенства $h \circ 0 = 0 \circ h = 0$;

$(H, +)$ коммутативен, т. е. $h_1 + h_2 = h_2 + h_1$ для всех h_1 и h_2 из H. Тогда $(H, +, \circ)$ называется полукольцом.

Примеры. 1. $(N_0, +, \circ)$ — полукольцо.

2. $(\mathfrak{P}(M), \cup, \cap)$ — полукольцо, в котором $\varnothing$ является нулевым элементом.

3. $(\mathfrak{P}(M), \cup, \cap)$ — полукольцо, в котором нулевым элементом является M.

4. Если $(M, \circ)$ — моноид, то $(P(M), \cap, \varnothing)$ — полукольцо, в котором $\varnothing$ — нулевой элемент.

МАТРИЦЫ И ВЕКТОРЫ НАД ПОЛУКОЛЬЦАМИ

Пусть $(H, +, \circ)$ — полукольцо и $n \in N$. Тогда множество $n \times n$-матриц с компонентами из H образует полукольцо, если определить сложение «+» и умножение «$\circ$» матриц $A = \|a_{ik}\|$ и $A' = \|a'_{ik}\|$ следующим образом:

$A + A' = \|a_{ik} + a'_{ik}\|$ (т. е. сложение покомпонентное) и

$$A \cdot A' = \| b_{ik} \|, \quad b_{ik} = a_{i1} \circ a'_{1k} + a_{i2} \circ a'_{2k} + \ldots + a_{in} \circ a'_{nk}.$$

Нулевым элементом полукольца матриц является так называемая *нулевая матрица*, все элементы которой равны нулевому элементу 0 из H. Единичным элементом этого полукольца называется *единичная матрица* $E = \|e_{ik}\|$, где e_{ii} при $i = 1, \ldots, n$ — единичный элемент моноида $(H, \circ)$ и $e_{ij} = 0$ при $i \neq j$, $1 \leqslant i, j \leqslant n$.

Множество n-компонентных векторов над некоторым моноидом $(H, +)$ (при использовании аддитивных обозначений) образует моноид с *нулевым вектором* $(0, 0, \ldots, 0)$ в качестве нулевого элемента, если определить сложение покомпонентно (как в случае матриц).

Пусть z — вектор-строка с компонентами $z_1, \ldots, z_n$ и s — вектор-столбец с компонентами $s_1, \ldots, s_n$, а $A = \|a_{ik}\|$ — $n \times n$-матрица. Тогда по определению $b = z \cdot A$ — вектор-строка с компонентами $b_j = z_1 \circ a_{1j} + z_2 \circ a_{2j} + \ldots + z_n \circ a_{nj}$ и $c = A \cdot s$ — вектор-столбец с компонентами $c_j = a_{j1} \circ s_1 + a_{j2} \circ s_2 + \ldots + a_{jn} \circ s_n$. Кроме того, считается, что $z \cdot s = z_1 \circ s_1 + z_2 \circ s_2 + \ldots + z_n \circ s_n$. Отсюда, например, получаем $z \cdot (A \cdot s) = z \cdot c = b \cdot s = (z \cdot A) \cdot s \in H$.

ГОМОМОРФИЗМЫ

Пусть $(H_1, \circ_1)$ и $(H_2, \circ_2)$ — полугруппы. Отображение $h: H_1 \to H_2$ называется *полугрупповым гомоморфизмом* из H_1 в H_2, если для любых x и y из H_1 выполняется равенство $h(x \circ_1 y) = h(x) \circ_2 h(y)$, т. е. если отображение h сохраняет произведение (образ произведения равен произведению образов).

Если, кроме того, H_1 и H_2 являются моноидами с единичными элементами e_1 и e_2 соответственно и $h(e_1)=e_2$, то h называется *моноидным гомоморфизмом*, $h(H_1)$ — *гомоморфным образом* H_1.

Пример. Отображение h из **N** в **N**, определенное равенством $h(n)=2^n$, является полугрупповым гомоморфизмом из $(\mathbf{N}, +)$ в $(\mathbf{N}, \circ)$ и моноидным гомоморфизмом из $(\mathbf{N}_0, +)$ в $(\mathbf{N}, \circ)$.

Гомоморфный образ подполугруппы (подмоноида) является подполугруппой (соответственно — подмоноидом, если речь идет о моноидном гомоморфизме).

Если $(H_1, \circ_1)$ — группа, $(H_2, \circ_2)$ — моноид и h — сюръективный моноидный гомоморфизм из H_1 на H_2, то $(H_2, \circ_2)$ является группой [где $h(x)^{-1}=h(x^{-1})$] и h называется *групповым гомоморфизмом.*

В случаях, когда не может возникнуть недоразумений, говорят просто о гомоморфизмах.

Гомоморфизм h называется *эпиморфизмом*, если отображение h сюръективно, и *изоморфизмом*, если h биективно.

Суперпозиция гомоморфизмов является гомоморфизмом, а отображение, обратное для биективного гомоморфизма (изоморфизма), — изоморфизмом.

ОТНОШЕНИЯ КОНГРУЭНТНОСТИ

Отношение эквивалентности ρ на полугруппе $(H, \circ)$ называется *отношением конгруэнтности* (*конгруэнцией*), если оно стабильно относительно операции $\circ$, т. е. если для любых m_i и m'_i из M при $i=1,2$ выполнено условие: из $m_1 \rho m'_1$ и $m_2 \rho m'_2$ вытекает, что $(m_1 \circ m_2)\, \rho\, (m_1' \circ m_2')$.

Классы эквивалентности относительно ρ называются при этом *классами конгруэнции.*

Фактормножество H/ρ может быть обращено в полугруппу (а если H — моноид, то и в моноид) таким образом, что каноническое отображение ν_ρ будет эпиморфизмом. Для этого достаточно определить операцию $\circ$ на H/ρ равенством $[x] \circ [y] = [x \circ y]$ для любых x и y из H. Нетрудно показать независимость этого определения от выбора представителей x и y в классах эквивалентности, т. е. показать, что для любых $x' \in [x]$ и $y' \in [y]$ выполнено $[x \circ y] = [x' \circ y']$. Если H — моноид, то $[e_H]$ — единичный элемент в H/ρ).

Из теоремы о разложении отображений (см. конец разд. 1.3) вытекает метод, позволяющий множество M, которое является образом полугруппы (моноида) $(H, \circ)$ при отображении f, обратить в полугруппу (в моноид) [1]. Для этого достаточно определить операцию $\cdot$ на M равенством $m \cdot m' = i_f(i_f^{-1}(m) \circ i_f^{-1}(m'))$.

Теореме о разложении отображений соответствует *теорема о гомоморфизмах:* если $h : H \to H'$ — эпиморфизм, то i_h — изоморфизм из H/ρ_h на H'.

---

[1] Данный метод корректен только в случае, когда ρ_f оказывается конгруэнцией на $(H, \circ)$. — *Прим. перев.*

Пусть ρ — некоторое отношение на полугруппе $(H, \circ)$. *Порожденным отношением* ρ *отношением конгруэнтности* называется рефлексивное и транзитивное замыкание следующего симметричного отношения $\rho: m\rho m'$ тогда и только тогда, когда существуют x, y, y' и z такие, что $m = x \circ y \circ z$ и $m' = x \circ y' \circ z$, причем $y\rho y'$ или $y'\rho y$.

Если множество X является порождающей системой для полугруппы (моноида) $(H, \circ)$, то каждый гомоморфизм h из H в H' однозначно определяется уже совокупностью образов $h(x)$ элементов x из X. Действительно, каждый элемент m из H может быть записан как произведение $m = x_1 \circ x_2 \circ \ldots \circ x_n$, где $x_i \in X$ при $i = 1, \ldots, n$, и любое отображение $f: X \to H'$ [1] может быть однозначно продолжено до гомоморфизма из H в H' так, что $f(m) = f(x_1) \circ f(x_2) \circ \ldots \circ f(x_{in})$ для произвольного m из H, разложенного в произведение элементов из X.

СВОБОДНЫЕ ПОЛУГРУППЫ И МОНОИДЫ

Пусть X — порождающая система для полугруппы $(H, \circ)$. X называется *свободным порождающим множеством* для H и H — *свободной* (точнее — свободно порожденной множеством X) *полугруппой*, если из равенства $x_1 \circ x_2 \circ \ldots \circ x_k = y_1 \circ y_2 \circ \ldots \circ y_n$, где x_i, $y_i \in X$ при $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant n$, вытекает, что $k = n$ и $x_i = y_i$ при $1 \leqslant i \leqslant n$. Если X и X' — свободные порождающие множества для H, то $X = X'$, так как каждый элемент x из X может быть представлен в виде $x = x'_1 \circ \ldots \circ x'_n$ с множителями из X, а каждый множитель x'_i при $1 \leqslant i \leqslant n$ может быть, в свою очередь, представлен как произведение элементов из X, откуда вытекает, что $n = 1$ и, следовательно, $x \in X'$.

Итак, каждый элемент свободной полугруппы имеет в точности одно представление в виде произведения элементов свободного порождающего множества.

Если $(M, \circ)$ — моноид, такой что $(M - e_M, \circ)$ — свободно порожденная множеством X полугруппа, то $(M, \circ)$ называется *свободно порожденным множеством* X *моноидом*.

Пример. $(\mathbf{N}, +)$ — свободно порожденный множеством $\{1\}$ моноид.

СВОБОДНЫЙ МОНОИД СЛОВ НАД МНОЖЕСТВОМ

Для любого множества X описанным ниже способом может быть построен свободно порожденный множеством X моноид $F(X)$.

Пусть $n \in \mathbf{N}_0$. Отображение $w: \{1, \ldots, n\} \to X$ называется словом *длины* n над X. При этом $w(i)$ записывается как w_i, w — как $w_1 w_2 \ldots w_n$ и для длины слова w используется обозначение $|w|$

---

[1] Автор, очевидно, имеет в виду отображение f такое, что для всех x и y из X выполнено $f(x \circ y) = f(x) \circ f(y)$. — *Прим. перев.*

(т. е. считается, что $|w|=n$). При $n=0$ выполняется равенство $\{1, \ldots, n\}=\varnothing$, так что слово длины 0, есть отображение $w=(\varnothing, X, W)$, где $W\subseteq\varnothing\times X=\varnothing$, и потому $W=\varnothing$. Итак, существует единственное слово длины 0, обозначаемое Λ и называемое *пустым словом*.

Пусть $W^+(X)$ — множество всех слов конечной ненулевой длины над множеством X, т. е. $W^+(X)=\{x_1x_2 \ldots x_n \mid n\in N, x_i\in X$ при $i=1, \ldots, n\}$, и $W(X)$ — множество всех слов конечной длины над X, т. е. $W(X)=\{\Lambda\}\cup W^+(X)$.

На множестве $W(X)$ вводится операция $\cdot$. Для u и v из $W(X)$ отображение $u\cdot v: \{1, \ldots, |u|+|v|\}\to X$ определяется равенствами $u\cdot v(i)=u(i)$ при $i=1, \ldots, |u|$ и $u\cdot v(j)=v(|u|+j)$ при $j=1, \ldots, |v|$. Тогда $(W(X), \cdot)$ — моноид и $(W^+(X), \cdot)$ — свободно порожденная множеством X полугруппа. Поскольку каждая свободно порожденная множеством X полугруппа изоморфна $(W^+(X), \cdot)$, то $(W^+(X), \cdot)$ называется *порожденной* X *свободной полугруппой* и обозначается $F^+(X)$. При этом опускается знак операции, состоящей просто в приписывании слов друг к другу (конкатенации). Соответственно, $(W(X), \cdot)$ называется *порожденным* X *свободным моноидом* и обозначается $F(X)$.

Пусть H — полугруппа и $X\subseteq H$. Тогда H является свободно порожденной X полугруппой в том и только в том случае, когда каждое отображение f из X в некоторую полугруппу H' может быть единственным образом продолжено до гомоморфизма H в H'. Для доказательства заметим, что H изоморфна $F(X)$.

Отметим, в частности, что каждый моноид, свободно порожденный множеством X, является образом $F(X)$ при каноническом изоморфизме, который совпадает на X с тождественным отображением.

Слово над X часто называют также *последовательностью символов* из X. Множество X, рассматриваемое как порождающая система для $F(X)$, называется *алфавитом*.

При представлении слова w над X в виде $w=x_1x_2 \ldots x_n$ предполагается, что все x_i определены однозначно. Если, например, Y — подмножество свободного моноида $F(X)$, то моноид $F(Y)$ не изоморфен, вообще говоря, подмоноиду Y^* моноида $F(X)$ (скажем, при $Y=\{a, aa\}$). Действительно, в $F(Y)$ элементы множества Y рассматриваются как неразложимые объекты, так что представление некоторого слова w как последовательности элементов множества Y может отличаться от представления w как последовательности элементов из X. Как это может быть осуществлено на практике, известно всем, знакомым с языками программирования высокого уровня (вспомните об использовании служебных слов).

ГОМОМОРФИЗМЫ, ПРАВИЛА СОКРАЩЕНИЯ

Если $h: F(X)\to F(X')$ — моноидный гомоморфизм, такой что $h(X)\subseteq X'\cup\Lambda$, то h называется *алфавитным*; если при этом $\Lambda\notin h(X)$, то h называется Λ-*свободным*.

Если гомоморфизм h алфавитный, то $h(F(X))$ — свободный моноид и $h^{-1}: \mathcal{P}(F(X')) \to \mathcal{P}(F(X))$ — полугрупповой гомоморфизм, т. е. $h^{-1}(UV)=h^{-1}(U)h^{-1}(V)$ и $h^{-1}(U^+)=(h^{-1}(U))^+$ для всех $U, V \subseteq F(X')$. Если же, кроме того, гомоморфизм h является Λ-свободным или если $\Lambda \in U$, то выполняется равенство $h^{-1}(U^*)=(h^{-1}(U))^*$.

Примеры. 1. Отображение $h: X \to F(X)$, определенное для каждого $x \in X$ равенством $h(x)=xx$, является неалфавитным гомоморфизмом, отображающим $F(X)$ изоморфно на свободный подмоноид моноида $F(X)$.

2. Определенное равенством $h(w)=|w|$ отображение из $F(X)$ в $(\mathbf{N}_0, +)$ есть Λ-свободный алфавитный моноидный гомоморфизм.

Для $F(X)$ существуют следующие правила сокращения [для $u, v, w \in F(X)$]: из $uv=uw$ следует, что $v=w$, и из $uv=wv$ — что $u=w$.

Верно следующее более общее утверждение (теорема Леви): если u, v, u′ и v′ — элементы из $F(X)$ такие, что $uv=u'v'$, то:

при $|u|>|u'|$ существует единственное слово w в $F^+(X)$ такое, что $u=u'w$ и $v'=wv$;

при $|u|=|u'|$ выполнены равенства $u=u'$ и $v=v'$;

при $|u|<|u'|$ существует единственное слово w′ в $F^+(X)$ такое, что $u'=uw$ и $v=w'v'$.

Доказательство вытекает из рис. 1.4.1.

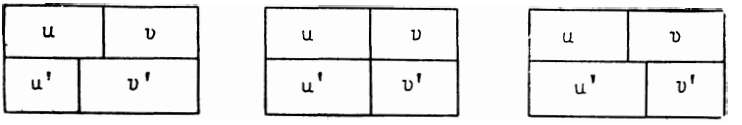


Рис. 1.4.1

Отметим, в частности, что из равенства $uv=\Lambda$ следует, что $u=v=\Lambda$.

1.5 МЕТОДЫ ДОКАЗАТЕЛЬСТВ

Представленные ниже три важных (и простых) метода доказательств, хотя и не будут описаны полностью, будут объяснены на примерах.

КОСВЕННОЕ ДОКАЗАТЕЛЬСТВО

Основная идея. Если должно быть доказано высказывание вида «из предположения V вытекает утверждение B», то вместо него для некоторого выводимого из V утверждения V_a (может быть, что $V_a=V$) доказывается высказывание «из отрицания B вытекает отрицание V_a».

Чтобы обосновать этот метод, заметим, что если верно V, то верно и V_a, так что по закону исключенного третьего (tertium non datur) отрицание V_a не может быть верным. Для высказывания B

по тому же закону исключенного третьего также имеет место либо утверждение «B верно», либо «B ложно». Если доказано, что из отрицания B вытекает отрицание V_a, то предположение о том, что высказывание B ложно, приводит к противоречию с предположением о истинности V_a, а потому и V. В силу этого, если справедливо утверждение о истинности V, то должно быть верно и B. Доказательства такого рода называют также доказательствами от противного (reductio ad absurdum[1]).

Чтобы описанным способом доказать утверждение вида «B истинно», нужно найти верное высказывание V, отрицание которого может быть выведено из отрицания B.

Примеры. 1. Классическим примером является доказательство Евклида для высказывания B= «существует бесконечно много простых чисел». В качестве истинного утверждения, достаточного для истинности B, при этом используется высказывание V= «если $n \in \mathbf{N}$ и $n \neq 1$, то либо n само простое число, либо существует простое число, на которое n делится». Допустим, что верно отрицание высказывания B, т. е. предположим, что существует лишь конечное число простых чисел, скажем, $p_1, \ldots, p_k$. Число $m = p_1, p_2, \ldots, p_k + 1$ не делится ни на одно из чисел p_i (при $i = 1, \ldots, k$). Поскольку по предположению никаких простых чисел, отличных от $p_1, \ldots, p_k$, не существует и $m \neq 1$, то отсюда вытекает, что V не может быть верным. Итак, наше предположение ложно и B истинно.

2. **Утверждение:** пусть M — конечное множество; отображение f из M в себя сюръективно тогда и только тогда, когда оно инъективно.

Доказательство. а) Пусть f инъективно. Тогда $|f(M)| = |M|$. Если бы f не было сюръективным, то существовал бы элемент m в M такой, что $f(M) \subseteq M - m$, а отсюда следует, что $|f(M)| \leqslant |M| - 1$, что противоречит полученному выше равенству.

б) Пусть f сюръективно. Тогда $|f(M)| = |M|$. Если бы f не было инъективным, то существовали бы элементы m и m′ в M такие, что $m \neq m'$ и $f(m) = f(m')$. Тогда выполнялось бы равенство $f(M) = f(M - m)$, а из него вытекает, что $|f(M)| \leqslant |M| - 1$, что противоречит предположению.

«ПРИНЦИП ЯЩИКОВ» ДЕДЕКИНДА

«Принцип ящиков» Дедекинда — это один из важнейших методов доказательств, имеющий особенно широкое применение в теории конечных автоматов. Он состоит в следующем: если m объектов распределяются по n ящикам и $m > n$, то по меньшей мере один ящик содержит более одного объекта. Формально этот принцип выражается следующим образом: если G и S — конечные множества и $|G| > |S|$, то не существует биекции из G на S.

Доказательство (от противного). Если бы существовала биекция f из G на S, то выполнялись бы равенства $|S| = |f(G)| = |G|$, что противоречит предположению.

[1] Доведение до абсурда (лат.) — *Прим. перев.*

Пример. В качестве части доказательства корректности метода Варшалла (из разд. 1.3) должно быть доказано следующее утверждение: пусть R — отношение на конечном множестве M; тогда $(x, y) \in R^+$ в том и только в том случае, когда в графе отношения R существует путь длины не более $|M|$ из x в y, т. е. когда существуют $m \leqslant |M|$ и пары (x_i, y_i) при $i=1, \ldots, m$ такие, что $x_1=x$, $y_m=y$ и $x_{i+1}=y_i$ при $i=1, \ldots, m-1$.

Доказательство. Пусть $(x, y) \in R^+$ и (x_j, y_j), $j=1, \ldots, n$, где $x_1=x$, $y_n=y$ и $x_{j+1}=y_j$ — путь минимальной длины из x в y. Если бы было выполнено неравенство $n>|M|$, то не все x_j при $j=1, \ldots, n$ были бы различны, поскольку отображение $f: \{1, \ldots, n\} \to M$ по «принципу ящиков» Дедекинда не может быть биекцией. Пусть, скажем, $x_i=x_k$ при некоторых $1 \leqslant i < k \leqslant n$. Тогда существует путь $(x_1, y_1), (x_2, y_2), \ldots, (x_{i-1}, y_{i-1}), (x_k, y_k), \ldots, (x_n, y_n)$ из x в y длины, меньшей n, что противоречит предположению о минимальности n. Итак, должно выполняться неравенство $n \leqslant |M|$. ■

ДОКАЗАТЕЛЬСТВО МЕТОДОМ ПОЛНОЙ ИНДУКЦИИ

В рассмотренных выше примерах использовался тот факт, что в каждом непустом множестве натуральных чисел содержится наименьший элемент. Это свойство множества натуральных чисел может быть сформулировано следующим образом.

Принцип полной индукции: если $T \subseteq \mathbf{N}_0$, $k \in \mathbf{N}_0$ и выполнены условия:

1) $k \in T$;

2) для каждого n из $\mathbf{N}_0$ при $n \geqslant k$ из $\{k, k+1, \ldots, n\} \subseteq T$ вытекает, что $(n+1) \in T$,

то $\mathbf{N}_0 - \{1, \ldots, k-1\} \subseteq T$.

Отметим, в частности, что если $k=0$, то $T=\mathbf{N}_0$.

Действительно, если бы существовало число $m \in (\mathbf{N}_0 - \{1, \ldots, k-1\}) - T$, то существовало бы и наименьшее число m_0 с таким свойством. Из условия 1) следует, что должно быть выполнено неравенство $m_0 > k$. Но тогда $\{k, k+1, \ldots, m_0-1\} \subseteq T$, а отсюда и из условия 2) вытекает, что $m_0 \in T$.

Доказательство методом полной индукции проводится следующим образом. Пусть требуется доказать, что некоторое высказывание $P(n)$ верно при всех $n \geqslant k$. В этом случае выполняются следующие построения.

1. *Посылка индукции.* Доказывается справедливость $P(k)$.

2. *Заключение по индукции*:

а) **Предположение индукции.** Предполагается, что для некоторого произвольного, но фиксированного $n \geqslant k$, высказывание $P(i)$ верно при всех i из множества $\{k, k+1, \ldots, n\}$ [можно предполагать лишь истинность $P(n)$].

б) *Индуктивный шаг.* Доказывается, что если верно предположение индукции, то верно и $P(n+1)$.

По принципу полной индукции в этом случае $P(n)$ выполнено при всех $n \geqslant k$.

Примеры. 1. Пусть M и K — непустые конечные множества, $|M|=m$ и $|K|=k$. Тогда существует ровно k^m различных отображений из M в K.

Доказательство. Проведем доказательство методом полной индукции по m. Пусть K — произвольное фиксированное множество и $|K|=k$. Для любого множества M, где $|M|=m$, пусть $a(m, k)$ — число различных отображений из M в K.

Посылка индукции. Пусть $m=1$ (k произвольно). Тогда множество M — одноэлементное, например $M=\{x\}$. Но в этом случае для каждого y из K существует в точности одно отображение f из M в K, определяемое равенством $f(x)=y$. Поэтому $a(1, k)=k=k^m$.

Предположение индукции. Пусть m — некоторое произвольное, но фиксированное натуральное число. Предположим, что утверждение $a(m, k)=k^m$ справедливо для любого множества M, где $|M|=m\geqslant 1$ при произвольном k.

Индуктивный шаг. Пусть теперь M — множество такое, что $|M|=m+1$. Так как $m\geqslant 1$, то в M содержится по меньшей мере два элемента. Пусть A_x для некоторого фиксированного элемента x из M есть множество всех отображений из M—x в K. Из предположения индукции имеем $|A_x|=k^m$. Множество A всех отображений из M в K получаем, сопоставляя каждому отображению f' из A_x совокупность из k отображений f, совпадающих на M—x с f'. Таким образом, для множества графиков A_G отображений из M в K имеем $A_G=\{qrf'\cup(x, y)\,|\,f'\in A_x, y\in K\}$, а отсюда следует, что $a(m, k)=|A_G|=|A_x|\cdot k=k^m\cdot k=k^{m+1}$. Утверждение доказано.

В качестве частного случая при $k=2$ получаем равенство $|\mathscr{P}(M)|=2^m$, так как множество отображений из M в $\{0, 1\}$ есть множество характеристических функций подмножеств множества M, а это множество может быть биективно отображено на $\mathscr{P}(M)$.

2. **Утверждение:** метод Варшалла корректен.

Доказательство. Пусть M, R и R_0 определены, как при описании метода, и $R_{j+1}=R_j\cdot R$ для произвольного j из $\mathbf{N}_0$. Нам необходимо показать, что при любом j из **N** выполнено равенство

$R_j=\{(x, y)\,|$ в графе отношения R существует путь длины j из x в y$\}$.

Посылка индукции. Пусть $j=1$. Тогда $R_j=R$ и утверждение выполнено.

Предположение индукции. Пусть утверждение о R_j истинно при некотором $j\geqslant 1$.

Индуктивный шаг. По построению $R_{j+1}=R_j\cdot R$. Поэтому включение $(x, y)\in R_{j+1}$ выполняется тогда и только тогда, когда существует $z\in M$ такое, что в графе отношения R содержатся путь длины j из x в z и ребро (z, y), составляющие путь длины $j+1$ из x в y. ■

ГЛАВА 2.

АВТОМАТЫ МИЛИ

2.1. ВВОДНЫЙ ПРИМЕР

В качестве вводного примера будет рассмотрена практическая задача. Ниже мы увидим, каким образом приведенное здесь решение этой задачи может быть упрощено.

Пример 2.1.1. В силовой установке требуется постоянно контролировать направление вращения цилиндрического вала с помощью автономно работающего прибора. Этот прибор должен в определенные моменты времени выдавать соответствующий направлению вращения вала сигнал, который далее может использоваться в других звеньях системы управления.

Допустим, что в качестве датчика на конце вала закреплена изолированная от него шайба, разделенная на четыре сектора, из которых одна пара противоположных секторов сделана проводящей, а другая — непроводящей. Пусть также у свободной стороны шайбы расположен скользящий контакт (щетка), который держит шайбу под постоянным напряжением. Два других скользящих контакта B_1 и B_2 размещены так, что они касаются края шайбы и пробегают при ее вращении выделенные секторы один за другим, и, кроме того, могут одновременно находиться в пределах наименьшего из секторов. Напряжения на контактах B_1 и B_2 рассматриваются как входы конструируемого автомата A, и считается, что эти входы (при соответствующем нормировании) принимают значения 0 и 1. В качестве выхода автомата A можно использовать напряжение 1, если шайба вращается по часовой стрелке, и напряжение 0, если она вращается в противоположном направлении (рис. 2.1.1.).

Техническая реализация прибора далее обсуждаться не будет. Скажем только, что в системе предполагается наличие датчика тактов, устанавливающего моменты времени, в которые автомат A воспринимает входы и вырабатывает соответствующий выход. Следует отметить, что промежутки времени, в течение которых измеряются напряжения на контактах, должны быть очень короткими по сравнению с периодом вращения.

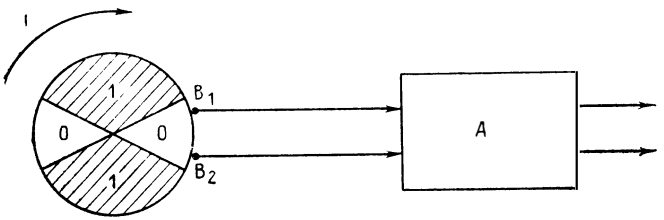


Рис. 2.1.1. Индикатор

Итак, в данном случае имеются четыре варианта входных комбинаций (входов) автомата A. a=(0, 0), b=(1, 0), c=(1, 1), d=(0, 1), где пара (i, j) означает, что к контакту B_1 приложено напряжение i, а к контакту B_2 — напряжение j.

Поскольку очевидно, что по отдельному входу автомата направление вращения определено быть не может, то ясно, что автомат должен в некотором смысле суммировать входы в предшествующие моменты времени и запоминать каким-либо способом состояние системы в данный момент для использования этой информации в дальнейшем. В качестве состояний системы будем рассматривать восемь пар, первая компонента которых — последний по времени вход, а вторая — выход (0 или 1):

$z_1=(a, 1)$, $z_2=(b, 1)$, $z_3=(c, 1)$,

$z_4=(d, 1)$, $z_5=(d, 0)$, $z_6=(c, 0)$,

$z_7=(b, 0)$, $z_8=(a, 0)$.

По состоянию и (новому) входу (например, по z_1 и a, или по z_1 и b, или z_1 и d и так далее) непосредственно может быть определено направление вращения (выход при z_1 и a равен 1, при z_1 и b равен 1, при z_1 и d равен 0 и так далее).

Некоторые комбинации состояний и входов недопустимы: z_1 или z_8 и c, z_2 или z_7 и d, z_3 или z_6 и a, z_4 или z_5 и b. В таких случаях следует предполагать, что произошла ошибка, а автомат должен порождать выход (1), сигнализирующий об этом. Мы будем считать, что ошибочный вход прекращается в тот момент, когда в автомат A поступает сигнал, отличный от ошибочного.

Итак, автомат A имеет два рода выходов (выходных информаций): один — для указания направления вращения вала и второй — для сигнализации об ошибках (0 в случае, если ошибки не было). Итак, A имеет четыре выходных комбинации (четыре выхода): p=(0, 0), q=(1, 0), r=(1, 1), s=(0, 1), где первая компонента каждой пары определяет направление вращения.

Теперь можно описать способ функционирования автомата A таблицей, в которой новое состояние и соответствующий выход ставятся в соответствие старому состоянию и полученному входу (при этом вместо z_i мы пишем просто i) (рис. 2.1.2).

Отметим, что мы не делали никаких предположений о том, в каком именно состоянии находится автомат в начале своей работы, так что первые его выходы могут оказаться неверными — так же, как и при наличии ошибки во входе. Однако не позже того, как ось совершит один оборот, выход станет верным (конечно, если не будет ошибок во входе).

Автомат A может быть очень удобно описан графом, изображенным на рис. 2.1.3.

Направления стрелок от 1 к 2 и соответственно от 5 к 6 и т. д. соответствуют направлению вращения шайбы.

Рассмотренный датчик может быть описан также как автомат с множеством входов X={a, b, c, d}, множеством выходов Y={p,

Состояние \ Вход	a	b	c	d
1	1/q	2/q	1/r	5/r
2	8/p	2/q	3/q	2/r
3	3/r	7/p	3/q	4/q
4	1/q	4/r	6/p	4/q
5	1/q	5/s	6/p	5/p
6	6/s	7/p	6/p	4/q
7	8/p	7/p	3/q	7/s
8	8/p	2/q	8/s	5/p

Рис. 2.1.2. Таблица автомата A

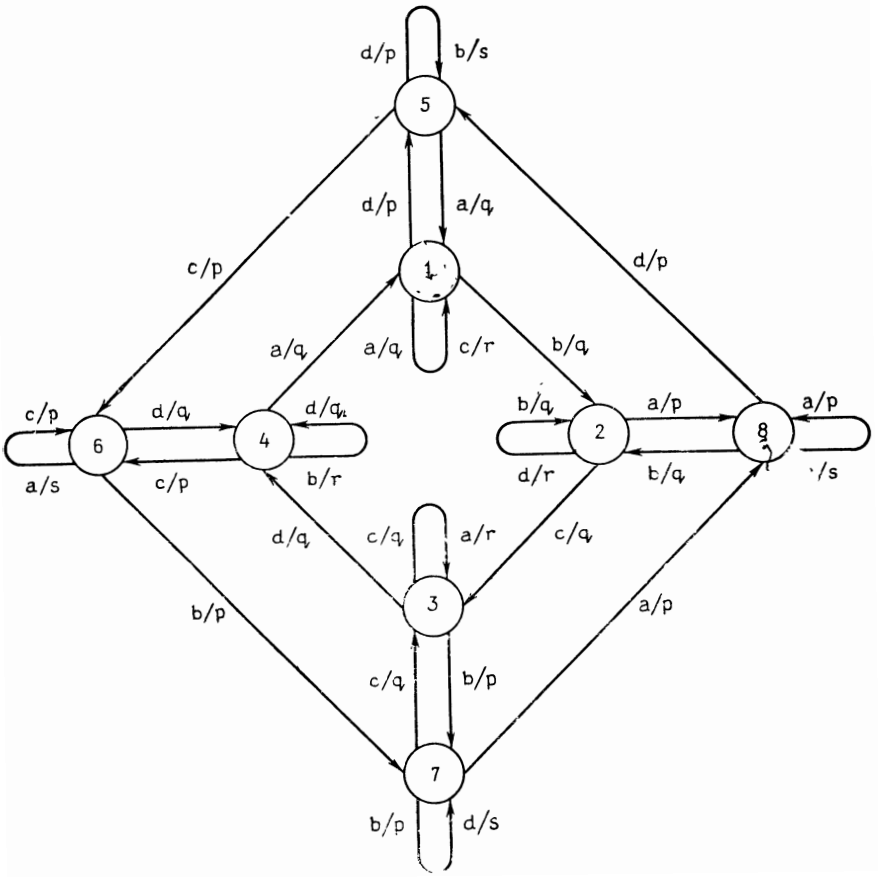


Рис. 2.1.3. Граф автомата A

q, r, s} и множеством состояний $Z=\{z_1, \ldots, z_8\}$. Функционирование этого автомата (зависимость изменения состояний и выходов от входов в данных состояниях) будет при этом задаваться вышеприведенной таблицей, т. е. двумя функциями $f: Z\times X\to Z$ и $g: Z\times X\to Y$.

Дальнейшие примеры можно найти в упражнениях 2.1—2.4.

2.2. ОПРЕДЕЛЕНИЕ, ПРИМЕР И КОНТРПРИМЕР

Автоматы рассмотренного выше типа будут теперь формально определены и исследованы.

ОПРЕДЕЛЕНИЕ АВТОМАТА МИЛИ

Определение 2.2.1. (Конечный) *автомат Мили* есть пятерка $A=(Z, X, Y, f, g)$. Здесь Z, X и Y — конечные множества (множества *состояний, входов* и *выходов* соответственно), а f и g — отображения (функции *переходов* и *выходов* соответственно), причем $f: Z\times X\to Z$ и $g: Z\times X\to Y$, g — сюръекция.

Равенство $f(z, x)=z'$ означает, конечно, что при входе x автомат, находящийся в состоянии z, переходит в состояние z', а равенство $g(z, x)=y$ означает, что при этом на выходе появляется y.

Требование сюръективности для отображения g не является существенным ограничением. Действительно, в Y не имеет смысла включать элементы, которые заведомо не могут появиться на выходе. Часто, однако, множество выходов определяют «с запасом», т. е. бóльшим, чем это необходимо в действительности.

Замечание. Из приведенного примера легко видеть, каким образом автоматы Мили могут быть представлены взвешенными ориентированными *графами*.

Представлению некоторого автомата Мили графом отвечает конструкция так называемой *переходно-выходной матрицы*: пусть $A=(Z, X, Y, f, g)$, где $Z=\{z_1, \ldots, z_n\}$, тогда переходно-выходной матрицей для A называется $n\times n$-матрица $M=\|m_{ik}\|$ с $m_{ik}=\{(x, y)\in X\times Y \mid f(z_i, x)=z_k, g(z_i, x)=y\}$.

Указание. В дальнейшем, если не оговорено противное, мы будем считать, что любой рассматриваемый автомат Мили задан в виде, соответствующем определению 2.2.1. Кроме того, будем считать, что ни одно из множеств X, Y и Z не пусто.

Попробуем теперь построить автомат, выполняющий арифметические операции над целыми неотрицательными двоичными числами. Двоичные числа должны при этом обрабатываться последовательно, т. е. за i-й такт (i=1, 2, ...) должны вводиться i-е разряды всех операндов (аргументов операции, рассматриваемой как отображение), начиная с самых младших разрядов, и должен появляться на выходе i-й разряд результата. При этом подразумевается, что вслед за старшим разрядом любого числа идет необходимое число нулей.

Пример 2.2.2. Автомат для последовательного сложения (последовательностный сумматор) определяется графом, изображенным на рис. 2.2.1. Состояние z_i этого автомата соответствует «переносу i в следующий разряд». Автомат должен начинать работу в состоянии z_0.

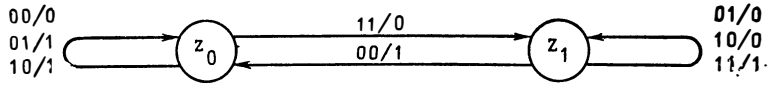


Рис. 2.2.1. Граф последовательностного сумматора

В то же время имеет место следующее утверждение.

КОНТРПРИМЕР

Теорема 2.2.3. Не существует конечного автомата Мили, способного перемножать сколь угодно длинные (большие) двоичные числа.

Доказательство. *Предположение*: пусть существует конечный автомат Мили, способный перемножать произвольные двоичные числа, и пусть этот автомат A имеет n состояний, $n<p$.

Утверждение: автомат A не может вычислить произведение $2^p \cdot 2^p$.

Доказательство. Автомат A начинает работу в некотором состоянии. В течение первых 2p тактов A должен выдавать в качестве выхода 0 независимо от того, в каком состоянии он находится и получает ли он в качестве входа 00 или 11. В $(2p+1)$-м такте (т. е. тогда, когда должен быть определен старший разряд результата) автомат A будет находиться в некотором состоянии, в котором он уже был по меньшей мере один раз после того, как получил на вход 11. Это вытекает из того, что вследствие неравенства $p>n$ не все состояния, в которых A находился после получения на входе 11, различны, и из того, что после входа 11 автомат A еще p раз получил на входе 00. Поэтому вход 00 на $(2p+1)$-м такте должен, как и раньше, приводить к выходу 00, чего быть не должно. ■

Теорема и ее доказательство демонстрируют ограниченность возможностей автоматов Мили, выражающуюся в некоторой «забывчивости» — при длинных входных последовательностях последние выходы зависят только от последних входов.

2.3. РЕАКЦИЯ, ЭКВИВАЛЕНТНОСТЬ, СОКРАЩЕНИЕ

Чтобы достаточно подробно изучить возможности автоматов Мили, нужно описывать формальным образом поведение таких автоматов на протяжении длительных отрезков времени (т. е. в течение достаточно длинных последовательностей тактов). Иначе говоря, нужно определять, как некоторый автомат Мили

реагирует на конечные последовательности входов. Для этого будем рассматривать конечные последовательности входов из X как элементы *порожденного множеством* X *свободного моноида* F(X) (см. гл. 1):

входную последовательность длины n запишем как *слово* $x_1, \ldots, x_n$ из F(X) (где $x_i \in X$);

последовательность длины 0 (что означает «отсутствие входа») есть единичный элемент Λ из F(X) (термин: *пустое слово*);

полугрупповая операция в F(X) — конкатенация: $u \cdot v = uv$;

$|w|$ означает длину входной последовательности w (слова w из F(X));

X^n — множество всех слов w из F(X), имеющих длину n:

$$X^n = \{w \in F(X) \mid |w| = n\}, \text{ так что } X^0 = \{\Lambda\} \text{ и } X^{n+1} = X^n \cdot X.$$

Точно так же мы будем рассматривать выходные последовательности как элементы моноида F(Y).

РЕАКЦИЯ И ЭКВИВАЛЕНТНОСТЬ СОСТОЯНИЙ И АВТОМАТОВ МИЛИ

Определение 2.3.1. Пусть $A = (Z, X, Y, f, g)$ — автомат Мили, а F(X) и F(Y) — порожденные множествами X и Y соответственно свободные моноиды с единичным элементом Λ.

1. Отображения $f^* : Z \times F(X) \to Z$ и $g^* : Z \times F(X) \to F(Y)$ задаются равенствами:

$$f^*(z, \Lambda) = z \text{ и } g^*(z, \Lambda) = \Lambda \text{ для всех } z \text{ из } Z;$$

$$f^*(z, wx) = f(f^*(z, w), x) \text{ и } g^*(z, wx) = g^*(z, w)\, g(f^*(z, w), x)$$

для всех z из Z, x из X и w из F(X).

2. Реакцией состояния z (для любого z из Z) называется порожденное этим состоянием входно-выходное отображение, т. е. отображение $g_z : F(X) \to F(Y)$, где $g_z(w) = g^*(z, w)$. *Реакцией* автомата A называется множество реакций всех его состояний: $L_A = \{g_z \mid z \in Z\}$.

3. *Состояния* z и z′ из Z называются *эквивалентными*, если они имеют одинаковые реакции, т. е. если $g_z = g_{z'}$. *Автоматы Мили* A и A′ называются *эквивалентными*, если они имеют одинаковые реакции, т. е. если L(A) = L(A′). Автомат Мили A называется *сокращенным*, если два любых различных состояния этого автомата не эквивалентны.

По поводу последней части определения 2.3.1 заметим, что для равенства двух отображений необходимо совпадение их областей определения, так что эквивалентные автоматы Мили с непустыми множествами состояний должны иметь одинаковые множества входов и выходов.

Замечание. Нетрудно заметить, что эквивалентность состояний (соответственно автоматов Мили) является рефлексивным, симметричным и транзитивным отношением на множестве всех состояний данного автомата (на множестве всех автоматов Мили).

Таким образом, она оказывается также отношением эквивалентности в чисто математическом смысле.

Как нетрудно видеть, автоматы из примеров 2.1.1 и 2.2.2 — сокращенные (достаточно рассмотреть входные последовательности длины 1).

Ясно также, что реакция автомата Мили на последовательное введение входных слов v и w должна быть равна его реакции на входное слово vw, — это непосредственно вытекает из п. 1 определения 2.3.1, что показывает разумность этого определения.

Теорема 2.3.2. Пусть $A=(Z, X, Y, f, g)$ — автомат Мили. Тогда для произвольных слов v и w из $F(X)$ и произвольного z из Z выполняются равенства:

$$f^*(z, v, w)=f^*(f^*(z, v), w);$$
$$g^*(z, vw)=g^*(z, v)g^*(f^*(z, v), w).$$

Доказательство. Оба утверждения будут доказаны методом полной индукции по длине слова w.

Пусть $|w|=0$, т. е. $w=\Lambda$. Тогда из определения 2.3.1 имеем:

$$f^*(z, v\Lambda)=f^*(z, v)=f^*(f^*(z, v), \Lambda);$$

$$g^*(z, v\Lambda)=g^*(z, v)=g^*(z, v)g^*(f^*(z, v), \Lambda).$$

Допустим теперь, что утверждение выполнено для всех w из $F(X)$ таких, что $|w|=k\geqslant 0$, и что $w=w'x$ — слово из $F(X)$, причем $x\in X$ и $|w'|=k$. Из определения 2.3.1 и предположения индукции (примененного к w') вытекают равенства:

$$f^*(z, vw)=f^*(z, vw'x)=f(f^*(z, vw'), x)=f(f^*(f^*(z, v), w'), x)=$$
$$=f^*(f^*(z, v), w'x)=f^*(f^*(z, v), w);$$
$$g^*(z, vw)=g^*(z, vw'x)=g^*(z, vw')g(f^*(z, vw'), x)=$$
$$=g^*(z, v)g^*(f^*(z, v), w')g(f^*(z, vw'), x)=$$
$$=g^*(z, v)g^*(f^*(z, v), w'x)=g^*(z, v)g^*(f^*(z, v), w).\blacksquare$$

Теперь мы можем доказать наиболее важную для автоматов Мили теорему.

Теорема 2.3.3. (теорема Хаффмана — Мили). Для эквивалентности двух состояний автомата Мили с n состояниями ($n>0$) достаточно, чтобы совпадали реакции этих состояний на входные последовательности длины, не превышающей $n-1$.

Доказательство. Пусть A — автомат Мили (как в определении 2.2.1). При любом натуральном числе k два состояния z и z′ автомата A будем называть *k-эквивалентными*, если для всех w из X^k выполнено равенство $g^*(z, w)=g^*(z', w)$. Здесь k-эквивалентность состояний является, очевидно, рефлексивным, симметричным и транзитивным отношением на Z. Пусть K_k — множество классов k-эквивалентных состояний из Z. Поскольку $(k+1)$-эквивалентные состояния являются также и k-эквивалентными, то каждый класс $(k+1)$-эквивалентности целиком содержится в некотором классе k-эквивалентности. Поэтому для любого натурального числа k выполняется неравенство $|K_k|\leqslant|K_{k+1}|$.

Промежуточное утверждение 1. Если выполняется равенство $K_i=K_{i+1}$, то при всех $j>i$ справедливо также равенство $K_j=K_i$, т. е. в таком случае i-эквивалентные состояния просто эквивалентны.

Доказательство. Нужно показать, что из $K_i=K_{i+1}$ вытекает $K_{i+1}=K_{i+2}$. Пусть z и z' — два состояния автомата A. Легко видеть, что в приведенной ниже последовательности высказываний каждое предыдущее влечет за собой последующее и наоборот:

z и z′ являются (i+2)-эквивалентными;

для всех x, x′ из X и w из X^1 выполнено равенство $g(z, x)\,g^*(f(z, x), wx')=g(z', x)\,g^*(f(z', x), wx')$;

$g(z, x)=g(z', x)$, а $f(z, x)$ и $f(z', x)$ являются (i+1)-эквивалентными состояниями при всех x из X;

$g(z, x)=g(z', x)$, а $f(z, x)$ и $f(z', x)$ являются i-эквивалентными состояниями при всех x из X;

для всех x из X и w из X^1 выполнены равенства $g(z, x)=g(z', x)$ и $g^*(f(z, x), w)=g^*(f(z', x), w)$;

для всех x из X и w из X^1 выполнено равенство $g^*(z, xw)=g^*(z', xw)$;

z и z′ являются (i+1)-эквивалентными.

Промежуточное утверждение 1 доказано.

Промежуточное утверждение 2. Если $K_i\neq K_{i+1}$, то $|K_i|\geqslant i+1$ для $i=1, 2, \ldots$

Доказательство. Справедливость утверждения будет доказана методом полной индукции по i.

Итак, пусть $i=1$ и $K_1\neq K_{i+1}$. Если бы выполнялось равенство $|K_1|=1$, то любые два состояния z и z′, а также и состояния $f(z, x)$ и $f(z', x)$ при произвольном входе x были бы 1-эквивалентны. Поэтому z и z′ были бы и 2-эквивалентны, т. е. было бы $K_1=K_2$, что противоречит предположению. Итак, должно выполняться неравенство $|K_1|\geqslant 2$. Для $i=1$ утверждение доказано.

Предположим, что утверждение выполнено при $i=k$ и что $K_k\neq K_{k+1}$. Если бы было выполнено неравенство $|K_{k+1}|<k+2$, то мы бы имели $k+1\leqslant|K_k|\leqslant|K_{k+1}|<k+2$, а отсюда вытекает, что $K_k=K_{k+1}$, что противоречит предположению.

Промежуточное утверждение 2 доказано.

Поскольку автомат A имеет только n состояний, то из вспомогательного утверждения 2 следует, что $|K_{n-1}|=|K_n|$. Из вспомогательного утверждения 1 вытекает, что в этом случае (n—1)-эквивалентность является эквивалентностью на множестве состояний автомата A. ■

Неулучшаемость границы n—1 в только что доказанной теореме показана в п. 1 упражнения 2.5.

Следствие 2.3.4. Проблема эквивалентности состояний автоматов Мили разрешима.

Метод определения классов эквивалентности состояний описан в разд. 2.4 и 2.5.

Следствие 2.3.5. Для автомата Мили A и A′ с m и n состояниями соответственно эквивалентны, если их реакции на все входные

последовательности длины, не большей $m+n-1$, совпадают. Вследствие этого проблема эквивалентности автоматов Мили разрешима.

Доказательство. Если бы автоматы A и A′ имели различные множества входов или выходов, то они по определению не могли бы быть эквивалентны. Поэтому мы можем предположить, что $A=(Z, X, Y, f, g)$ и $A'=(Z', X, Y, f', g')$, где Z и Z′—дизъюнктные (непересекающиеся) множества. Автоматы A и A′ можно объединить в один новый автомат $B=(\bar{Z}, X, Y, \bar{f}, \bar{g})$, где $\bar{Z}=Z \cup Z'$, $gr\bar{f}=grf \cup grf'$ и $gr\bar{g}=grg \cup grg'$. Вместо того чтобы доказывать, что автоматы A и A′ эквивалентны, достаточно показать, что для каждого состояния z автомата B, принадлежащего множеству Z, найдется эквивалентное состояние z′ автомата B, принадлежащее Z′ и наоборот. Из предыдущей теоремы вытекает, что для этого могут понадобиться входные последовательности, не большей, чем $m+n-1$, длины. ■

В п. 2 упражнения 2.5 показано, что число $m+n-1$ в следствии 2.3.5 не может быть выбрано меньшим.

ПОСТРОЕНИЕ СОКРАЩЕННОГО АВТОМАТА МИЛИ

Теорема 2.3.6 (теорема о сокращении). Для каждого автомата Мили может быть эффективно построен эквивалентный сокращенный автомат Мили.

Доказательство. Эквивалентный автомату A сокращенный автомат A_r получаем, объединяя все эквивалентные некоторому состоянию автомата A состояния этого автомата в одно отдельное состояние автомата A_r и определяя соответствующим образом функции переходов и выходов. Итак, положим, что $[z]$ — класс всех состояний автомата A, эквивалентных состоянию z этого автомата. Тогда A_r задается следующим образом: $A_r=(\{[z] \mid z \in Z\}, X, Y, f_r, g_r)$, где $f_r([z], x)=[f(z, x)]$ и $g_r([z], x)=g(z, x)$. Легко видеть, что отображения f_r и g_r определены корректно (независимо от выбора представителей в классе $[z]$) и что автоматы A_r и A эквивалентны.

Из теоремы 2.3.3 вытекает, что классы $[z]$ могут быть построены эффективно. ■

Для того чтобы лучше усвоить понятие сокращенного автомата Мили, читателю рекомендуется попытаться выполнить упражнение 2.6.

Дальнейшие возможности представления входно-выходного поведения автоматов Мили даются в упражнениях 2.7—2.10.

2.4. О СПОСОБЕ ОПРЕДЕЛЕНИЯ ЭКВИВАЛЕНТНОСТИ СОСТОЯНИЙ

Из доказательства теоремы 2.3.3. можно получить простой и (для автоматов с небольшим числом состояний) более менее быстрый метод определения эквивалентности состояний. Основная идея этого метода выражается следующим правилом.

(R_k). Состояния z и z′ k-эквивалентны ($k \geqslant 2$) тогда и только тогда, когда они 1-эквивалентны и когда при любом входе x состояния f(z, x) и f(z′, x) (k—1)-эквивалентны.

Итак, прежде всего должно быть определено отношение 1-эквивалентности. Далее последовательно [на основе правила (R_k)] должны определяться отношения k-эквивалентности для $k \geqslant 2$ до тех пор, пока отношения (k—1)- и k-эквивалентности не совпадут, что произойдет в худшем случае при k=n (см. проведенное выше доказательство).

Поскольку k-эквивалентность является рефлексивным, симметричным и транзитивным отношением, нет необходимости в перечислении всех пар k-эквивалентных состояний. Достаточно описать разбиение множества состояний на классы k-эквивалентности Для этой цели занумеруем состояния, т. е. положим, что $Z=\{z_1, \ldots, z_n\}$, и будем описывать отношения k-эквивалентности n-ками

Введем еще одно обозначение: для n-ки T j-ю компоненту будем обозначать T(j).

Итак, пусть k-эквивалентность представлена n-кой $\bar{A}_k$, где $A_k(j)$ — наименьший из всех индексов $i>0$, для которого z_i и z_j k-эквивалентны. При этом считается, что i может быть равно j, так что, в частности, $\bar{A}_k(1)=1$. В этом случае два состояния z_p и z_q являются k-эквивалентными тогда и только тогда, когда $\bar{A}_k(p)=\bar{A}_k(q)$.

Для того чтобы вычислить $\bar{A}_1$, занумеруем прежде всего входы, т. е. положим, что $X=\{x_1, \ldots, x^m\}$.

Далее будем действовать следующим образом. Прежде всего, вычислим n-ку $\bar{A}^1{}_1$, где для каждого j=1, ..., n компонента $\bar{A}^1{}_1(j)$ есть наименьший индекс $i>0$, для которого $g(z_i, x_1)=g(z_j, x_1)$ (допускается, что i=j!). Итак, $\bar{A}^1{}_1$ задает классы состояний с одинаковым выходом при входе x_1.

Определим теперь последовательно для r=2, ..., m по $\bar{A}_1{}^{r-1}$ соответствующие n-ки $\bar{A}^r{}_1$: для j=1, ..., n компонента $\bar{A}^r{}_1(j)$ есть наименьший индекс $i>0$, для которого $\bar{A}_1{}^{r-1}(i)=A_1{}^{r-1}(j)$ и $g(z_i, x_r)=g(z_j, x_r)$. В результате получим n-ку $\bar{A}^r{}_1$, задающую классы состояний, которые при каждом входе x_s, где s= 1, ..., r, порождают соответствующие равные выходы. Очевидно, что $\bar{A}^m{}_1=\bar{A}_1$.

Для построения A_k по A_1 и A_{k-1} действуем аналогично: определяем последовательно n-ки $\bar{A}^r{}_k$ для r=1, ..., m так, чтобы выполнялось равенство $\bar{A}^m{}_k=\bar{A}_k$. При этом $\bar{A}^r{}_k$ задает классы состояний, которые, с одной стороны, являются 1-эквивалентными и, с другой стороны, имеют (k—1)-эквивалентные последующие состояния при входах x_s для s= 1, ..., r.

При j=1, ..., n компонента $\bar{A}^1{}_k(j)$ является, таким образом, наименьшим из индексов $i>0$, для которого состояния z_i и z_j 1-эквивалентны и состояния $f(z_i, x_1)$ и $f(z_j, x_1)$ — (k—1)-эквивалентны.

При r=2, ..., m компонента $\bar{A}^r{}_k(j)$ — это наименьший из индексов $i>0$, для которого $\bar{A}_k{}^{r-1}(i)=\bar{A}_k{}^{r-1}(j)$ и состояния $f(z_i, x_r)$ и $f(z_j, x_r)$ — (k—1)-эквивалентны.

Во многих случаях может применяться ускоренный вариант описанного метода, в котором при $k>1$ для определения $\bar{A}^1{}_k$ вместо $\bar{A}_1$ используется $\bar{A}_{k-1}$, т. е. $\bar{A}^1{}_k$ задается правилом: $\bar{A}^1{}_k(j)$ — минимальный индекс $i>0$, для которого z_i и z_j (k—1)-эквивалентны и $f(z_i, x_1)$ и $f(z_j, x_1)$ тоже (k—1)-эквивалентны. Аналогично для определения $\bar{A}^r{}_k$ при $r>1$ вместо $\bar{A}_{k-1}$ используется $\bar{A}_k{}^{r-1}$.

ПРОСТЕЙШИЙ ТАБЛИЧНЫЙ МЕТОД

Пример 2.4.1 (определение классов эквивалентных состояний) Зададим автомат Мили A_1 графом, изображенным на рис. 2.4.1. Представим этот автомат его таблицей (см. замечание к определению 2.2.1) и продолжим эту таблицу по описанному выше способу четверками $\bar{A}^1{}_1$, $\bar{A}^2{}_1=\bar{A}_1$, $\bar{A}^1{}_2$, $\bar{A}^2{}_2=\bar{A}_2$ и так далее, записывая их как столбцы (рис. 2.4.2). Поскольку $\bar{A}^2{}_3=\bar{A}^2{}_2$, то $\bar{A}_3=\bar{A}_2$. Итак, эквивалентны только состояния z_1 и z_3, а состояния z_2 и z_4 не эквивалентны ни между собой, ни другим состояниям.

Легко видеть, что описанный метод может быть усовершенствован:

если определена n-ка $\bar{A}_{n-1}$, то процесс закончен, поскольку $\bar{A}_{n-1}=\bar{A}_n$;

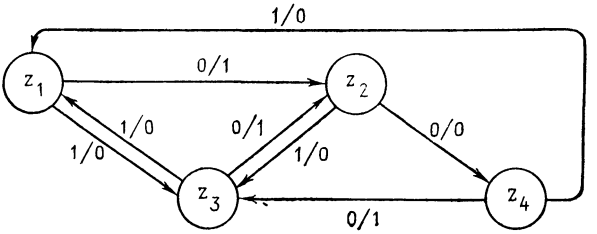


Рис. 2.4.1. Несокращенный автомат Мили A_1

	$x_1=0$	$x_2=1$	$\bar{A}^1_1$	$\bar{A}^2_1$	$\bar{A}^1_2$	$\bar{A}^2_2$	$\bar{A}^1_3$	$\bar{A}^2_3$
z_1	$z_2/1$	$z_3/0$	1	1	1	1	1	1
z_2	$z_4/0$	$z_3/0$	2	2	2	2	2	2
z_3	$z_2/1$	$z_1/0$	1	1	1	1	1	1
z_4	$z_3/1$	$z_1/0$	1	1	4	4	4	4

Рис. 2.4.2. Таблица автомата A_1 с дополнительными столбцами

вход, который во всех состояниях порождает одинаковые выходы, при $k=1$ может не рассматриваться;

при $k>1$ можно также не рассматривать вход x, сохраняющий все состояния автомата (т. е. такой вход, что для всех состояний z выполнено равенство $f(z, x)=z$), так же как и вход, переводящий все состояния в некоторое единственное состояние;

при вычислениях к таблице нужно приписывать только два столбца, а именно сначала столбцы с n-ками $\bar{A}_1^{r-1}$ и $\bar{A}^r_1$ (где $r\geqslant 2$), потом (при $k>1$) — с n-ками $\bar{A}_k^{r-1}$ и A^r_k и т. д.;

как только при некоторых j, k и r окажется выполненным равенство $\bar{A}^r_k(j)=j$, j-ю компоненту больше вычислять не нужно, а следует положить $\bar{A}_k^{r+1}(j)=j$ при $r<m$, $\bar{A}^1_{k+1}(j)=j$ при $r=m$ и далее оставлять j-ю компоненту неизменной; в частности, первая компонента каждого столбца равна 1;

для того чтобы при вычислении $\bar{A}^r_k$ не проверять для каждого j все $i<j$, можно рядом со столбцом $\bar{A}_k^{r-1}$ (или $\bar{A}_{k-1}$) добавлять еще один столбец $\bar{K}^r_k$ (соответственно $\bar{K}^1_k$), где $\bar{K}^r_k(j)=\bar{A}_k^{r-1}(i)$ [соответственно — $\bar{K}^1_k(j)=\bar{A}_{k-1}(i)$], а i определяется равенством $f(z_j, x_r)=z_i$. Столбец $\bar{A}^r_k$ (или $\bar{A}^1_k$) может быть после этого определен следующим образом: проходим оба столбца $\bar{A}_k^{r-1}$ и $\bar{K}^r_k$ (или $\bar{A}_{k-1}$ и $\bar{K}^1_k$) одновременно сверху вниз; встречая в строке i в первый раз пару $(a, b)=(\bar{A}_k^{r-1}(i), \bar{K}^r_k(i))$ [или $(a, b)=(\bar{A}_{k-1}(i), \bar{K}^1_k(i))$], полагаем $\bar{A}^r_k(j)=i$ (или $\bar{A}^1_k(j)=i$) для всех j таких, что $(\bar{A}_k^{r-1}(j), \bar{K}^r_k(j))=(a, b)$ [или $(\bar{A}_{k-1}(j), \bar{K}^1_k(j))=(a, b)$ соответственно]. Использование $\bar{K}^r_k$ оправдано только тогда, когда число классов k-эквивалентности невелико (в частности, при малых k) или если связь между парами (a, b) и соответствующими номерами строк i фиксируется в $(n\times n)$-таблицах T^r_k. Причем при первом появлении пары (a, b) номер строки i записывается на место (a, b) в таблице T^r_k, а при каждом следующем появлении пары (a, b) считывается значение, стоящее в T^r_k на месте (a, b). Можно использовать и единственную таблицу T, если записывать в нее вместе с i и соответствующие значения k и r.

Метод может применяться «вручную» только для автоматов с небольшим числом состояний, поскольку в худшем случае он требует вычисления mn^2 величин, заполняющих столбцы $\bar{A}_k^r$ (по n для каждого из самое большое mn столбцов). Кроме того, для вычисления каждой величины может понадобиться до $n-1$ сопоставлений с ранее вычисленными значениями. Если дополнительно используются столбцы $\bar{K}_k^r$ и таблица T, то все же для постоянных k и r нужно вычислить 3n величин (компонент $\bar{A}_k^r$, $\bar{K}_k^r$ и T), а для вычисления каждой из них сопоставить два значения, так что в этом случае число шагов в вычислениях имеет порядок mn^2.

2.5. МЕТОД ХОПКРОФТА — ГРИСА

БЫСТРЫЙ МЕТОД ОПРЕДЕЛЕНИЯ ЭКВИВАЛЕНТНОСТИ СОСТОЯНИЙ

Ниже описан вариант Д. Гриса метода Й. Хопкрофта, предназначенного для вычисления классов эквивалентных состояний автоматов Мили. Этот метод для автоматов с большим числом состояний n оказывается существенно более быстрым, чем вышеописанный, поскольку он в худшем случае требует для решения задачи порядка $cn\log(n)$ (c — константа, $\log(n)$ — логарифм n по основанию 2) условных единиц времени. Этот метод, конечно, сложнее, чем описанный в разд. 2.4, так что он подходит в основном только для реализации на вычислительной машине.

Важнейшие отличия описываемого ниже метода от метода из разд. 2.4 состоят в следующем.

1. Процесс определения $\bar{A}_k{}^r$ разбивается на подшаги, причем проверяется не просто то, являются ли состояния $f(z_l, x_r)$ и $f(z_j, x_r)$ (k—1)-эквивалентными, но на каждом подшаге выбирается целый класс (k—1)-эквивалентности и производится проверка: лежат ли все состояния, в которые автомат переходит из состояний выбранного класса при входе x_r, в одном классе (k—1)-эквивалентности или нет.

2. Выигрыш во времени (в числе элементарных операций) получается при этом за счет того, что можно избежать полного перебора таких классов.

3. Классы k-эквивалентных состояний рассматриваются как множества. Расщепление классов (разбиение их на подклассы) производится путем удаления из них некоторых состояний. Число таких актов расщепления может быть сделано небольшим, если классы, о которых идет речь, выбраны небольшими.

Прежде всего нам понадобятся одно определение и лемма. На их основе будет построен алгоритм последовательного приближения к решению. В заключение будет исследована сложность метода.

В дальнейшем символы Z, X, Y, f, g, n, m, A и т. п. без лишних оговорок будут использоваться, как в разд. 2.4.

Определение 2.5.1. 1. Подмножества $B_1, B_2, \ldots, B_p$ множества Z образуют *разбиение* Z, а B_i называются при этом *блоками* разбиения, если они не пусты, попарно дизъюнктны и покрывают в сумме все множество Z, т. е. если $\bigcup\{B_i \mid i=1, \ldots, p\}=Z$, причем $B_i \neq \varnothing$ и $B_i \cap B_j = \varnothing$ для $i \neq j$ при $1 \leqslant i, j \leqslant p$.

2. Разбиение $B_1, \ldots, B_p$ множества состояний Z называется *допустимым*, если все состояния из каждого блока являются 1-эквивалентными и если любые два эквивалентных состояния лежат в одном блоке разбиения $B_1, \ldots, B_p$, т. е. если из эквивалентности некоторых состояний z и z′ вытекает, что существует индекс i такой, что z и z′ лежат в блоке B_i.

Лемма 2.5.2. Разбиение множества Z, блоками которого являются классы 1-эквивалентности (разбиение на классы 1-эквивалентности), допустимо.

Доказательство. Классы эквивалентности относительно произвольного рефлексивного симметричного и транзитивного отношения на множестве Z образуют, очевидно, разбиение Z. Это же верно и для отношения 1-эквивалентности. Во всех классах соответствующего разбиения (во всех блоках) лежат только 1-эквивалентные состояния. Любые два эквивалентных состояния являются также и 1-эквивалентными (см. доказательство теоремы 2.3.3), так что они лежат в одном блоке. ■

Лемма 2.5.3. Разбиение $B_1, \ldots, B_p$ тогда и только тогда является разбиением Z на классы эквивалентных состояний, когда выполнены следующие условия:

1) разбиение допустимо;

2) для любых двух блоков B_i и B_j и любого входа x из X при любых $z, z' \in B_i$ из $f(z, x) \in B_j$ вытекает, что $f(z', x) \in B_j$.

Доказательство. а) Если разбиение $B_1, \ldots, B_p$ является разбиением множества Z на классы эквивалентных состояний, то оно допустимо, поскольку эквивалентные состояния 1-эквивалентны и поскольку (см. доказательство теоремы 2.3.3) состояния, в которые переходят эквивалентные состояния при любом входе x, снова эквивалентны.

б) Пусть выполнены условия 1) и 2) и пусть z и z′ — два произвольных состояния из произвольного блока B_i. Полной индукцией по k получаем, что состояния z и z′ являются k-эквивалентными при любом натуральном числе k, а потому и просто эквивалентными. Действительно, при $k=1$ утверждение вытекает из п. 1). Пусть оно верно при $k=q$. Из п. 2) следует, что при любом входе x из X состояния $f(z, x)$ и $f(z', x)$ — 1-эквивалентны. Из доказательства теоремы 2.3.3 в этом случае получаем, что z и z′ являются $(q+1)$-эквивалентными. ■

Переформулировав только что доказанную лемму, получим описание важнейшего шага метода Хопкрофта — Гриса.

Следствие 2.5.4. Пусть $B_1, \ldots, B_p$ — допустимое разбиение, не совпадающее с разбиением на классы эквивалентных состояний. Тогда существуют два блока B_i и B_j и вход x, для которых выполнено условие:

Существуют z и z′ в B_i такие, что $f(z, x) \in B_j$, но $f(z', x) \notin B_j$. (1)

Если в данном разбиении заменить блок B_i следующими дизъюнктными множествами:

$$\underline{B}_i = \{z \in B_i \mid f(z, x) \in B_j\} \text{ и } \overline{B}_i = \{z \in B_i \mid f(z, x) \notin B_j\},$$

то получившееся разбиение снова будет допустимым. Разбиение блока B_i на $\underline{B}_i$ и $\overline{B}_i$ описанным способом называется *расщеплением* B_i *относительно* (B_j, x).

Доказательство. Выполнение условия (1) вытекает непосредственно из леммы 2.5.3. Поскольку также выполнены условия $B_i = \underline{B}_i \cup \overline{B}_i$ и $\underline{B}_i \cap \overline{B}_i = \varnothing$, то B_1, ..., B_{i-1}, $\underline{B}_i$, $\overline{B}_i$, B_{i+1}, ..., B_p — разбиение множества Z. Все состояния в блоках $\underline{B}_i$ и $\overline{B}_i$ являются 1-эквивалентными, так как они принадлежат одному блоку B_i из допустимого разбиения.

Рассмотрим теперь два эквивалентных состояния z_1 и z_2 из B_i. Если бы состояние z_1 попало в блок $\underline{B}_i$, а состояние z_2 — в блок $\overline{B}_i$, то состояние $f(z_1, x)$ должно было бы принадлежать B_j, а состояние $f(z_2, x)$ — нет, но этого не может быть. Итак, оба состояния должны попасть в один блок, т. е. новое разбиение является допустимым. ■

Из сказанного мы немедленно получаем первый вариант описываемого метода.

Метод 2.5.5 (вариант 1 вычисления классов эквивалентности).

1. Начать с разбиения Z на классы 1-эквивалентности.
2. До тех пор, пока будут иметься блоки B_i и B_j и вход x такие, что для них будет выполнено условие (1), выполнять расщепление B_i относительно (B_j, x).

Доказательство корректности. Следует показать, во-первых, что метод сходится (дает результат за конечное число шагов), т. е. что цикл «до тех пор, пока» выполняется только конечное число раз, и, во-вторых, что получающееся разбиение является искомым разбиением на классы эквивалентных состояний.

Каждое расщепление любого блока B_i относительно любой пары (B_j, x) увеличивает число блоков на 1. Максимально возможное число блоков в любом разбиении множества Z есть $n = |Z|$, так что не более чем через $n-1$ расщепление условие (1) не будет выполнено ни для одной тройки вида (B_i, B_j, x). Это и означает, что метод сходится.

Как в начале каждого цикла «до тех пор, пока», так и после него рассматриваемое разбиение будет по построению допустимым. В момент, когда выполнение цикла станет невозможным, т. е. когда условие «до тех пор, пока» окажется невыполненным, будет выполнено условие 2) из леммы 2.5.3. Отсюда вытекает, что получившееся в результате разбиение будет в точности разбиением множества Z на классы эквивалентных состояний. ■

Аналогично тому, как из разбиения множества состояний на классы 1-эквивалентности последовательным расщеплением блоков может быть получено разбиение на классы эквивалентности, само разбиение на классы 1-эквивалентности также может быть получено путем соответствующих расщеплений, причем начинать можно с тривиального разбиения множества состояний Z, состоящего из одного блока Z, и использовать расщепления, описываемые в приведенном ниже определении.

Определение 2.5.6. Пусть $B_1, \ldots, B_p$ — разбиение множества Z.

1. Пусть x — вход из X и y — выход из Y, а B_i — блок из разбиения. *Расщеплением блока* B_i *относительно пары* (y, x) называется замена B_i двумя множествами $\underline{B}_i = \{z \in B_i \mid g(z, x) = y\}$ и $\bar{B}_i = \{z \in B_i \mid g(z, x) \neq y\}$.

2. Разбиение называется *1-допустимым,* если 1-эквивалентные состояния лежат в одном блоке.

Теперь мы немедленно получаем аналоги леммы 2.5.3 и следствия 2.5.4.

Лемма 2.5.7. 1. Разбиение $B_1, \ldots, B_p$ является разбиением множества состояний Z на классы 1-эквивалентности тогда и только тогда, когда оно 1-допустимо и когда для любого блока B_i, любого входа x и любого выхода y выполнено условие:

Из $z, z' \in B_i$ и $g(z, x) = y$ следует $g(z', x) = y$.

2. Пусть $B_1, \ldots, B_p$ — 1-допустимое разбиение, не являющееся разбиением на классы 1-эквивалентности. Тогда существуют блок B_i, вход x и выход y такие, что выполнено условие:

Существуют z и z′ в B_i такие, что $g(z, x) = y$, но $g(z', x) \neq y$. (2)

Если блок B_i расщепить относительно (y, x), то получающееся разбиение снова будет допустимым.

Доказательство. Поскольку состояния z и z′ являются 1-эквивалентными тогда и только тогда, когда выполняется равенство $g(z, x) = g(z', x)$ (для всех x из X), то ч. 1 утверждения очевидна, так же как и первое высказывание ч. 2.

Расщепление блока B_i относительно (y, x) порождает, как легко видеть, снова некоторое разбиение множества состояний Z. Поскольку для каждого z из $\underline{B}_i$ любое 1-эквивалентное состояние не может лежать в $\bar{B}_i$, но лежит в B_i, то оно должно лежать и в $\underline{B}_i$. Итак, получающееся разбиение является 1-допустимым.

Данная лемма порождает аналогичный методу 2.5.5 метод определения (вычисления) классов 1-эквивалентности.

Метод 2.5.8 (вариант 1 вычисления классов 1-эквивалентности).

1. Начать с тривиального, состоящего только из блока Z, разбиения.

2. До тех пор, пока будут иметься блок B_i, вход x и выход y такие, что для них будет выполнено условие (2), выполнить расщепление B_i относительно (y, x).

Доказательство корректности. Состоящее только из блока Z разбиение очевидным образом 1-допустимо. Каждое выполнение цикла «до тех пор, пока» на основании п. 2 леммы 2.5.7 приводит к замене 1-допустимого разбиения снова 1-допустимым разбиением.

Поскольку каждое разбиение множества Z состоит из не более чем n различных блоков, а каждое выполнение операции расщепления увеличивает число блоков на 1, то после конечного

числа циклов «до тех пор, пока» условие (2) окажется невыполненным, а это означает, что метод дает результат за конечное число шагов, т. е. сходится. В силу же п. 1 леммы 2.5.7 результатом работы будет разбиение множества состояний Z на классы 1-эквивалентных состояний. ■

Описанный метод кажется на первый взгляд менее эффективным, чем он есть на самом деле. Действительно, блок B_l, возникший в результате расщепления блока B_i относительно (y, x), а вместе с ним и все блоки B, возникающие в результате его дальнейшего расщепления, относительно пар вида (y′, x) больше расщепляться не будут. Это вытекает из того, что для тройки ($\underline{B}_i$, y′, x) (или ($\underline{B}$, y′, x)) не будет выполнено условие (2), так как для любого z из $\underline{B}_l$ уже выполнено равенство g(z, x)=y, а потому при y′≠y — и соотношение g(z, x)≠y′.

В дальнейшем, конечно, ни один блок, возникший при расщеплении относительно пары (y, x), расщепляться относительно этой пары не будет.

Поскольку порядок выбора в методе 2.5.8 тройки (B_i, y, x) не влияет на корректность этого метода, можно установить специальный порядок, позволяющий избежать лишней работы по поиску действительно расщепляемых блоков. С этой целью будем просматривать все входы x из X и для каждого x — все выходы y из Y и вносить в список L только фактически расщепляемые блоки. При этом будем вести дополнительные списки, в которые будем заносить получаемые при расщеплении блоки:

в L′ записываются при постоянном x блоки $\underline{B}_i$, полученные при расщеплении относительно (y, x);

в L″ записываются при постоянной паре (y, x) блоки $\bar{B}_i$, полученные при расщеплениях относительно этой пары;

в L_1 записываются все получающиеся одноэлементные блоки, которые далее расщепляться не могут.

Расщепление блока B_l производится путем последовательной проверки выполнения условия g(z, x)≠y для всех состояний z из B_l.

Метод 2.5.9 (вариант 2 вычисления классов 1-эквивалентности).

1. Начальный шаг: L:={Z}, L′:=∅, L″:=∅, L_1:=∅.

2. Для каждого x из X выполнить шаги 1) и 6).

1) Для каждого y из Y выполнить шаги 2) и 5).

2) До тех пор, пока не будет выполнено условие L=∅, выбирать один блок B_l из L, L:=L−{B_l} и выполнять шаги 3) и 4).

3) Если $|B_l|=1$, то занести B_l в список L_1, L_1:=L_1∪{B_l}. В противном случае занести B_l в список L′, L′:=L′∪{B_l}.

4) Для каждого z из B_l такого, что g(z, x)≠y, выполнить следующее:

проверить, содержится ли в списке L″ сопровождающий B_i блок B_k, в который должны заноситься элементы из B_l;

если блока B_k в L'' нет, организовать его: $B_k := \varnothing$, $L'' := L'' \cup \{B_k\}$;

перенести z из B_i в B_k: $B_i := B_i - \{z\}$, $B_k := B_k \cup \{z\}$;

если блок B_i оказался пустым, вычеркнуть его из списка L': $L' := L' - \{B_i\}$.

5) Переименовать L'' в L и L в L''.

6) Переименовать L' в L и L в L'.

3. Объединить L и L_1 в список L, $L := L \cup L_1$. Этот список содержит теперь классы 1-эквивалентности.

Доказательство корректности. Метод сходится, т. е. дает результат за конечное число шагов, так как должны быть последовательно обработаны пары (y, x) из конечного множества и так как цикл «до тех пор, пока» сходится (при каждом выполнении шага 2) число блоков в L уменьшается на 1).

Чтобы показать, что метод дает правильный результат, отметим сначала, что при фиксированной паре (y, x) списки L, L', L'' и L_1 перед выполнением цикла «до тех пор, пока» [шаг 2)] обладают следующими свойствами:

L содержит только те блоки, которые еще не расщеплялись относительно пары (y, x);

L' содержит только те блоки, которые не могут расщепляться относительно пар вида (y', x), где $y' \neq y$;

L'' содержит только те блоки, для которых следует проводить расщепление относительно следующих пар вида (y', x);

L_1 содержит только одноэлементные блоки.

Ясно, что после завершения «до тех пор, пока» цикла список L'' будет содержать все блоки, расщепление которых относительно последующих пар (y', x) должно еще быть исследовано, а список L будет пуст. Этим оправдывается переименование списков L и L'' на шаге 5), после которого перед выполнением шага 2) для следующей пары (y, x) приведенные выше условия для списков снова будут выполнены.

Поскольку при постоянном x при выполнении шага 2) для последнего y из Y больше никакие сопровождающие блоки B_k в L'' возникать не будут, после выполнения этого шага окажется выполненным равенство $L'' = \varnothing$, а после шага 5) — равенство $L = \varnothing$. Список L' будет содержать в этот момент все блоки. Этим оправдывается переименование списков на шаге 6), после которого перед выполнением шага 2) для следующего x для рассматриваемых списков опять-таки будут выполнены приведенные выше условия.

Итак, начиная с первого прохождения циклического шага 2) и до конца работы, списки при каждом начале выполнения шага 2) будут удовлетворять указанным условиям. Поэтому ясно, что в конце концов окажутся выполненными равенства $L' = L'' = \varnothing$, а потому в $L \cup L_1$ будут содержаться все блоки, причем ни один из них не будет расщепляться относительно любой пары (y, x). ■

Используя данный метод, мы получаем новый вариант метода 2.5.5, замечая, что порядок выбора троек (B_i, B_j, x) не имеет зна-

чения для его корректности. Это позволяет использовать специальный порядок такого выбора.

Метод 2.5.10 (вариант 2 вычисления классов эквивалентности).

1. Использовать метод 2.5.9.

2. До тех пор, пока имеются B_i, B_j и x, для которых выполнено условие (1), проводить расщепление всех имеющихся блоков относительно (B_j, x).

Ясно, что этот метод не слишком эффективен, так как он требует проверки всех возможных троек (B_i, B_j, x) с целью поиска состояний z и z′, удовлетворяющих условию (1). Поэтому мы должны, как и для метода 2.5.8, найти способ уменьшения числа рассматриваемых блоков. Этот способ вытекает из следующих двух лемм.

Лемма 2.5.11. После выполнения в методе 2.5.10 цикла «до тех пор, пока» для некоторой тройки (B_i, B_j, x), т. е. после того, как блок B_i расщеплен относительно пары (B_j, x) на блоки $\underline{B}_i$ и $\overline{B}_i$ при любом дальнейшем выполнении этого цикла ни один из блоков, возникающих при расщеплениях $\underline{B}_i$ и $\overline{B}_i$, не должен больше расщепляться относительно пары (B_j, x).

Доказательство. Пусть B — блок, возникший при расщеплении некоторого блока относительно пары (B_j, x). Тогда для всех z из B выполнено либо условие $f(z, x) \in B_j$, либо условие $f(z, x) \notin B_j$. То же самое верно и для любого блока B′, полученного из B в результате расщепления относительно произвольной пары «блок — вход» и являющегося потому подмножеством блока B. Расщепление такого блока относительно пары (B_j, x) не дает, таким образом, ничего нового. ■

Лемма 2.5.12. Пусть дано разбиение $B_1, \ldots, B_p$ множества состояний Z и разбиение некоторого (произвольного) блока B_i на $\underline{B}_i$ и $\overline{B}_i$ (здесь $\underline{B}_i \cup \overline{B}_i = B_i$ и $\underline{B}_i \cap \overline{B}_i = \varnothing$). Пусть также x — произвольный вход. Вместо того чтобы исследовать расщепление всех блоков относительно пар (B_i, x), $(\underline{B}_i, x)$ и $(\overline{B}_i, x)$, достаточно исследовать такие расщепления относительно любых двух пар из этих трех.

Доказательство. Допустим, что уже проведено расщепление всех блоков относительно (B_i, x) и $(\underline{B}_i, x)$. Тогда, как следует из доказательства леммы 2.5.11, для каждого (нового) блока B справедливо в точности одно из следующих четырех утверждений:

1) Из $z \in B$ следует, что $f(z, x) \in B_i$ и $f(z, x) \in \underline{B}_i$.

2) Из $z \in B$ следует, что $f(z, x) \in B_i$ и $f(z, x) \notin \underline{B}_i$.

3) Из $z \in B$ следует, что $f(z, x) \notin B_i$ и $f(z, x) \in \underline{B}_i$[1].

[1] Данное утверждение обретает нетривиальный смысл после замены B_i на $\overline{B}_i$ (см. далее). — *Прим. перев.*

4) Из $z \in B$ следует, что $f(z, x) \notin B_i$ и $f(z, x) \notin \underline{B}_i$.

Так как $\underline{B}_i \cup \overline{B}_i = B_i$ и $\underline{B}_i \cap \overline{B}_i = \varnothing$, то, учитывая вышесказанное, получаем, что для B справедливо одно из двух следующих утверждений:

5) $z \in B$ влечет за собой $f(z, x) \in \overline{B}_i$.

6) $z \in B$ влечет за собой $f(z, x) \notin \overline{B}_i$.

Следовательно, расщепление блока B относительно $(\overline{B}_i, x)$ не дает ничего нового и может поэтому не проводиться.

Из соображений симметрии вытекает, что и расщепление относительно $(\underline{B}_i, x)$ может не проводиться, если уже проведено расщепление относительно (B_i, x) и $(\overline{B}_i, x)$.

Предположим теперь, что проведено расщепление всех блоков относительно (B_i, x) и $(\overline{B}_i, x)$. Тогда для любого блока B выполняется в точности одно из приведенных выше утверждений 1) — 4) с заменой B_i на $\overline{B}_i$. Отсюда же, как и раньше, следует, что для B выполнено одно из утверждений 5) или 6) (с заменой $\overline{B}_i$ на B_i). ■

Как и в описании метода 2.5.9, будем далее рассматривать некоторый список, а именно — список P пар (B_i, x), относительно которых вообще должно проводиться расщепление. Когда согласно лемме 2.5.12 можно удалить из списка одну из нескольких пар, будем удалять пару, содержащую блок с наибольшим числом элементов. Поскольку нас не интересует точная структура списка P, будем описывать его просто как множество и использовать соответствующие теоретико-множественные операции.

Метод 2.5.13 (вариант 3 вычисления классов эквивалентности).

1. Применить метод 2.5.9.

2. Положить $P := \{(B_i, x) \mid B_i \in L, x \in X\}$.

3. До тех пор, пока не будет выполнено условие $P = \varnothing$, выполнять последовательно шаги 1)—5).

1) Выбрать из P пару (B_j, x) с минимальным значением $|B_j|$.

2) Провести расщепление множества сотояний Z (целиком) относительно пары (B_j, x).

3) Удалить (B_j, x) из P: $P := P - \{(B_j, x)\}$.

4) Произвести расщепление блоков из L относительно пары (B_j, x), используя результаты шага 2).

5) Для каждого блока B_i из L, расщепленного на шаге 4) на блоки $\underline{B}_i$ и $\overline{B}_i$ (при $\underline{B}_i \neq \varnothing$ и $\overline{B}_i \neq \varnothing$), и для каждого входа x′ из X выполнить следующее:

если пара (B_i, x') содержится в списке P, удалить ее из этого списка и ввести в него пары (B_i, x') и $(\overline{B}_i, x')$: $P := (P -$

—$\{(B_i, x')\}) \cup \{(\underline{B}_i, x')\} \cup \{(\bar{B}_i, x')\}$. В противном случае

если $|\underline{B}_i|$ меньше, чем $|\bar{B}_i|$, то ввести в P пару $(\underline{B}_i, x')$;

если же это условие не выполнено, ввести в P пару $(\bar{B}_i, x')$.

4. После выполнения этих действий в списке L будут содержаться все блоки разбиения на классы эквивалентности.

Доказательство корректности. а) *Сходимость.* Цикл «до тех пор, пока» может быть пройден только конечное число раз, потому что его выполнение прекращается, как только множество P становится пустым, а это происходит после конечного числа прохождений цикла. Действительно:

каждый раз пара, выбранная на шаге 1), удаляется из списка P на шаге 3);

число пар на шаге 5) (в списке P) возрастает только тогда, когда некоторый блок действительно расщепляется, причем для каждого такого блока в список P вводится дополнительно не более m пар;

всего возможно не более n расщеплений блоков.

б) *Правильность результата.* Покажем, что перед началом и после каждого прохождения цикла «до тех пор, пока» верны высказывания Ц1, Ц2 и Ц3, составляющие так называемый инвариант цикла:

Ц1. Блоки из списка L образуют допустимое разбиение множества состояний Z.

Ц2. Список P содержит только пары (B, x), относительно которых должно проводиться расщепление блоков из L.

Ц3. Если B — блок из L, x — вход из X и пара (B, x) не входит в список P, то для любого блока B_k из L и для любых двух состояний z и z′ из B_k выполнено условие: из $f(z, x) \in B$ вытекает, что $f(z', x) \in B$.

Если сказанное действительно верно, то результат, к которому приводит применение метода, правилен, так как из выполнения условий Ц1—Ц3 в момент, когда перестает выполняться условие «до тех пор, пока», следует, что в списке L содержатся только нерасщепляемые блоки (см. Ц2 и Ц3), образующие допустимое разбиение (Ц1). Поэтому по лемме 2.5.3 полученное разбиение действительно является разбиением на классы эквивалентных состояний.

Истинность инварианта цикла перед началом первого его выполнения вытекает из леммы 2.5.2 и из способа исходного заполнения списка L.

Истинность высказываний Ц1 и Ц2 после каждого прохождения цикла очевидна. Истинность высказывания Ц3 на шагах 1) и 2) цикла не меняется.

Допустим теперь, что высказывание Ц3 справедливо перед выполнением шага 3). После однократного выполнения шагов 3), 4) и 5) для произвольных $B \in L$ и $x \in X$ таких, что $(B, x) \notin P$, возможны тогда следующие три случая:

а) Блок B уже перед выполнением шага 4) содержался

в списке L. В этом случае истинность ЦЗ для B и x вытекает из предположения.

б) (B, x) является парой (B_j, x), выброшенной из списка P на шаге 3). Тогда истинность ЦЗ для этой пары вытекает из леммы 2.5.11, поскольку на шаге 4) все блоки из L будут расщеплены относительно этой пары.

в) (B, x) является парой, которой не было в списке L перед началом цикла [см. последний вариант шага 5)]. Тогда истинность ЦЗ для этой пары вытекает из леммы 2.5.12, поскольку по предположению перед выполнением цикла ЦЗ было справедливо для пары (B_i, x') такой, что $(B, x)=(\bar{B}_i, x')$ или $(B, x) = (B_i, x')$.

Итак, высказывание ЦЗ, а вместе с ним и инвариант цикла в целом верны после каждого выполнения цикла. ■

Опишем теперь более подробно шаги 2) и 4). На шаге 2) должны быть определены все состояния, которые удаляются из блоков при их расщеплении относительно (B_j, x). Для этого выбираются состояния z, для которых выполняется включение $f(z, x)\in B_j$, и заносятся в соответствующий список D. Итак, шаг 2) имеет вид:

2′) $D:=\varnothing$;

для каждого z' из B_j занести все z из Z такие, что $f(z, x)=z'$, в список D.

4′) Для каждого блока B из L выполнить следующее: образовать новый блок $\underline{B}$, называемый сопряженным блоком для B, и заменить блок B на разность $B-\underline{B}: \underline{B}:=B\cap \cap D$; $B:=B-\underline{B}$.

Для быстрого выполнения шага 2′) полезно заполнить таблицу, в которую для каждого z' и для каждого x занести все z такие, что $f(z, x)=z'$, т. е. построить таблицу отображения $f': Z\times X\to \mathcal{P}(Z)$, где $f'(z, x)=\{z'|f(z', x)=z\}$. Тогда шаг 2) можно записать так:

2″) $D:=\varnothing$;

для каждого z из B_j положить $D:=D\cup f'(z, x)$.

Шаг 4′) все еще недостаточно эффективен, так как на нем каждый раз должны обрабатываться все блоки из списка L. Из-за этого следует прежде всего выделить блоки, которые вообще могут расщепляться, т. е. блоки, содержащие состояния из D. Среди этих блоков нужно еще выделить такие, которые все же не будут на самом деле расщепляться, а именно блоки B, для которых выполнено условие: для всех z' из B верно $f(z', x)\in \in B_j$. Чтобы оставшиеся, т. е. действительно расщепляемые блоки, легко находить в списке L, полезно каждому блоку присвоить номер, т. е. с самого начала рассматривать L как упорядоченное множество; при этом блок с номером i обозначается B_i, как это уже делалось выше. Единичные шаги мы далее упорядочим таким образом, чтобы проходить D только один раз. Итак, получаем:

4″) Для каждого z из D выполнить следующее:
пусть i — номер блока из L, в котором лежит z.
Если для всех z′ из B_i выполнено условие $f(z', x) \subseteq B_j$, оставить все без изменений, иначе — сделать следующее:
если у блока B_i еще нет сопряженного блока $B_k = \overline{B_i}$, то организовать такой блок, положив $B_k := \varnothing$;
в любом случае перенести состояние z из B_i в B_k:
$B_i := B_i - \{z\}$; $B_k := B_k \cup \{z\}$.

Из сказанного следует, что шаги 2″) и 4″) корректны, причем метод описан так, что он легко может быть реализован, т. е. может быть написана программа на языке программирования высокого уровня. Для этого остается только выбрать подходящую *структуру данных* — прежде всего таким образом, чтобы обеспечить возможность быстрого выполнения шагов 2″), 4″) и 5):

вместе с L должна быть сформирована еще одна таблица T_L, задающая для каждого состояния z номер блока из L, содержащего это состояние;

для каждого блока B_i из L должно храниться в памяти число b_i его элементов;

для каждого выполнения шага 4″) нужна таблица номеров блоков, сопряженных с фактически расщепляемыми; эту таблицу лучше всего формировать на шаге 2″);

далее, на шаге 4″) нужна таблица T_j, определяющая для каждого блока B_i из L число состояний z′ из B_i со свойством $f(z', x) \in B_j$; изначально [на шаге 2″)] эта таблица должна заполняться нулями, а при каждом добавлении $f'(z, x)$ к D числа в таблице должны соответственно возрастать; при использовании этих таблиц (массивов данных) первый разбор случаев на шаге (4″) осуществим за постоянное время (независимо от m и n или $|Y|$);

конкретная реализация списков, таблиц и множеств (блоков) в виде структур данных существенно зависит от используемого языка программирования. Отметим только, что время, необходимое для поиска конкретного элемента, а также для записи элемента, не зависит от размера списка, таблицы или множества и может быть оценено сверху некоторой постоянной величиной.

Описанные структуры данных используются, конечно, и при реализации метода 2.5.9, в частности, там тоже нужна таблица номеров сопровождающих (сопряженных) блоков. При программировании следует иметь в виду, что переименование списков должно производиться за постоянное время.

Теперь остается провести анализ сложности метода. Легко видеть, что при его использовании необходим объем памяти $c_1mn + c_2n + c_3m + c_4$ ячеек для натуральных чисел (c_1, ..., c_4 — малые константы), если представлять состояния z_l, входы x_j и выходы y_k их индексами i, j и k. Поскольку нам нужны четыре таблицы (или списка) размера mn (для g, f, f′ и P), если записывать в P не пары (B_j, x), а пары (j, x), то $c_1 = 4$. Для L, L′, L″, L_1, T_L,

чисел элементов в блоках, D, номеров сопряженных блоков, T_j нужно по n мест в памяти (если в L, L′, L″, L_1 записывать только номера блоков). Во сколько раз константа c_2 отличается от 9, зависит от того, используется ли повторно место, которое занимают списки L′, L″ и L_1, после окончания работы метода 2.5.9 и от способов хранения блоков (все блоки некоторого разбиения содержат в совокупности n элементов). Значения констант c_3 и c_4 зависят в основном от конкретной реализации.

Теорема 2.5.14. Для реализации метода 2.5.13 необходимо не более $c_1mn+c_2n+c_3m+c_4$ ячеек памяти (c_1, ..., c_4 — константы).

Определим теперь временну́ю сложность метода. Будем, как обычно, исходить из того, что для выполнения каждой из основных операций, из которых построены все операции метода, требуется одно и то же время, не большее, чем некоторая постоянная величина, зависящая от конкретной вычислительной машины и от конкретного языка программирования. Таким образом, нам нужно только оценить сверху число необходимых операций.

Лемма 2.5.15. Пусть $|Y|=p$. Тогда время выполнения метода 2.5.9 не превышает $c_1'mnp+c_2'n+c_3'$, причем c_1', c_2' и c_3' — константы.

Доказательство. При постоянных y и x шаг 4) в цикле «до тех пор, пока» 2) выполняется не более n раз и сам цикл поэтому также выполняется не более n раз. Так как можно считать, что каждое выполнение шагов 5) и 6) требует постоянного времени, а объединение $L:=L\cup L_1$ осуществимо за время, не большее, чем $c_2'n$, то утверждение доказано. ■

Теорема 2.5.16. Время выполнения метода 2.5.13 для автомата Мили с m входами, n состояниями и p выходами не больше, чем $k_1mn\log(n)+k_2mnp+k_3mn+k_4n+k_5$, где k_1, ..., k_5 — константы.

Доказательство. Время, необходимое для первоначального заполнения списка P, не превышает k_3mn+k.

Однократное выполнение шагов 1) и 3) требует постоянного времени, скажем t_1 и t_3.

Промежуточное утверждение 1. В течение всех прохождений цикла «до тех пор, пока» порождается не более 2n различных блоков.

Доказательство. Пусть число классов 1-эквивалентности равно q_0. Будем считать, что при первом прохождении цикла расщепляется q_1 блоков, при втором — q_2 блоков, ..., при последнем r-м прохождении — q_r блоков. Тогда число блоков в конце работы составит $q_0+q_1+\ \ldots\ +q_r$. Суммарное же число порожденных блоков есть $q_0+2q_1+2q_2+\ \ldots\ +2q_r\leqslant 2(q_0+q_1+\ \ldots\ +q_r)\leqslant 2n$.

Промежуточное утверждение 1 доказано.

Из только что доказанного утверждения немедленно вытекает:

цикл «до тех пор, пока» выполняется не более 2mn раз, так как каждый порожденный в процессе работы блок B_j с некото-

рым x из X в виде пары (B_j, x) вносится в список P не более одного раза;

шаг 5) выполняется всего (при всех прохождениях цикла) не более 2n раз, так что суммарные затраты времени на выполнение этого шага могут быть оценены сверху величиной t_5mn (t_5 — константа);

суммарное время выполнения шагов 1) и 3) оценивается сверху величинами t_1mn и t_3mn.

Теперь нам остается только оценить время, необходимое для выполнения шагов 2″) и 4″).

Промежуточное утверждение 2. Для любого состояния z из множества Z и любого входа x из X в процессе реализации метода 2.5.13 не более $\log(n)+1$ раз возможна ситуация, когда на шаге 1) из списка P выбирается пара (B_j, x) такая, что $z \in B_j$.

Доказательство. Предположим сначала, что z лежит в блоке B, причем $(B, x) \in P$, и что пара (B, x) выбрана из списка P на шаге 1). Предположим далее, что на некотором следующем шаге блок B расщепляется относительно некоторой пары (B_j, x') на блоки $\underline{B}$ и $\overline{B}$. Пусть $\underline{B}$ содержит меньше элементов, чем $\overline{B}$. Тогда на шаге 5) в список P вводится только пара $(\underline{B}, x)$. Очевидно, что $|\underline{B}| \leqslant |B|/2$.

Пусть теперь $B_1, B_2, \ldots, B_r$ — все такие блоки, что $z \in B_j$ при $1 \leqslant j \leqslant r$ и при выполнении цикла «до тех пор, пока» они встречаются в выбираемых на шаге 1) парах (B_j, x), причем именно в данном порядке. Тогда верна следующая цепочка неравенств:

$$n \geqslant |B_1| \geqslant 2|B_2| \geqslant \ldots \geqslant 2^{r-1}|B_r| \geqslant 2^{r-1}.$$

Отсюда вытекает, что $r-1 \leqslant \log(n)$, т. е. число блоков не превышает $\log(n)+1$.

Промежуточное утверждение 2 доказано.

Из промежуточного утверждения 2 получаем:

1. Общее число выполнений операции объединения $D := D \cup f'(z, x)$ на шаге 2″) ограничено сверху величиной $mn\log(n)+mn$. Шаг 2″) выполняется не более 2mn раз (всякий раз, когда выполняется цикл «до тех пор, пока»). Итак, суммарное время, затрачиваемое на выполнение шага 2), ограничено сверху величиной $t_2mn\log(n)+t_2'mn$ (t_2 и t_2' — константы).

2. Общее число состояний z, вводимых при всех выполнениях шага 2″) в D и используемых далее на шаге 4″), не превышает $mn(\log(n)+1)$, поскольку на шаге 2″) при постоянном x в D вводится не более $n(\log(n)+1)$ состояний. Если t_4 — время выполнения шага 4″) при постоянном z (при использовании таблиц T_j описанным выше способом это время можно считать постоянным), то полное время, нужное для выполнения шага 4″), не превышает $t_4mn(\log n)+t_4mn$.

Суммируя сказанное, для времени выполнения метода 2.5.13 получаем верхнюю границу:

$c_1'mnp+c_2'n+c_3'$	для 2.5.9 по лемме 2.5.15,
$+k_3mn+k$	для начального заполнения P,
$+t_1mn$	для 1),
$+t_2\,mn\log(n)+t_2'mn$	для 2″),
$+t_3mn$	для 3),
$+t_4mn\log(n)+t_4mn$	для 4″),
$+t_5mn$	для 5),
$+t$	для организации и окончания цикла «до тех пор, пока»

$=(t_2+t_4)mn\log(n)+c_1'mnp+(k_3+t_1+t_2'+t_3+t_4+t_5)mn+$
$+c_2'n+c_3'+t+k.$ ■

Следствие 2.5.17. При постоянных m и p и возрастающем n время выполнения метода 2.5.13 ограничено сверху величиной $cn\log(n)$.

Доказательство. При постоянных m и p верхняя граница из 2.5.16 приобретает вид $cn\log(n)+c'n+c''=n(c\log(n)+c')+c''$. Поскольку c′ и c″ — константы, то ими можно пренебречь как слагаемыми при больших n. ■

2.6. РАЗЛИЧИМОСТЬ ВХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Допустим, что мы хотим использовать автоматы для того, чтобы некоторые сигнальные последовательности, недоступные непосредственному наблюдению, перерабатывать в понятные для нас выходные последовательности. При этом мы должны, в частности, рассмотреть вопрос: в какой степени некоторый конкретный автомат может помочь нам различать входные последовательности с помощью выходных последовательностей? В теореме 2.3.3 показано, что это возможно не всегда.

Далее будем считать, что A — автомат Мили, описанный как и раньше, обычным образом: $A=(Z, X, Y, f, g)$.

Сначала мы зададимся вопросом: при каких условиях две входные последовательности (совершенно) неразличимы?

Определение 2.6.1. Две входные последовательности v и w из $F(X)$ называются *неразличимыми автоматом* A [1], если для любого z из Z и любого u из $F(X)$ выполняется равенство $g^*(z, vu)=g^*(z, wu)$. В противном случае последовательности v и w называются *различимыми автоматом* A. Автомат A называется *различающим входы* [2], если любые две входные последовательности различимы автоматом A.

Отметим, что любые две входные последовательности различных длин всегда различимы автоматом A.

---

[1]) Или неразличимыми для автомата A. — *Прим. перев.*

[1]) Или неразличимыми для автомата A. — *Прим. перев.*

Нетрудно показать, что автоматы Мили из примеров 2.1.1 и 2.2.2 не являются автоматами, различающими входы, — для автомата из примера 2.1.1 можно рассмотреть, скажем, входные слова cdd и bcd в состоянии 6.

РАЗЛИЧАЮЩИЙ ВХОДЫ АВТОМАТ МИЛИ

Пример 2.6.2. Различающий входы автомат Мили задается графом, изображенным на рис. 2.6.1.

Лемма 2.6.3. Входные последовательности v и w тогда и только тогда неразличимы автоматом A, когда для любого состояния z автомата A состояния $f^*(z, v)$ и $f^*(z, w)$ эквивалентны и выполнено равенство $g^*(z, v) = g^*(z, w)$.

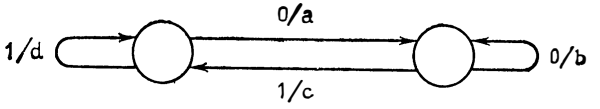


Рис 2.6.1. Различающий входы автомат Мили

Доказательство. Пусть v и w неразличимы автоматом A и z — произвольное состояние этого автомата. Тогда для всех u из F(X) выполнены равенства $g^*(z, v)g^*(f^*(z, v), u) = g^*(z, vu) = g^*(z, wu) = g^*(z, w)g^*(f^*(z, w), u)$. Отсюда вытекает, что реакции состояний $f^*(z, v)$ и $f^*(z, w)$ равны.

Обратное высказывание доказывается аналогично. ■

Следствие 2.6.4. Если последовательности v_i и w_i при $i = 1,2$ неразличимы автоматом A, то и последовательности v_1v_2 и w_1w_2 неразличимы этим автоматом.

Доказательство. а) Из леммы 2.6.3 непосредственно следует, что если v и w неразличимы и z_1 и z_2 эквивалентны, то и состояния $f^*(z_1, v)$ и $f^*(z_2, w)$ также эквивалентны.

б) Пусть z — произвольное состояние автомата A. Тогда по лемме 2.6.3 из предположения вытекает, что выполнены равенства $g^*(z, v_1v_2) = g^*(z, v_1)g^*(f^*(z, v_1), v_2) = g^*(z, w_1)g^*(f^*(z, w_1), v_2) = g^*(z, w_1) = g^*(f^*(z, w_1), w_2) = g^*(z, w_1w_2)$.

Поскольку состояния $f^*(z, v_1)$ и $f^*(z, w_1)$ эквивалентны, то из а) следует, что $f^*(z, v_1v_2) = f^*(f^*(z, v_1), v_2)$ и $f^*(z, w_1w_2)$ тоже эквивалентны. Итак, на основании леммы 2.6.3 последовательности v_1v_2 и w_1w_2 неразличимы автоматом A. ■

Дальнейшие аналогичные высказывания можно найти в упражнении 2.12.

Замечание. Из следствия 2.6.4 вытекает, что отношение неразличимости автоматом A является отношением конгруэнтности на входном моноиде F(X). Отсюда следует, что класс конгруэнтности [w] для слова $w = x_1x_2 \ldots x_k$ (где x_i — элементы X) является произведением $[x_1] \cdot [x_2] \cdot \ldots \cdot [x_k]$ классов конгруэнтности $[x_i]$ элементов x_i. Классы [x] для x из X образуют разбиение множества X. Порожденный классами [x] свободный моноид $F(\bar{X})$ — это, очевидно, фактормоноид моноида F(X) по отноше-

нию неразличимости автоматом A. Таким образом, для каждого автомата Мили A можно задать различающий входы автомат Мили A′, функционирующий, в принципе, так же, как и A, заменив в A входной алфавит X на множество $\bar{X}$ классов неразличимых входов из X. Технические детали этого построения мы опускаем.

ДЛИНА РАЗЛИЧИМЫХ ВХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Покажем теперь, что вопрос о том, является ли некоторый автомат Мили различающим входы, разрешим. Точнее говоря, мы найдем для каждого автомата Мили A число $k=k(A)$ такое, что A является различающим входы, если любые две входные последовательности длины, не большей k, оказываются различимыми автоматом A. Мы получим только верхнюю границу для числа k. Вопрос о различимости двух входных последовательностей очевидным образом разрешим на основании леммы 2.6.3 и теоремы Хаффмана — Мили.

Теорема 2.6.5. (Чен). Пусть A — автомат Мили с n состояниями. Если любые две последовательности входов длины $n^{2n}-1$ различимы автоматом A, то A — автомат, различающий входы.

Доказательство. Пусть $k=n^{2n}-1$.

а) Если все входные последовательности длины k различимы автоматом A, то и все более короткие входные последовательности различимы этим автоматом. Действительно, если бы слова v и w из F(X) такие, что $|v|=|w|=j<k$, были неразличимы автоматом A, то для всех z из Z и всех u′ из F(X) выполнялось бы равенство $g^*(z, vu')=g^*(z, wu')$. Если теперь u — некоторое слово длины k—j из F(X), то из сказанного следует, что слова vu и wu длины k были бы неразличимы автоматом A.

б) Пусть $Z=\{z_1, z_2, ..., z_n\}$. Пусть также $T=Z^{2n}$ — множество всех 2n-ок t состояний автомата A. Символом t(i) будем обозначать i-ю компоненту $t: t=(t(1), t(2), ..., t(2n))$. Положим $t_0=(z_1, z_2, ..., z_n, z_1, z_2, ..., z_n)$.

Определим теперь рекурсивно отображение

$$\bar{f}: T\times\Big(\tilde{\bigcup_{i=1}^{\infty}} X^i\times X^i\Big)\to T,$$

полагая для всех t из T, всех x и x′ из X и всех w и w′ из X^j, где $j=1, 2, ...$:

$$\bar{f}(t, x, x') = (f(t(1), x), ..., f(t(n), x), f(t(n+1), x'), ...$$

$$..., f(t(2n), x')),$$

$$\bar{f}(t, wx, w'x') = \bar{f}(\bar{f}(t, w, w'), x, x').$$

Предположение. Пусть существуют два различных слова $w=x_1 ... x_m$ и $w'=x_1' ... x_m'$, неразличимых автоматом A и таких, что все слова меньшей длины попарно различимы этим автоматом.

Из исходных допущений теоремы и из п. а) вытекает, что $m>k$. Поэтому в последовательности t_0, $t_1=\bar{f}(t_0, x_1, x_1')$, $t_2=\bar{f}(t_0, x_1x_2, x_1'x_2')$, ..., $t_m=\bar{f}(t_0, w, w')$ хотя бы один элемент t из T должен встретиться дважды (в T содержится только $k+1$ элемент). Итак, существуют индексы i и j, где $i<j\leqslant m$, такие, что $t_i=t_j$.

Пусть $w_0=x_1x_2\ldots x_{i-1}x_ix_{j+1}\ldots x_m$ и $w'_0=x'_1x'_2\ldots x'_{i-1}x'_ix'_{j+1}\ldots x'_m$.

1) Пусть $w_0\neq w_0'$, а также пусть $g^*(z_p, w)=y_{p1}y_{p2}\ldots y_{pm}$ и $g^*(z_p, w')=y'_{p1}y'_{p2}\ldots y'_{pm}$ для $p=1, \ldots, n$ (где y_{pq} и y'_{pq} — подходящие элементы множества Y).

Поскольку w и w′ неразличимы, то при $p=1, \ldots, n$ и $q=1, \ldots, m$ выполняется равенство $y_{pq}=y'_{pq}$, а при $p=1, \ldots, n$ и всех u из $F(X)$ — равенство $g^*(f^*(z_p, w), u)=g^*(f^*(z_p, w'), u)$.

Итак, при $p=1, \ldots, n$ имеем

$$g^*(z_p, w_0)=y_{p1}\ldots y_{pi-1}y_{pi}y_{pj+1}\ldots y_{pm}=y'_{p1}\ldots y'_{pi}y'_{pj+1}\ldots y'_{pm}=g^*(z_p, w'_0)$$

и, вследствие того, что $t_i=t_j$, получаем также

$$f^*(z_p, w_0)=f^*(z_p, w) \text{ и } f^*(z_p, w_0')=f^*(z_p, w').$$

В общем, для всех u из $F(X)$ и всех $p=1, \ldots, n$ справедливо равенство $g^*(z_p, w_0u)=g^*(z_p, w_0'u)$. Таким образом, в данном случае w_0 и w_0' неразличимы, но они короче, чем w, что противоречит предположению.

2) Если $w_0=w_0'$, то должно быть выполнено условие $x_{i+1}\ldots x_j\neq x'_{i+1}\ldots x'_j$ (так как $w\neq w'$). Поэтому также

$$w_1=x_1\ldots x_j\neq w_1'=x_1'\ldots x_j'.$$

Как и в случае 1), имеем

$$g^*(z_p, w_1)=g^*(z_p, w_1') \text{ и } f^*(z_p, w_1)=f^*(z_p, x_1\ldots x_i)=$$
$$=f^*(z_p, x_1'\ldots x_i')=f^*(z_p, w_1') \text{ для } p=1, \ldots, n,$$

а отсюда вытекает неразличимость слов w_1 и w_1', что снова противоречит предположению [1].

Итак, предположение ложно, т. е. любые две входные последовательности различимы автоматом A. ■

Утверждения о влиянии величины множества входов приведены в упражнениях 2.13 и 2.14.

При изучении длинных входных последовательностей часто приходится сравнивать не все выходы, но только k последних из них, и выяснять, являются ли состояния, в которые автомат переходит в конце работы, эквивалентными.

Определение 2.6.6. Пусть k — натуральное число.

---

[1] Противоречие возникает, конечно, лишь при $j<m$, но это строгое неравенство можно считать выполненным, так как последовательность $t_0, t_1, \ldots, t_m$ удовлетворяет условию: из $t_k(r)=t_k(s)$ следует $t_{k+1}(r)=t_{k+1}(s)$ при $k=1, \ldots, m-1$ и $1\leqslant r<s\leqslant n$ или $n+1\leqslant r<s\leqslant 2n$, откуда вытекает, что она не может содержать все 2n-ки из множества T. Отметим, что, используя данное соображение, нетрудно улучшить оценку $n^{2n}-1$. Читатель может сделать это в качестве дополнительного упражнения. — *Прим. перев.*

1) Для каждого слова u из $F(Y)$ определим k-*окончание* (или k-суффикс) $\eta_k(u)$ слова u следующим образом:

а) если $|u| \leqslant k$, то $\eta_k(u) = u$;

б) если $u = y_1 \ldots y_n$, где $n > k$, то $\eta_k(u) = y_{n-k+1} \ldots y_n$.

2) Две входные последовательности v и w называются k-*финально неразличимыми автоматом* A, если для всех состояний z из Z и всех слов u из $F(X)$ имеет место равенство

$$\eta_k(g^*(z, vu)) = \eta_k(g^*(z, wu)).$$

В противном случае v и w называются k-*финально различимыми автоматом* A. Автомат A называется k-*финально различающим входы,* если любые две входные последовательности являются k-финально различимыми автоматом A.

Конечно, если v и w неразличимы автоматом A, то они и k-финально неразличимы (при произвольном k). Обращение этого высказывания неверно, так как даже слова различной длины могут быть k-финально неразличимыми. Из k-финальной неразличимости вытекает j-финальная неразличимость для всех $j \leqslant k$.

Теорема 2.6.7. Пусть k — произвольное натуральное число.

1. Если две входные последовательности равной длины, не большей k, являются k-финально неразличимыми автоматом A, то они неразличимы этим автоматом.

2. Утверждения леммы 2.6.3 и следствия 2.6.4 остаются верными, если заменить термин «различимость» на «k-финальная различимость» и рассматриваемые выходные последовательности — на их k-окончания.

3. Если автомат A имеет n состояний и является $(n^{2n}-1)$-финально различающим входы, то он является автоматом, различающим входы.

Доказательство. Пункт 1 проверяется непосредственно; пункт 2 доказывается простой переформулировкой доказательств леммы и следствия; пункт 3 с помощью п. 1 немедленно получается из теоремы 2.6.5. ■

ТЕОРЕМА О ПЕРИОДИЧНОСТИ

Поставим, наконец, следующий вопрос. Пусть автомат Мили A, находящийся в состоянии z, получает на вход смешанную периодическую последовательность w_p, т. е. слово $w_j = x_1 \ldots x_j$, где $x_{m+p} = x_m$ при $m \geqslant r$; можно ли различить в этом случае последовательности w_j и w_i различной длины, если сравнивать только k последних выходов?

Теорема 2.6.8 (теорема о периодичности). Пусть z — произвольное состояние автомата A и пусть число состояний, достижимых из состояния z, равно n, т. е. пусть

$$n = |\{z' \in Z \mid z' = f^*(z, w),\ w \in F(X)\}|.$$

Пусть также $x_1, x_2, \ldots$ — произвольная смешанная периодическая последовательность входов x_i из X, т. е. такая, что существуют натуральные числа r и p, для которых при всех $m \geqslant r$ выполнено равенство $x_{m+p} = x_m$. Пусть, наконец, $w_j = x_1 x_2 \ldots x_j$ для каждого натурального числа j.

Тогда существуют натуральные числа s и q такие, что

1) $r \leqslant s \leqslant r+(n-1)p$,

2) $q \leqslant pn$,

3) $s+q \leqslant r+pn$,

и такие, что для любого i, где $i \geqslant s$, и любого k, где $k \leqslant i-s+1$, последние k выходов автомата A, начавшего работу в состоянии z и получившего на вход w_i и w_{i+q}, попарно равны, т. е. $\eta_k(g^*(z, w_i)) = \eta_k(g^*(z, w_{i+q}))$.

Доказательство. Пусть $z_1 = z$ и $z_m = f(z_{m-1}, x_{m-1})$ при $m > 1$. Рассмотрим последовательность из $pn+1$ пары (z_m, x_m) при $m = r, \ldots, r+pn$. Поскольку только n из состояний z_m могут быть различными, то по «принципу ящиков» Дедекинда должно иметься по меньшей мере $p+1$ индексов $m_1, \ldots, m_t$, где $t \geqslant p+1$ и $r \leqslant m_j \leqslant r+pn$, таких, что $z_{m_1} = z_{m_2} = \ldots = z_{m_t}$ (поскольку $pn+1$ индекс разделяется на n групп, то в каждой группе не может быть меньше, чем по $p+1$ индексу).

Далее, так как существует только p различных остатков при делении натуральных чисел на p, то среди индексов m_j найдутся по меньшей мере два, скажем m_a и m_b, которые при делении на p будут давать одинаковый остаток. Это означает, что для них будет существовать натуральное число c такое, что $m_b = m_a + cp$. Но тогда из периодичности последовательности $x_1, x_2, \ldots$ получаем, что $x_{m_a} = x_{m_b}$.

Пусть $s = m_a$ и $q = cp$. Тогда $(z_s, x_s) = (z_{s+q}, x_{s+q})$, а отсюда вытекает, что $z_{s+1} = z_{s+q+1}$, а вследствие равенства $x_{s+1} = x_{s+q+1}$ имеем $z_{s+2} = z_{s+q+2}$. В общем случае при $j \geqslant s$ получаем $(z_j, x_j) = (z_{j+q}, x_{j+q})$.

Если $k \leqslant i-s+1$, т. е. $i-k+1 \geqslant s$, то из периодичности последовательности вытекает, что

$$\eta_k(g^*(z, w_i)) = g^*(z_{i-k+1}, x_{i-k+1}, \ldots x_i) =$$
$$= g^*(z_{i-k+1+q}, x_{i-k+1+q} \ldots x_{i+q}) = \eta_k(g^*(z, w_{i+q})).$$

Наконец, из $r \leqslant m_a = s \leqslant m_a + p \leqslant m_b = s+q \leqslant r+pn$ и $q \geqslant p$ сразу получаем пп. 1), 2) и 3). ■

Следствие 2.6.9 Пусть A — автомат Мили, в котором из каждого состояния достижимы не более n различных состояний.

1. В обозначениях теоремы 2.6.8 верно следующее утверждение: любые два входных слова w_i и w_{i+q} являются k-финально неразличимыми автоматом A.

2. Автомат A порождает для входной последовательности периода p выходную последовательность периода $q \leqslant pn$.

Доказательство. Пункт 1) получаем, применяя теорему 2.6.8 к каждому состоянию автомата A; эквивалентность состояний $f^*(z, w_i)$ и $f^*(z, w_{i+q})$ вытекает из доказательства теоремы. Пункт 2 получаем, полагая в теореме 2.6.8 $k = 1$. ■

Теорема о периодичности и ее следствие являются важным вспомогательным средством для доказательства того, что некоторые задачи не могут быть решены автоматами Мили. Иначе говоря, они используются для доказательства того, что некоторые отображения из $F(X)$ в $F(Y)$ не могут быть представлены как реакции состояний автомата Мили. Например, теорема 2.2.3 очевидным образом вытекает из п. 2 следствия 2.6.9.

Из п. 1 следствия 2.6.9 в противовес примеру 2.6.2 получаем:

Следствие 2.6.10. Для каждого автомата Мили A существует бесконечно много натуральных чисел k таких, что A не является k-финально различающим входы.

Доказательство. Используя обозначения теоремы 2.6.8, выберем $k=i-s+1$ для $i=s, s+1, \ldots$ и применим п. 1 следствия 2.6.9. ■

2.7. АВТОМАТЫ МИЛИ С КОНЕЧНОЙ ПАМЯТЬЮ

По теореме 2.3.3 каждое состояние автомата Мили однозначно[1] определяется конечным набором входных слов вместе с соответствующими выходными словами. Это означает, что автомат Мили может «содержать» только конечное множество входно-выходных связей. Поэтому выход зависит только от некоторого ограниченного числа предыдущих входов. Мы увидим, однако, что здесь не существует функциональной зависимости, даже при использовании выходов в предыдущие моменты времени в качестве дополнительных аргументов.

ОПРЕДЕЛЕНИЕ, КОНТРПРИМЕР

Определение 2.7.1. Автомат Мили $A=(Z, X, Y, f, g)$ называется автоматом Мили с *конечной памятью*, если для него существуют натуральные числа p, q и отображение $h: X^{p+1} \times Y^{q} \to Y$ такие, что для всех z из Z и всех слов $w=x_1 \ldots x_k$ из $F(X)$, где $k > \max(p, q)$, выполнено равенство

$$y_k = h(x_k, x_{k-1}, \ldots, x_{k-p}, y_{k-1}, y_{k-2}, \ldots, y_{k-q})$$

[при этом считается, что $y_1 \ldots y_k = g^*(z, x_1 \ldots x_k)$].

Наименьшее число m, для которого существуют не превышающие его числа p и q [т. е. $m=\max(p, q)$], удовлетворяющие приведенному выше условию, называется *памятью* автомата Мили A.

Итак, автомат Мили имеет конечную память m, если существует функция h, с помощью которой выход автомата в любой наперед заданный момент времени k может быть определен только по входу x_k в этот момент и по входам и выходам $x_{k-1}, \ldots, x_{k-m}$ и $y_{k-1}, \ldots, y_{k-m}$ в предыдущие m моментов времени, без учета состояний самого автомата.

Теорема 2.7.2. (Гилл). 1. Существуют (конечные) автоматы Мили, не обладающие конечной памятью.

---

[1] С точностью до эквивалентности. —*Прим. перев.*

2. Пусть A — сокращенный автомат Мили с конечной памятью m и n состояниями. Тогда $m \leqslant n(n-1)/2$.

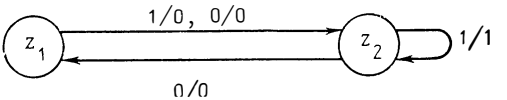


Рис. 2.7.1. Автомат Мили, не обладающий конечной памятью

Доказательство. 1. Определяемый **графом,** изображенным на рис. 2.7.1, автомат Мили не имеет конечной памяти. Для доказательства этого факта рассмотрим входные слова 0^k1, где $k=1, 2, \ldots$, и соответствующие выходные слова. Легко видеть, что при произвольных p и q и $k>\max(p, q)$ нельзя установить только на основании последних $p+1$ входов и q выходов, будет ли следующим выходом 1 или 0 (даже в том случае, когда известно, в каком состоянии автомат начал работу).

2. Для доказательства нам понадобится следующая лемма.

Лемма 2.7.3. Пусть A — сокращеный автомат Мили с конечной памятью m (см. определение 2.7.1). Тогда существует отображение h′, которое позволяет определить соответствующее состояние автомата A по последним m входам и m выходам, т. е. отображение h': $X^m \times Y^m \to Z$ такое, что для всех z из Z и всех $x_1 \ldots x_k$ из F(X) при $k \geqslant m$ выполнено равенство

$$h'(x_k, x_{k-1}, \ldots, x_{k-m+1}, y_k, y_{k-1}, \ldots, y_{k-m+1}) = f^*(z, x_1, \ldots, x_k),$$

где считается, что $y_1 \ldots y_k = g^*(z, x_1 \ldots x_k)$.

Доказательство леммы. *Предположение*: пусть доказываемое утверждение неверно, т. е. пусть существуют по меньшей мере одно входное слово $x_1 \ldots x_m$ и два различных состояния z и z′ такие, что $g^*(z, x_1 \ldots x_m) = g^*(z', x_1 \ldots x_m)$, но $z_m = f^*(z, x_1 \ldots x_m) \neq f^*(z', x_1 \ldots x_m) = z'_m$.

Поскольку автомат A — сокращенный, то состояния z_m и z'_m не эквивалентны. Поэтому существует кратчайшее слово $x_{m+1} \ldots x_{m+n}$, где $1 \leqslant n \leqslant |Z|-1$ (по теореме Хаффмана — Мили), такое, что

$$g^*(z_m, x_{m+1} \ldots x_{m+n}) \neq g^*(z'_m, x_{m+1} \ldots x_{m+n}).$$

Из сказанного вытекает, что

$$g^*(z, x_1 \ldots x_{m+n}) \neq g^*(z', x_1 \ldots x_{m+n}), \text{ но}$$

$$g^*(z, x_1 \ldots x_{m+n-1}) = g^*(z', x_1 \ldots x_{m+n-1}).$$

Из предположения об автомате A (см. определение 2.7.1) следует, однако, что должны выполняться равенства
$g^*(z, x_1 \ldots x_{m+n}) = g^*(z, x_1 \ldots x_{m+n-1})\, h(x_{m+n} \ldots x_n, y_{m+n-1} \ldots y_n) = g^*(z', x_1 \ldots x_{m+n})$.

Получено противоречие. ■

Доказательство п. 2 теоремы 2.7.2. Пусть A — сокращенный автомат Мили с конечной памятью m и n состояниями.

Из минимальности числа m вытекает, что существуют входное слово $w = x_1 \ldots x_{m-1}$ из F(X) и два различных состояния z_0 и z_0' из Z такие, что $g^*(z_0, x_1 \ldots x_{m-1}) = g^*(z_0', x_1 \ldots x_{m-1})$. Действительно,

если бы для всех $z \neq z'$ из Z и всех u из X^{m-1} было выполнено условие $g^*(z, u) \neq g^*(z', u)$, то каждое отображение $g_u : z \to Y^{m-1}$, определенное равенством $g_u(z) = g^*(z, u)$, было бы инъективным. В этом случае при любых z из Z, x из X и v из X^j, где $j \geqslant m$, можно было бы однозначно определить $g(f^*(z, v), x)$ по x и по последним m—1 входам и выходам, т. е. по $u = \eta_{m-1}(v)$ и $u' = \eta_{m-1}(g^*(z, v))$, следующим образом: $g(f^*(z, v), x) = g(f^*(g_u^{-1}(u'), u), x)$. Так что автомат A имел бы в данном случае память m—1.

Можно, далее, считать, что при $i = 1, \ldots, m-1$ выполнено условие $z_i = f^*(z_0, x_1 \ldots x_i) \neq f^*(z_0', x_1 \ldots x_i) = z_i'$. Действительно, если бы для $z \neq z'$ и произвольных u из X^{m-1} из равенства $g^*(z, u) = g^*(z', u)$ всегда следовало бы равенство $f^*(z, u) = f^*(z', u)$, то можно было бы определить частичное отображение $t: X^{m-1} \times Y^{m-1} \to Z$, где $t(u, u') = f^*(z, u)$ при $g^*(z, u) = u'$. Тогда для каждого $\bar{z}$ из Z и каждого v из X^j при $j \geqslant m$ выполнялось бы равенство $f^*(\bar{z}, v) = t(\eta_{m-1}(v), \eta_{m-1}(g^*(\bar{z}, v)))$, откуда бы следовало, что автомат A имеет память m—1.

Если мы теперь покажем, что для любой пары натуральных чисел i и j таких, что $0 \leqslant i < j < m$, множества $\{z_i, z_i'\}$ и $\{z_j, z_j'\}$ различны, то п. 2) теоремы будет доказан, поскольку число таких множеств $\{z_i, z_i'\}$ не может быть больше числа всех двухэлементных подмножеств множества состояний Z, т. е. больше $n(n-1)/2$.

Чтобы показать, что упомянутые двухэлементные множества действительно различны, предположим, что существуют i и j такие, что $\{z_i, z_i'\} = \{z_j, z_j'\}$. Поскольку всегда $z_i \neq z_i'$, нужно рассмотреть только следующие два случая.

Случай 1. $z_i = z_j$, $z_i' = z_j'$.

Тогда $f^*(z, x_1 \ldots x_i \ldots x_j x_{i+1} \ldots x_j \ldots x_{m-1}) = z_{m-1} \neq z'_{m-1} = f^*(z', x_1 \ldots x_i \ldots x_j x_{i+1} \ldots x_j \ldots x_{m-1})$, но $g^*(z, x_1 \ldots x_i \ldots x_j x_{i+1} \ldots x_j \ldots x_{m-1}) = g^*(z', x_1 \ldots x_i \ldots x_j x_{i+1} \ldots x_j \ldots x_{m-1})$, что противоречит лемме.

Случай 2. $z_i = z_j'$, $z_i' = z_j$.

Тогда (аналогично тому, что было сделано в случае 1), включая во входную последовательность слово $x_{i+1} \ldots x_j x_{i+1} \ldots x_j$, можно заставить автомат перейти из состояния z_i (или z_i') через состояние $z_j = z_i'$ (соответственно через $z_j' = z_i$ снова в состояние $z_i = z_j'$ (соответственно в $z_i' = z_j$), что опять-таки противоречит лемме. ■

Замечание. Отметим, что лемма 2.7.3 обратима, т. е. утверждение о существовании отображения h′ (вместо h) может служить определением автомата Мили с конечной памятью.

Вопрос о том, имеет ли данный автомат Мили конечную память, разрешим (см. упражнение 2.15). Оценка в теореме 2.7.2 — точная (см. упражнение 2.16). Достаточное, но не необходимое условие конечности памяти приводится в упражнении 2.17.

УПРАЖНЕНИЯ

2.1. Постройте автомат Мили $A=(Z, X, Y, f, g)$ с $X=\{0, 1\}=Y$, порождающий выход 1 тогда и только тогда, когда последние четыре входных символа равны 0101.

2.2. Постройте «генератор четности», т. е. автомат Мили с $X=Y=\{0, 1\}$, получающий на вход последовательность кодовых слов длины 3 [слов длины 3 из $F(X)$], разделенных символом 0, и порождающий на выходе эти же кодовые слова, сопровождаемые так называемым битом четности (т. е. после трех знаков кодового слова должна идти единица или ноль в зависимости от того, четное ли число символов 1 содержит данное слово).

2.3. Постройте автомат Мили, вычисляющий максимум (минимум) двух положительных целых двоичных чисел. [Указание. Добавляя при необходимости нужное число нулей перед меньшим числом, подавайте на вход автомата последовательно, начиная со старшего разряда, пары знаков сравниваемых чисел; выходом должно быть двоичное представление максимума (минимума).]

2.4. Постройте автомат, вычисляющий дополнения, т. е. автомат Мили $X=Y=\{0, 1\}$, который должен выполнять следующее:

а) для вводимого, начиная с младшего разряда в двоичной записи, натурального числа d (допускается введение дополнительных нулей после старшего разряда) автомат A в качестве выхода должен порождать двоичную запись числа 2^n-d, где n — число всех введенных цифр (включая дополнительные нули);

б) целое число (со знаком + или —) считается заданным следующим образом: неотрицательное число z — в виде $0d(z)$, где $d(z)$ — двоичная запись z (допускаются дополнительные нули), отрицательное число $-z$ (где $z>0$) — в виде $1d(2^n-z)$, причем n больше, чем число значащих цифр в $d(z)$; тогда автомат A должен порождать аналогичную запись для числа $-z$.

2.5. (Мили) 1. Для каждого натурального числа n постройте автомат Мили A, показывающий, что в теореме 2.3.3 нельзя ограничиться более короткими входными последовательностями, т. е. автомат Мили, обладающий двумя $(n-2)$-эквивалентными состояниями, не являющимися $(n-1)$-эквивалентными.

2. Для каждой пары натуральных чисел m, n постройте два автомата Мили A и A′ с m и n состояниями соответственно и с выделенными состояниями z и z′ так, что будет верно следующее: z и z′ являются $(n+m-2)$-эквивалентными, но и не эквивалентными. Отсюда следует, что и в следствии 2.3.5 нельзя ограничиться более короткими входными последовательностями.

2.6.* Сокращенный автомат Мили является «наименьшим» представителем класса всех ему эквивалентных автоматов. Можно ли определить понятие «наименьший автомат Мили» иным способом? [Указание. Назовите автомат Мили минимальным, если для него не существует эквивалентного автомата Мили с меньшим числом состояний. Покажите, что каждый минимальный автомат Мили является сокращенным и каждый сокращенный автомат Мили минимален. Покажите далее, что два эквивалентных минимальных автомата Мили равны с точностью до обозначения состояний.]

2.7.* (Рейни.) Пусть X и Y — конечные множества. Отображение $h: F(X)\to F(Y)$ называется автоматным (или конечной последовательностной словарной функцией), если существуют автомат Мили A и состояние z этого автомата такие, что h равно реакции g_z состояния z.

Покажите, что отображение $h: F(X) \to F(Y)$ является автоматным тогда и только тогда, когда выполнены следующие три условия:

1) $|h(w)| = |w|$ — для любого w из F(X) («сохранение длины»);

2) для любого u из F(X) существует отображение $h_u: F(X) \to F(Y)$ такое, что для всех v из F(X) выполнено условие $h(uv) = h(u)h_u(v)$ («секвенциальность»);

3) множество определенных в п. 2) функций h_u (так называемых состояний h) конечно.

[Указание. Для доказательства достаточности условий 1)—3) выберите состояния h в качестве состояний формируемого автомата.] Условия 1)—3) дают дополнительные возможности для доказательства того, что некоторые отображения не могут быть реакциями состояний автоматов Мили.

2.8.* (Грей, Харрисон.) Входно-выходное поведение автомата Мили может быть описано не только с помощью реакций его состояний, но и, например, следующим образом.

Преобразование, определенное автоматом Мили A (называемое также последовательностным отношением), есть множество

$$T(A) = \{(v, w) \in F(X) \times F(Y) \mid \text{существует } z \in Z \text{ такое, что } g^*(z, v) = w\}.$$

Подмножество T множества $X^* \times Y^*$ называется (Мили-)автоматным преобразованием, если существует автомат A Мили такой, что $T = T(A)$.

Покажите, что подмножество T множества $F(X) \times F(Y)$ является (Мили-) автоматным преобразованием тогда и только тогда, когда существует конечный набор автоматных отображений $h_1, \ldots, h_n$ (см. упражнение 2.7) такой, что:

1) $T = \bigcup \{gr\, h_i \mid i = 1, \ldots, n\}$;

2) для каждого x из X и каждого h_i существует h_j такое, что для каждого w из F(X) выполнено равенство $h_i(xw) = h_i(x)h_j(w)$.

Покажите далее, что если (Мили-) автоматное преобразование является графиком некоторого отображения, то последнее является автоматным, и что в то же время не каждый график автоматного отображения является (Мили-) автоматным преобразованием.

2.9. Два автомата Мили $A = (Z, X, Y, f, g)$ и $A' = (Z', X, Y, f', g')$ можно назвать слабо эквивалентными, если для каждого состояния z из Z и каждого слова w из F(X) существует z' из Z' такое, что выполнено равенство $g_z(w) = g'_{z'}(w)$, и наоборот.

Верны ли тогда следующие утверждения? Если нет — постройте контрпримеры.

1. Из эквивалентности автоматов Мили A и A′ вытекает их слабая эквивалентность.

2. Если автоматы Мили A и A′ слабо эквивалентны, то они эквивалентны.

3. Если A и A′ слабо эквивалентны, то $T(A) = T(A')$.

4. Если $T(A) = T(A')$, то A и A′ слабо эквивалентны.

2.10.* При анализе упражнений 2.1 и 2.2 возникает мысль, что при описании автомата следует рассматривать только последний выход, порождаемый им для данной входной последовательности. Это приводит к следующему варианту определения 2.3.1, п. 1): Пусть A — автомат Мили. Характером состояния z автомата A называется отображение

$$\tilde{g}_z: F(X) \to Y \cup \Lambda;$$

$\tilde{g}_z(\Lambda)=\Lambda$, $\tilde{g}_z(x)=g(z, x)$ для всех x из X;

$\tilde{g}_z(wx)=g(f^*(z, w), x)$ для всех x из X и w из F(X).

Определите понятия «характер автомата A», «характерная эквивалентность» и «характерно сокращенный» по аналогии с определением 2.3.1. Затем покажите, что теоремы 2.3.3 и 2.3.6, следствия 2.3.4 и 2.3.5 и результат упражнения 2.5 остаются справедливыми, если везде заменить термин «реакция» на термин «поведение», «эквивалентность» — на «характерная эквивалентность» и «сокращенный» — на «характерно сокращенный». Докажите далее, что два состояния и соответственно два автомата Мили эквивалентны тогда и только тогда, когда они характерно эквивалентны.

2.11. Напишите программы, реализующие методы, описанные в разд. 2.4 и 2.5, и сравните время их работы для следующих двух серий автоматов Мили A_{4n} и B_{4n}, $n=1, 2, 3, \ldots$, при больших n:

$A_{4n}=(\{1, 2, \ldots, 4n\}, \{0, 1\}, \{0, 1\}, f, g)$,

где $f(1, 0)=f(1, 1)=1$ и $f(i, 0)=i-1$ и $f(i, 1)=i$ при $2\leqslant i\leqslant 4n$;

$g(1, 0)=g(1, 1)=g(2, 0)=1$ и $g(2, 1)=g(i, 1)=g(i, 0)=0$ при $3\leqslant i\leqslant 4n$;

$B_{4n}=(\{1, 2, \ldots, 4n\}, \{0, 1\}, \{0, 1\}, f, g)$,

где $f(i, 0)=f(i, 1)=2n+2i-1$ и $f(n+i, 0)=f(n+i, 1)=2i-1$ при $1\leqslant i\leqslant n$;

$f(2n+i, 0)=f(2n+i, 1)=2i-1$ при $1\leqslant i\leqslant 2n$;

$g(n+i, 0)=g(n+i, 1)=g(2n+1, 0)=g(2n+i, 1)=1$ при $1\leqslant i\leqslant n$;

$g(i, 0)=g(i, 1)=g(3n+i, 0)=g(3n+i, 1)=0$ при $1\leqslant i\leqslant n$.

Убедитесь далее, что автоматы A_i для метода, описанного в разд. 2.4, и B_i для метода 2.5.13 представляют «наихудшие случаи».

2.12. (Гинзбург.) Пусть A — автомат Мили, описанный обычным образом, и v_1, v_2, w_1 и w_2 — входные слова автомата A.

Покажите следующее.

1. Если v_2 и w_2, а также v_1v_2 и w_1w_2 неразличимы автоматом A, то также v_1w_2 и w_1v_2 неразличимы этим автоматом, но v_1 и w_1 не обязательно неразличимы.

2. Если v_1 и w_1, а также v_1v_2 и w_1w_2 неразличимы автоматом A, то v_2 и w_2 не обязательно неразличимы. Однако если дополнительно выполнено условие: для каждого состояния z автомата A существует z′ такое, что $f^*(z', v_1)=z$ либо $f^*(z', w_1)=z$, то v_2 и w_2 неразличимы автоматом A.

2.13. * (Гинзбург.) Пусть A — автомат Мили с n состояниями и m различными выходами ($|Y|=m$).

Покажите следующее.

1. Если A имеет более чем m^n различных входов ($m^n<|X|$), то A не является автоматом, различающим входы.

2 Среди каждых $(mn)^n+1$ входов (из X) есть по меньшей мере два неразличимых автоматом A. [Указание. Сначала докажите: если k из N и $T\subseteq X$ таковы, что $(m^kn)^n<|T|^k$, то существуют два различных входных слова $x_1 \ldots x_k$ и $x'_1 \ldots x'_k$, где $x_i, x'_i\in T$ при $i=1, \ldots, k$, неразличимых автоматом A.]

2.14. (Гинзбург.) Покажите, что при каждом $m\geqslant 2$ и каждом n число входов в утверждениях упражнения 2.13 не может быть уменьшено.

2.15. (Гилл.) Придумайте метод, с помощью которого для каждого автомата Мили можно установить, имеет ли он конечную память, и если имеет,

то найдите величину памяти. [Указание. Исследуйте, какие пары состояний и при каких входах снова переходят в пары состояний.]

2.16. (Гилл.) Постройте автомат Мили с четырьмя состояниями, показывающий, что оценка в п. 2) теоремы 2.7.2 точна.

2.17. (Штуцки, Вальтер.) Говорят, что автомат Мили A обладает фундаментальным свойством, если для любых двух слов u и u′ из $F(X)$ и любых двух состояний z и z′ выполнены условия:

1) если $g^*(z, u)=g^*(z', u)$, то $g^*(z, w)=g^*(z', w)$ для всех слов w из $F(X)$ с длиной $|u|$;

2) если $g^*(z, u)=g^*(z, u')$, то $g^*(z'', u)=g^*(z'', u')$ для всех состояний z″ автомата A.

Покажите, что автомат Мили, обладающий фундаментальным свойством, имеет конечную память, но что не каждый автомат Мили, имеющий конечную память, обладает фундаментальным свойством.

ОБЗОР ЛИТЕРАТУРЫ

Описанная в этой главе модель конечных автоматов была первоначально описана в [20], см. также [1]. Пример 2.1.1 в основном соответствует работе [19]. К вопросу о реализации автоматов Мили в виде переключательных схем относятся прежде всего работы [12, 14, 31].

Теорема 2.2.3 и дальнейшие замечания о возможностях автоматов Мили взяты из [21, 18]. Идея, лежащая в основе доказательства теоремы 2.3.3, и соответствующий метод сокращения восходят к работам [15, 20]. См. в связи с этим также работы [7, 8]. Метод 2.5.13 был изначально описан в [13].

В разд. 2 5 представлен приспособленный для случая автоматов Мили метод из [11] с использованием содержащейся в той же работе идеи доказательства, принадлежащей С. Эвену.

Основные результаты разд. 2.6 и упражнения 2.12—2 14 заимствованы из [6], см также [7, 22].

Теорема 2.7.2. и дальнейшие результаты из теории автоматов Мили с конечной памятью взяты из книги [5], см. также [18].

Рассмотрение последовательностных словарных функций (упражнение 2.7) восходит к работе [23], см., например, также [26, 3, 4, 30 и 28]. По поводу упражнения 2 8 см. [10, 26 и 24].

Иные понятия эквивалентности (отличные от введенных определением 2.3.1 и в упражнениях 2.8—2.10) можно найти в [25, 16, 17, 29 и 9].

По поводу упражнения 2.17 см. работы [29, 27]. Автоматы Мили с фундаментальным свойством (определение см. в упражнении 2.17) играют важную роль в теории линейных автоматов.

Наконец, указание на возможности использования автоматов Мили в теории передачи сообщений содержится в [2].

ГЛАВА 3.

АВТОМАТЫ МУРА

3.1. ВВОДНЫЙ ПРИМЕР

В качестве вводного примера рассмотрим простейшую задачу по теории языков программирования. Для понимания этого примера от читателя требуется знакомство с использованием металингвистических «формул» в форме Бэкуса — Наура[1].

ПРОСТЕЙШИЙ АНАЛИЗАТОР СИНТАКСИСА

Пример 3.1.1. Пусть $X_D = \{0, 1, .\}$. Ниже следующие восемь металингвистических формул, обозначенных последовательно буквами m, n, ..., t, определяют подмножество множества $F(X_D)$, элементы которого могут рассматриваться как записи двоичных чисел без знака.

m : ⟨двоичное число без знака⟩ : : = ⟨целое двоичное число⟩
n : ⟨двоичное число без знака⟩ : : = ⟨двоичная дробь⟩
o : ⟨двоичное число без знака⟩ : : = ⟨целое двоичное число⟩ ⟨двоичная дробь⟩
p : ⟨двоичная дробь⟩ : : = ⟨точка⟩ ⟨целое двоичное число⟩
q : ⟨целое двоичное число⟩ : : = ⟨целое двоичное число⟩ ⟨двоичная цифра⟩
r : ⟨целое двоичное число⟩ : : = ⟨двоичная цифра⟩
s : ⟨точка⟩ : : = .
t : ⟨двоичная цифра⟩ : : = 1 | 0

Процесс, состоящий в замене металингвистических переменных, стоящих в левых частях, на соответствующие металингвистические переменные из правых частей выписанных формул, будем называть расшифровкой. Двоичное число без знака .1 получается, например, в результате расшифровки из формулы n следующим образом:

⟨двоичное число без знака⟩ : : = ⟨двоичная дробь⟩
: : = ⟨точка⟩⟨целое двоичное число⟩
: : = ⟨точка⟩⟨двоичная цифра⟩
: : = ⟨точка⟩1
: : = .1

Для описания этого процесса достаточно указать используемые формулы в порядке их применения, т. е. указать так называемую

[1] **Naur P. (ed).** Revised report on the algorithmic language ALGOL 60. — Comm. ACM, 1962, 6 : 1, p. 1—17. Перевод на русский язык: Алгоритмический язык Алгол 60. — М.: Мир, 1965. — *Прим. перев.*

последовательность расшифровки. Для .1 эта последовательность такова: n p r t s. Для, скажем, 10.011 последовательность расшифровки следующая: o p q t q t r t s q t r t.

Нашей целью будет построение «анализатора двоичных чисел без знака», т. е. автомата, работающего следующим образом.

Пусть $X=X_D \cup \{\&\}$, где & — символ, отличный от всех элементов множества X_D и используемый в качестве ограничителя. Когда автомату предлагается некоторое слово w из $F(X)$, он должен прочитывать это слово посимвольно слева направо и при прочтении каждого символа порождать на выходе символ из множества $Y=\{m, s, tr, tq, po, pn, piep, ?\}$ так, чтобы было выполнено следующее условие: если $w=u\&\&$ и u — двоичное число без знака в указанном выше смысле, то последовательность выходов (исключая последний) должна быть последовательностью расшифровки для u, записанной «справа налево»; после прочтения слова w автомат должен порождать выход «piep» до тех пор, пока на его вход не будет подано новое двоичное число без знака.

Ради полноты потребуем, чтобы автомат мог сигнализировать об ошибках (выходом «?»). Такой выход должен появляться по меньшей мере один раз, если анализируемое слово имеет вид, отличный от u&&[1]. В остальном нас не будет интересовать, как автомат реагирует на слова, не имеющие нужного вида.

Будем теперь исходить из представления о способе функционирования автоматов, несколько отличного от принятого в гл. 2. В частности, будем считать, что автомат в каждом состоянии порождает определенный выход, не зависящий от того, что автомат получает на вход.

В качестве состояний автомата будем рассматривать следующие ситуации (одновременно определяя соответствующие выходы):

z_0: начало работы (ожидание появления на входе двоичного числа): piep

z_1: прочитана только одна двоичная цифра: tr

z_2: прочитаны только двоичные цифры (по меньшей мере две): tq

z_3: прочитаны только двоичные цифры и один знак &: m

z_4: после по меньшей мере одной двоичной цифры прочитана точка: s

z_5: в состоянии z_4 прочитана двоичная цифра: tr

z_6: после того, как автомат побывал в состоянии z_4, прочитаны по меньшей мере две двоичные цифры: tq

z_7: после того, как автомат побывал в состоянии z_4, прочитаны по меньшей мере одна двоичная цифра и знак &: po

z_8: первый прочитанный знак — точка: s

---

[1] Следует отметить, что предложенный автором в качестве решения автомат не удовлетворяет в точности этому требованию (рассмотрите, например, слово &1&&1&&). — *Прим. перев.*

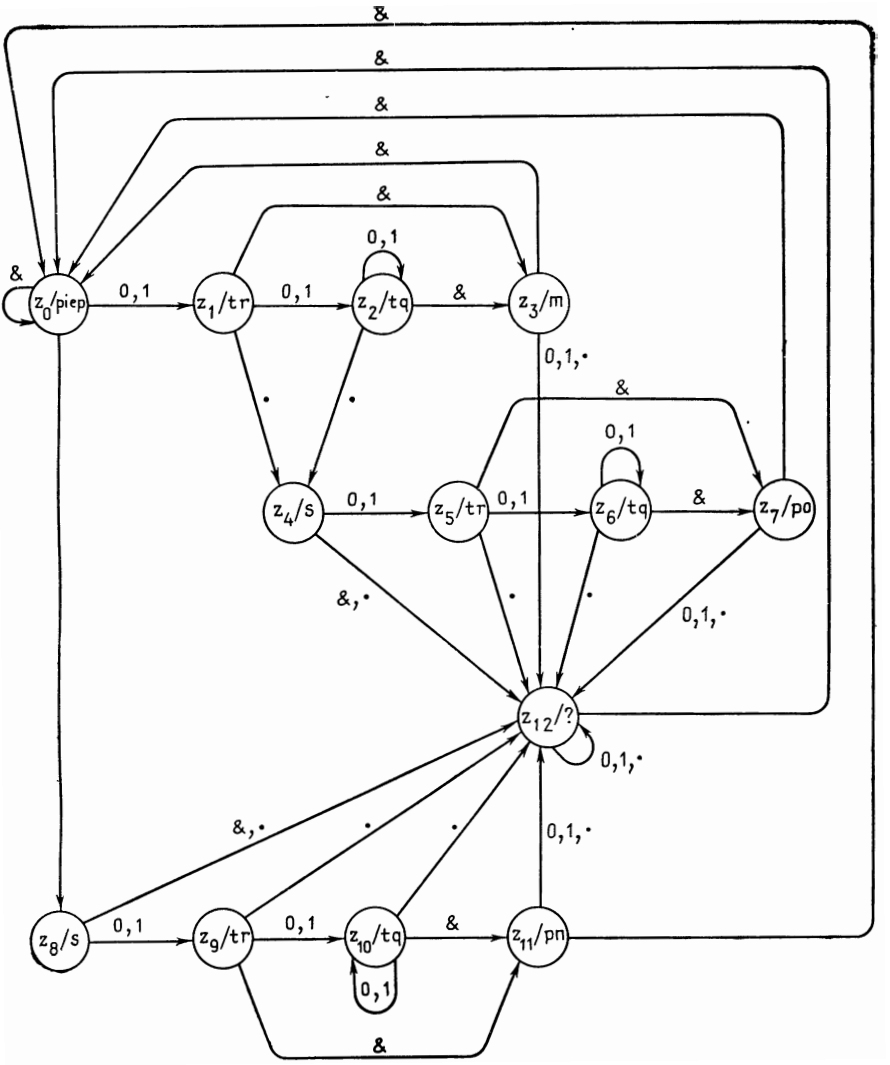


Рис. 3.1.1. Анализатор двоичных чисел без знака

z_9: в состоянии z_8 прочитана по меньшей мере одна двоичная цифра: tr

z_{10}: после того, как автомат побывал в состоянии z_8, прочитаны по меньшей мере две двоичные цифры: tq

z_{11}: в состоянии z_9 или z_{10} прочитан знак &: pn

z_{12}: состояние, в которое автомат переходит во всех остальных случаях; автомат покидает это состояние только при появлении на входе знака &: ?

Теперь ясно, как работает данный автомат. Мы опишем его

ориентированным графом, вершины которого соответствуют состояниям. Под обозначением состояний в вершинах указаны выходы, которые порождаются автоматом, находящимся в этих состояниях. Ребра графа определяют переходы автомата из одного состояния в другое под воздействием указанных входов. Этот граф изображен на рис. 3.1.1.

3.2. ОПРЕДЕЛЕНИЕ И ПЕРВОЕ СРАВНЕНИЕ С АВТОМАТАМИ МИЛИ

Автоматы описанного выше типа теперь будут формально определены, исследованы и сравнены с автоматами Мили из гл. 2.

Определение 3.2.1. (Конечный) *автомат Мура* есть пятерка $A=(Z, X, Y, f, h)$. Здесь Z, X, Y и f означают то же, что и в определении 2.2.1, а h — сюръективное отображение из Z в Y, называемое *функцией выходов*.

Замечание. Как и в случае автоматов Мили, предполагается, что множества Z, X и Y не пусты.

Ясно, что автоматы Мура (как и автоматы Мили) могут быть описаны не только ориентированными графами, но и таблицей для функций f и h или матрицей переходов и таблицей для h.

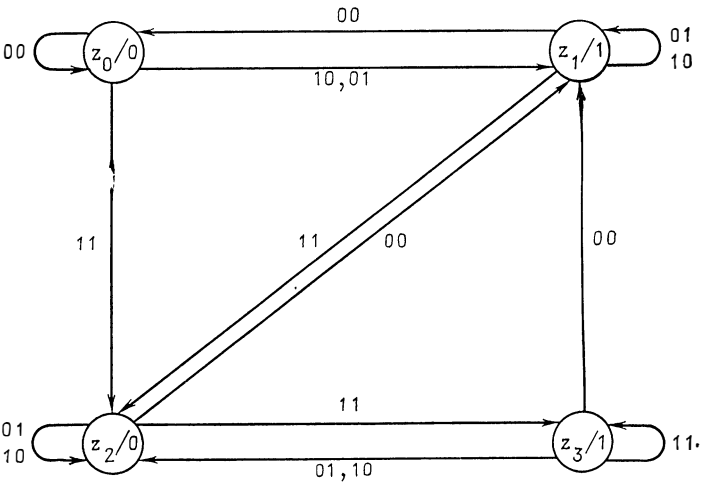


Рис. 3.2.1. Граф последовательностного сумматора

Для того чтобы сравнить определения 2.2.1 и 3.2.1, рассмотрим следующий пример.

Пример 3.2.2. Построим автомат Мура, работающий так же, как последовательностный сумматор из примера 2.2.2. Автомат имеет четыре состояния: по два для каждого из выходов 0 и 1, причем одно из таких состояний «запоминает» перенос 1 в следу-

ющий разряд, а другое — нет. Первый выход, порождаемый автоматом при начале работы, не должен, конечно, приниматься во внимание. На рис. 3.2.1 приведен граф данного автомата Мура.

ВХОДНО-НЕЗАВИСИМЫЕ АВТОМАТЫ МИЛИ

При формальном сравнении определений 2.2.1 и 3.2.1 может показаться, что автоматы Мура могут быть заданы как автоматы Мили, у которых выход не зависит от входа, т. е. как автоматы Мили, выходная функция которых удовлетворяет условию: для всех x и x′ из X и всех z из Z выполняется равенство $g(z, x) = g(z, x')$. Автоматы Мили с этим свойством будем называть *входно-независимыми.*

Представление об автоматах Мура как о входно-независимых автоматах Мили не соответствует, однако, представлению о способе функционирования автоматов Мура, использованному в примерах 3.1.3 и 3.2.2: в автоматах Мура реализуется временна́я связь между переходами из одного состояния в другое и выходами иная, нежели в автоматах Мили. У последних выход, соответствующий некоторому входу и определенному состоянию, порождается во время перехода автомата в следующее состояние. У автоматов же Мура сначала порождается выход, а потом происходит переход в следующее состояние, причем выход определяется только состоянием автомата. В частности, автомат Мура порождает некоторый выход еще перед тем, как получит первый вход — это выход, соответствующий начальному состоянию автомата (см. пример 3.1.1, состояние z_0). Конечно, этот первый выход не представляет особого интереса.

Кроме того, нетрудно заметить, что вообще не существует входно-независимого автомата Мили, работающего как последовательностный сумматор. Действительно, для автомата Мили, работающего в качестве последовательностного сумматора, из равенства $g(z, 00)=0$ при некотором состоянии z должно вытекать равенство $g(z, 01)=1$ (поскольку в состоянии z «запоминается» факт отсутствия переноса 1 в следующий разряд).

АВТОМАТЫ МИЛИ, ПРЕДСТАВИМЫЕ КАК АВТОМАТЫ МУРА

Нашему представлению о способе функционирования автоматов Мура в большей степени отвечает следующее представление о них как о частных случаях автоматов Мили: пусть A — автомат Мура (см. определение 3.2.1). Положим $g(z, x)=h(f(z, x))$ для каждого z из Z и каждого x из X. Тогда $B=(Z, X, Y, f, g)$ — автомат Мили, который для всех непустых входных последовательностей порождает такие же выходные последовательности, как и автомат A, если, конечно, не учитывать самый первый выход автомата A.

Сказанное становится ясным при анализе примеров 3.1.1 и 3.2.2. Следует отметить, что при переходе от автоматов одного ви-

да к автоматам другого вида необходимо изменение содержательных представлений, используемых при определении состояний автоматов. Так, в примере 3.2.2 состояние z_1, скажем, должно пониматься как состояние, которое автомат принимает в том случае, когда на выходе должен появиться символ 1 и отсутствует перенос в следующий разряд.

И наоборот, можно сказать, что автомат Мили $B=(Z, X, Y, f, g)$ представим как автомат Мура, если существует отображение h такое, что диаграмма на рис. 3.2.2 является коммутативной.

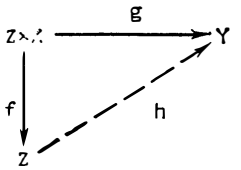
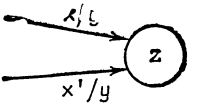


Рис. 3.2.2



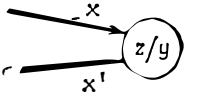


Рис. 3.2.3

Действительно, в этом случае из равенства $f(z, x)=f(z', x')$ при произвольных z и z′ из Z и произвольных x и x′ из X вытекает равенство $g(z, x)=g(z', x')$. Поэтому на всех ребрах, входящих на графе автомата B в одну вершину (состояние), должен быть указан один и тот же выход. Присоединяя этот выход к данному состоянию (рис. 3.2.3), получаем автомат Мура $A(Z, X, Y, f, h)$, который (если не учитывать его первый выход) имеет такое же входно-выходное поведение, как и автомат B.

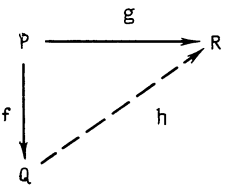


Рис. 3.2.4

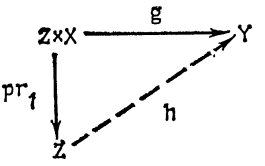


Рис. 3.2.5

Нам будет полезна следующая легко доказываемая лемма.

Лемма 3.2.3. Для отображений $f: P \to Q$ и $g: P \to R$ отображение h такое, что диаграмма на рис. 3.2.4 коммутативна, существует тогда и только тогда, когда выполняется включение

$$\{(p, p') \mid f(p)=f(p')\} \subseteq \{(p, p') \mid g(p)=g(p')\}.$$

Доказательство. Если диаграмма коммутативна, т. е. если существует отображение h, то из $f(p)=f(p')$ вытекает цепочка равенств $g(p)=h(f(p))=h(f(p'))=g(p')$.

Если, наоборот, выполняется указанное в формулировке включение, то отображение h может быть задано следующим образом:

$$h(q) = \begin{cases} g(p), \text{ если } q=f(p), \\ \text{произвольно в противном случае.} \end{cases}$$

Отображение h определено, таким образом, корректно, так как из $q=f(p)$ и $q=f(p')$ следует, что $g(p)=g(p')$. ■

На базе леммы 3.2.3 можно охарактеризовать входно-независимые автоматы Мили с помощью коммутативных треугольных диаграмм.

Следствие 3.2.4. Автомат Мили $A=(Z, X, Y, t, g)$ является входно-независимым тогда и только тогда, когда существует отображение h такое, что коммутативна диаграмма на рис. 3.2.5, где pr_1 — проекция декартова произведения на его первую компоненту.

Доказательство. По лемме 3.2.3 коммутативность диаграммы эквивалентна условию: из $z=z'$ следует $g(z, x)=g(z', x')$ для всех x и x′ из X. ■

3.3. РЕАКЦИЯ, ЭКВИВАЛЕНТНОСТЬ, СОКРАЩЕНИЕ

РЕАКЦИЯ СОСТОЯНИЙ, ЭКВИВАЛЕНТНОСТЬ И ТЕОРЕМА О СОКРАЩЕНИИ ДЛЯ АВТОМАТОВ МУРА

Чтобы иметь возможность достаточно подробно изучать соотношение между автоматами Мили и Мура, нужно описывать поведение автоматов Мура на протяжении длительных промежутков времени.

Определение 3.3.1. Пусть A — автомат Мура в обычных обозначениях и f^*: $Z \times F(X) \to Z$ — функция, заданная, как в определении 2.3.1.

Реакцией h_z *состояния* z называется отображение h_z: $F(X) \to F(Y)$, задаваемое следующим образом:

$h_z(\Lambda)=h(z)$;

$h_z(x)=h_z(\Lambda)h(f(z, x))=h(z)h(f(z, x))$ — для всех x из X;

$h_z(wx)=h_z(w)h(f(f^*(z, w), x))=h_z(w)h(f^*(z, wx))$ — для всех $w \neq \Lambda$ из F(X) и всех x из X.

Остальные понятия из определения 2.3.1 переносятся на случай автоматов Мура без изменений.

Замечание. Отметим, что пустой вход порождает непустой выход, поскольку отображение h_z определено здесь несколько иначе, чем в 2.3.1.

Интересный класс автоматов Мура описан в упражнении 3.1.

Теоремы и следствия из гл. 2 могут быть без труда доказаны для случая автоматов Мура. Например, может быть доказана следующая теорема.

Теорема 3.3.2 (теорема о сокращении). Два состояния автомата Мура с n состояниями и m выходами эквивалентны, если их

реакции на все входные последовательности длины, не большей n—m, одинаковы. Таким образом, для каждого автомата Мура может быть эффективным образом построен эквивалентный сокращенный автомат Мура.

Доказательство первой части теоремы проводится так же, как доказательство теоремы 2.3.3. Следует только отметить, что уже последовательности длины 0 порождают разбиение множества состояний на m классов 0-эквивалентных состояний (напомним, что h сюръективно). Вторая часть теоремы доказывается так же, как теорема о сокращении для автоматов Мили. Приведенная граница для необходимой длины входных последовательностей точна (см. упражнение 3.2).

ТЕОРЕМА МУРА О НЕОПРЕДЕЛЕННОСТИ

Естественным образом возникает вопрос: существует ли для каждого сокращенного автомата Мура A входная последовательность w, порождающая для всех состояний попарно различные выходные последовательности, то есть такая последовательность, что, наблюдая соответствующую выходную последовательность, можно однозначно определить состояние, в котором автомат находился перед началом работы? Ответ на этот вопрос отрицательный.

Теорема 3.3.3 (теорема Мура о неопределенности). Существует сокращенный автомат Мура $A(Z, X, Y, f, h)$ такой, что *ни для одного* слова w из $F(X)$ не выполнено условие: $h_z(w) \neq h_{z'}(w)$ для всех z и z′ из Z таких, что $z \neq z'$.

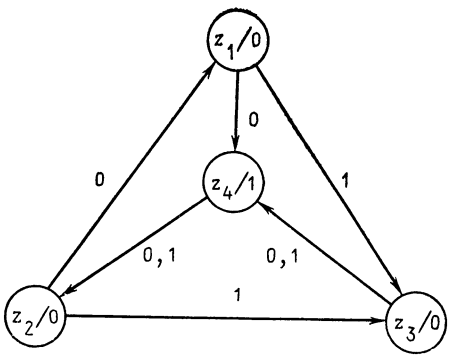


Рис. 3.3.1. Автомат Мура U

Доказательство. Автомат Мура U, граф которого приведен на рис. 3.3.1, функционирует требуемым образом.

Действительно, любое начинающееся с символа 0 слово не позволяет различить состояния z_1 и z_3 (оба эти состояния при входе 0 переходят в z_4 и порождают выход 0). Любое же начинающееся с символа 1 слово не позволяет различить состояния z_1 и z_2. Наконец, пустое входное слово не позволяет различить состояния z_1, z_2 и z_3. В то же время, автомат U — сокращенный. ■

В качестве дополнения читателю рекомендуется выполнить упражнение 3.3.

Предостережение. Доказательство теоремы 3.3.2 не допускает представления автоматов Мура как частных случаев автоматов Мили. Это становится ясным при сравнении примеров 3.2.2 и 2.2.2. Если представить автомат Мура A из примера 3.2.2 как автомат Мили B, то для B получится переходно-выходная матрица, изображенная на рис. 3.3.2.

Из этой матрицы сразу видно, что состояния z_0 и z_1 и состояния z_2 и z_3 эквивалентны в смысле определения 2.3.1 и что соответствующий сокращенный автомат B_r, получающийся в результате применения конструкции из доказательства теоремы 2.3.6, имеет граф, изображенный на рис. 2.2.1, т. е. совпадает с последовательностным сумматором из примера 2.2.2. Этот сокращенный автомат Мили не представим, очевидно, как автомат Мура (см. полученное выше условие). Автомат же Мура из примера 3.2.2 является в то же время сокращенным.

$$\begin{pmatrix} (00,0) & (01,1),(10,1) & (11,0) & \emptyset \\ (00,0) & (01,1),(10,1) & (11,0) & \emptyset \\ \emptyset & (00,1) & (01,0),(10,0) & (11,1) \\ \emptyset & (00,1) & (01,0),(10,0) & (11,1) \end{pmatrix}$$

Рис. 3.3.2. Переходно-выходная матрица последовательностного сумматора

Из вышесказанного вытекает следствие.

Следствие 3.3.4. Класс автоматов Мили, представимых как автоматы Мура, не замкнут относительно операции сокращения.

Сокращенный автомат Мура, представленный как автомат Мили, не обязательно является сокращенным.

3.4. РАВНОСИЛЬНОСТЬ АВТОМАТОВ МИЛИ И МУРА

ПОСТРОЕНИЕ АВТОМАТА МИЛИ ПО АВТОМАТУ МУРА И АВТОМАТА МУРА ПО АВТОМАТУ МИЛИ

Мы видели, что не каждый автомат Мили может быть представлен как автомат Мура. Однако оба эти понятия в определенном смысле все же равносильны.

Определение 3.4.1. Пусть $F^+(X)=F(X)-\Lambda$, т. е. пусть $F^+(X)$ — свободно порожденная множеством X полугруппа (см. гл. 1). Пусть также $A=(Z, X, Y, f, g)$ — автомат Мили и $A'=(Z', X, Y, f', h)$ — автомат Мура. Пусть, далее $\bar{g}_z$ и $\bar{h}_{z'}$ — соответственно *ограничения* (сужения) реакций g_z и $h_{z'}$ на $F^+(X)$ для каждого состояния z автомата A и соответственно для каждого состояния z′ автомата A′ [т. е. пусть $\bar{g}_z(w)=g_z(w)$ и $h_{z'}(\Lambda)\bar{h}_{z'}(w)=h_{z'}(w)$ для всех слов w из $F^+(X)$]. Тогда автоматы A и A′ называются *равносильными,* если множества их реакций, ограниченных на $F^+(X)$, совпадают, т. е. если

$$\bar{L}(A)=\{\bar{g}_z \mid z\in Z\}=\{\bar{h}_{z'} \mid z'\in Z'\}=\bar{L}(A').$$

Теорема 3.4.2. Для каждого автомата Мура A может быть построен равносильный автомат Мили B так, что B будет сокращенным, если A сокращенный.

Доказательство. Пусть $A=(Z, X, Y, f, h)$. На содержательном уровне искомый метод таков: граф равносильного автомату A автомата Мили получаем, сопоставляя каждому ребру в графе автомата A (рис. 3.4.1) ребро, изображенное на рис. 3.4.2. После этого производится соответствующее сокращение.

Определим на Z отношение R следующим образом:

zRz' тогда и только тогда, когда $f(z, x)=f(z', x)$ для всех x из X.

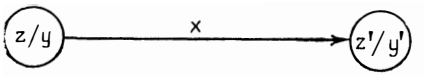


Рис. 3.4.1

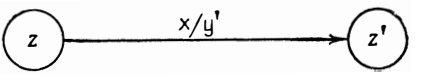


Рис. 3.4.2

R является, очевидно, отношением эквивалентности. Пусть $\bar{Z}$ — множество классов эквивалентности $[z]$ для z из Z. Тогда $B=(\bar{z}, X, Y, \bar{f}, g)$, где $\bar{f}([z], x)=[f(z, x)]$ и $g([z], x)=h(f(z, x))$ для всех z из Z и всех x из X, — автомат Мили. Действительно, отображения $\bar{f}$ и g определены корректно, поскольку для всех z' из $[z]$ выполнены равенства $[f(z', x)]=[f(z, x)]$ и $h(f(z', x))=h_z(x_1, \ldots, x_n)$,

Автоматы B и A равносильны, так как для любого z из Z и $\bar{z}=[z]$ при всех $x_1, \ldots, x_n$ из X выполняются равенства

$$g_{\bar{z}}(x_1 \ldots x_n)=$$

$$=h(f(z, x_1))h(f(f(z, x_1), x_2)) \ldots h(f^*(z, x_1 \ldots x_n))=$$

$$=h_z(x_1 \ldots x_n),$$

т. е. $\bar{g}_{\bar{z}}=\bar{h}_z$.

Допустим, что автомат B — не сокращенный. Это означает, что существуют состояния z и z' из Z такие, что $[z]\neq[z']$, но $g_{[z]}=g_{[z']}$. Очевидно, что в таком случае состояния $f(z, x)$ и $f(z', x)$ автомата A различны, но эквивалентны (как состояния автомата Мура), т. е. автомат A не сокращенный. ■

Читателю рекомендуется выполнить упражнения 3.4.

Теорема 3.4.3. Два автомата Мили, равносильных одному автомату Мура, эквивалентны.

Доказательство. Достаточно заметить, что у автомата Мили реакция g_z, полностью определяется ограничением $\bar{g}_{\bar{z}}$, поскольку всегда $g_z(\Lambda)=\Lambda$. ■

Читателю рекомендуется выполнить также первую часть упражнения 3.5.

Теорема 3.4.4. Для каждого автомата Мили $A=(Z, X, Y, f, g)$ можно задать равносильный автомат Мура B с не более чем $|Z|\cdot|Y|$ состояниями, причем сокращенный, если A — сокращенный. Автомат B будет иметь столько же состояний, сколько их

у автомата A, тогда и только тогда, когда A представим как автомат Мура, т. е. когда для всех z и z′ из Z и всех x и x′ из X из равенства f(z, x)=f(z′, x′) вытекает равенство g(z, x) = =g(z′, x′).

Доказательство. Основная идея состоит в следующем. Если автомат A не представим как автомат Мура, то следует искать способ адекватного расширения множества состояний. Это становится особенно понятным при рассмотрении ситуации в общем виде (как в лемме 3.2.3).

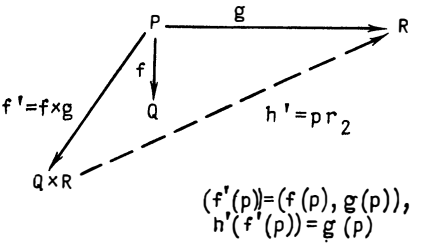


Рис. 3.4.3

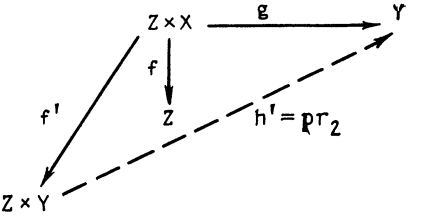


Рис. 3.4.4

Пусть заданы отображения f: P→Q и g: P→R. Если не существует отображения h (см. лемму), то переходим к следующей диаграмме (рис. 3.4.3), в которой заведомо существует соответствующее отображению h отображение h′, делающее диаграмму коммутативной.

Нетрудно заметить, что отображение h существует в том и только в том случае, когда f′(P) является графиком некоторого частичного отображения.

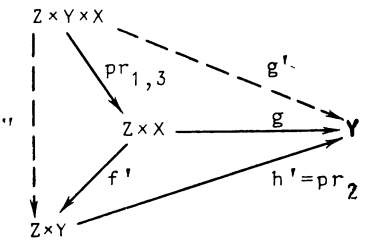


Рис. 3.4.5

В нашем частном случае имеем диаграмму, приведенную на рис. 3.4.4, т. е. новым множеством состояний оказывается множество Z×Y. Эквивалентный автомату A автомат Мили A′=(Z×Y, X, Y, f″, g′) и равносильный автомату A′ автомат Мура B′=(Z×Y, X, Y, f″, h′) получаем, определяя функции f″ и g′ так, чтобы диаграмма на рис. 3.4.5 была коммутативной.

Итак, имеем

$$f''(z, y, x)=f'(z, x)=(f(z, x), g(z, x)) \text{ и } g'(z, y, x)=g(z, x).$$

Очевидно, что для каждого z из Z все состояния (z, y) автомата Мили A′ эквивалентны между собой и эквивалентны состоянию z автомата A. Далее, каждое состояние (z, y) автомата B′ равносильно состоянию (z, y) автомата A′ [однако состояния (z, y) и (z, y′) автомата B′ при y≠y′ не эквивалентны!]. Итак,

автомат B′ равносилен автомату A и является сокращенным, если таковым является A.

Несмотря на сказанное, автомат B′ может иметь все же слишком много состояний: нам нужны только элементы из $f'(Z, X)$ и для каждого z из $Z-f(Z, X)$ — только одна пара (z, y_0). Итак, пусть y_0 — фиксированный элемент множества Y и

$$\bar{Z}=f'(Z, X)\cup\{(z, y_0)\,|\,z\in Z-f(Z, X)\}.$$

Тогда $B=(\bar{Z}, X, Y, \bar{f}, \bar{h})$ (где $\bar{f}$ и $\bar{h}$ — соответственно ограничения f'' и h' на $\bar{Z}$ — искомый автомат Мура. Остальные утверждения из формулировки теоремы вытекают из вышесказанного. ■

Замечание. Примеры 2.2.2. и 3.2.2 показывают, что в конструкции теоремы 3.4.4 нельзя обойтись менее чем $|Z|\cdot|Y|$ состояниями для автомата Мура.

В качестве дополнения читателю рекомендуется выполнить упражнения 3.5, 3.6 и 3.7 п. 1)—3).

3.5. ДАЛЬНЕЙШИЕ ПРИМЕРЫ

Пример 3.5.1. Пусть G — конечная группа. Ее элементы g и g′ называются сопряженными, если в G существует такой элемент h, что $g'=hgh^{-1}$. Нетрудно проверить, что отношение «быть сопряженными элементами» является отношением эквивалентности на G. Пусть K_G — множество классов сопряженных элементов G и $\tilde{g}$ — (однозначно определенный) класс, содержащий элемент g (для любого g из G). Легко видеть, что $\tilde{g}=\{hgh^{-1}\,|\,h\in G\}$.

Для группы G определим автомат Мура K(G) следующим образом: $K(G, G, K_G, \cdot, \sim_G)$, где $\cdot$ — умножение в G, т. е. $\cdot(g, g')=g\cdot g'$ и $\sim_G$ — отображение, сопоставляющее элементу g соответствующий ему класс $\tilde{g}$.

Автоматы K(G) используются в теории конечного быстрого преобразования Фурье.

Для наглядности рассмотрим группу S_3 всех подстановок множества {1, 2, 3} с элементами

$$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ a=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ b=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\ c=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\ d=$$

$$=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\ f=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}.$$

Как нетрудно вычислить, выполняются равенства $\tilde{e}=\{e\}$, $\tilde{a}=\{a, b\}$, $\tilde{b}=\{b, a\}$, $\tilde{c}=\{c, d, f\}$, $\tilde{d}=\{d, c, f\}$, $\tilde{f}=\{f, c, d\}$. Итак, в данном случае имеются три класса сопряженных элементов:

$k_1=\tilde{e}$, $k_2=\tilde{a}$ и $k_3=\tilde{c}$.

Автомат $K(S_3)$ может быть описан таблицей для функций переходов и выходов, представленной на рис. 3.5.1 (таблица для функции переходов является не чем иным, как таблицей умножения для группы S_3).

Вход / Состояние	e	a	b	c	d	f	Выход
e	e	a	b	c	d	f	k_1
a	a	b	e	f	c	d	k_2
b	b	e	a	d	f	c	k_2
c	c	d	f	e	a	b	k_3
d	d	f	c	b	e	a	k_3
f	f	c	d	a	b	e	k_3

Рис. 3.5.1. Функции переходов и выходов автомата $K(S_3)$

В дальнейшем мы будем сравнивать между собой структуры различных автоматов, причем также структуры автоматов, не являющихся эквивалентными, а лишь функционирующих «сходным образом». С этой целью рассмотрим прежде всего некоторые примеры.

КОНТРОЛЬ ПЕРЕПОЛНЕНИЯ ПРИ СЛОЖЕНИИ

Пример 3.5.2 (контроль переполнения при сложении). Требуется построить автомат Мура, который, просматривая последовательно два вводимых в него неотрицательных целых двоичных числа, решает вопрос: меньше ли сумма этих чисел, чем 2^n, где n — максимальная длина (число значащих цифр) рассматриваемых чисел. Выход автомата после введения в него последней значащей цифры должен быть равен 0, если данное условие вы-

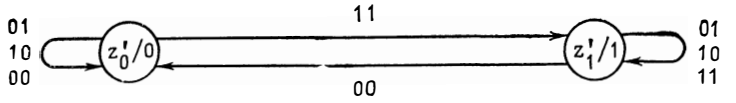


Рис. 3.5.2. Автомат Мура для контроля переполнения при сложении

полнено. Очевидно, данный автомат должен быть похож на последовательностный сумматор из примера 3.2.2. Он и может быть получен из последовательностного сумматора, если объединить состояния z_0 и z_1 в одно новое состояние z_0', состояния z_2 и z_3 — в состояние z_1' и соответствующим образом изменить функции переходов и выходов. Граф искомого автомата Мура изображен на рис. 3.5.2.

Пример 3.5.3 (тест для двоичных чисел без знака). Требуется построить автомат Мура, который для данной последовательности символов устанавливает, является ли она двоичным числом без знака в смысле примера 3.1.1 или нет. Этот автомат Мура получаем из автомата, построенного в примере 3.1.1, следующим образом.

а) Заменяем выход piep, m, s, tr, tg, po, pn на выход 1 и выход ? на выход 0.

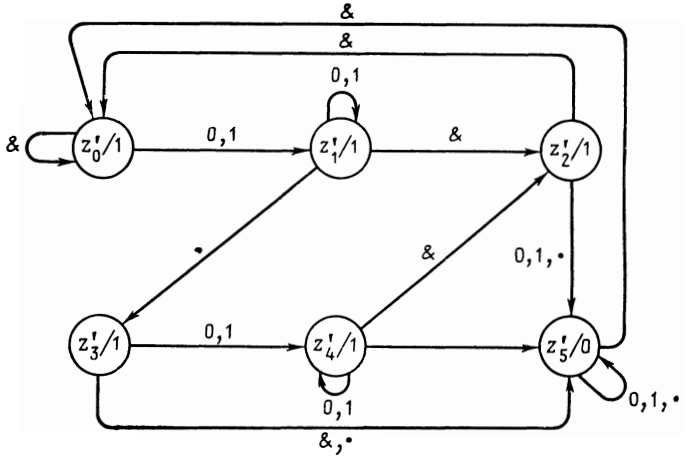


Рис. 3.5.3. Автомат Мура для проверки двоичных чисел без знака

б) Объединяем состояния z_1 и z_2 в z_1', состояния z_3, z_7 и z_{11} в z_2', состояния z_4 и z_8 в z_3' и состояния z_5, z_6, z_9 и z_{10} в z_4'.

в) Переименовываем остальные состояния: z_0 в z_0' и z_{12} в z_5'.

г) Изменяем соответствующим образом функции переходов и выходов.

Искомый автомат Мура задается графом, изображенным на рис. 3.5.3.

Пример 3.5.4. Пусть $(G, \cdot)$ и $(G', \odot)$ — две группы, причем G' является гомоморфным образом G, т. е. существует сюръективное отображение φ: $G \to G'$ такое, что для всех g и f из G выполняется равенство $\varphi(g \cdot f) = \varphi(g) \odot \varphi(f)$. Пусть, далее, K(G) и K(G′) — автоматы, сопоставленные группам G и G′ (см. пример 3.5.1). Тогда, очевидно, автомат K(G′) можно получить из автомата K(G), если в графе последнего:

1) заменить входы g на $\varphi(g)$;

2) заменить выходы k из K_G на соответствующие классы $\tilde{\varphi}(k) = \{\varphi(g) \mid g \in k\}$;

3) все состояния, имеющие один и тот же образ при отображении φ, объединить в соответствующее состояние K(G′);

4) соответствующим образом изменить функции переходов и выходов.

Итак, автомат K(G′) может быть получен из автомата K(G) только с помощью функции φ, причем требуется совместимость этой функции с функциями переходов и выходов.

3.6. ГОМОМОРФИЗМЫ И ИЗОМОРФИЗМЫ

РАЗЛИЧНЫЕ ПОНЯТИЯ ГОМОМОРФИЗМА

Последние три примера оправдывают введение следующего определения.

Определение 3.6.1. Пусть $A=(Z, X, Y, f, h)$ и $A'=(Z', X', Y', f', h')$ — два автомата Мура. Тройка отображений $\varphi=(\varphi_Z, \varphi_X, \varphi_Y)$, где φ_Z: $Z\to Z'$, φ_X: $X\to X'$ и φ_Y: $Y\to Y'$, называется *гомоморфизмом* (или, точнее, ZXY-гомоморфизмом) из A в A′, если выполнены следующие условия:

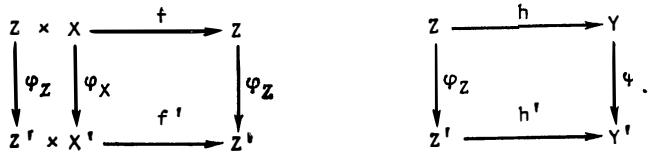


Рис. 3 6.1

1) $\varphi_Z(f(z, x))=f'(\varphi_Z(z), \varphi_X(x))$ — для всех z из Z и всех x из X;

2) $\varphi_Y(h(z))=h'(\varphi_Z(z))$ — для всех z из Z, т. е. если коммутативны обе диаграммы на рис. 3.6.1.

φ называется *гомоморфизмом из* A *на* A′ (или *эпиморфизмом*), если отображения φ_Z, φ_X и φ_Y сюръективны. A′ называется при этом гомоморфным образом A.

φ называется изоморфизмом из A на A′, если φ — гомоморфизм из A на A′ и отображения φ_Z, φ_X и φ_Y биективны. Если существует изоморфизм из A на A′, то A и A′ называются *изоморфными*.

Если одно из отображений, входящих в тройку φ, является тождественным, то оно исключается из φ. При этом гомоморфизм φ приобретает название UV-гомоморфизм, где U и V — те из множеств Z, X, Y, на которых соответствующие отображения не тождественны. То же имеем и в случае, когда тождественны два из трех отображений, входящих в φ. Так, говорят о *Z-гомоморфизме*, если $\varphi_X=\mathrm{id}_X$ и $\varphi_Y=\mathrm{id}_Y$, и о ZY-гомоморфизме, если $\varphi_X=\mathrm{id}_X$.

Гомоморфный образ автомата Мура имеет в некотором смысле сходную, но, вообще говоря, более простую структуру. Изоморфные автоматы Мура совпадают с точностью до обозначений: говорят, что они равны с точностью до изоморфизма.

Нетрудно проверить следующие *утверждения.*

1. Автомат Мура K(G′) из примера 3.5.4 является гомоморфным образом автомата K(G) при ZXY-гомоморфизме $\varphi' = (\varphi, \varphi, \widetilde{\varphi})$.

2. Автомат Мура из примера 3.5.3 является гомоморфным образом автомата Мура из примера 3.1.1 при ZY-гомоморфизме $\varphi = (\varphi_Z, \mathrm{id}_X, \varphi_Y)$, причем:

$\varphi_Z(z_0) = z_0'$;

$\varphi_Z(z_1) = z_1'$ для i=1, 2, $\varphi_Z(z_1) = z_2'$ для i=3, 7, 11;

$\varphi_Z(z_i) = z_3'$ для i=4, 8, $\varphi_Z(z_1) = z_4'$ для i=5, 6, 9, 10;

$\varphi_Z(z_{12}) = z_5'$;

$$\varphi_Z(y) = \begin{cases} 0 \text{ при } y = ? \\ 1 \text{ в противном случае.} \end{cases}$$

3. Автомат Мура из примера 3.5.2 *не является* гомоморфным образом последовательностного сумматора из примера 3.2.2, поскольку не существует отображения φ_Y, удовлетворяющего условию 2) определения 3.6.1, хотя отображения $\varphi_X = \mathrm{id}_X$ и φ_Z, где $\varphi_Z(z_0) = \varphi_Z(z_1) = z_0'$ и $\varphi_Z(z_2) = \varphi_Z(z_3) = z_1'$, и удовлетворяют условию 1) этого определения.

4. Если A — автомат Мура и $\bar{A}$ — эквивалентный автомату A сокращенный автомат Мура, то $\bar{A}$ является гомоморфным образом A при Z-гомоморфизме $\tau = \varphi_Z$, сопоставляющем каждому состоянию автомата A эквивалентное (однозначно определенное) состояние автомата $\bar{A}$.

Утверждение 4 наводит на мысль о возможности установления дальнейших связей между понятием Z-гомоморфизма и понятиями сокращения и эквивалентности.

Теорема 3.6.2. 1. Если A′ есть Z-гомоморфный образ A, то A′ эквивалентен A. Обращение этого высказывания неверно: если два автомата Мура эквивалентны, то не обязательно один из них является гомоморфным образом другого.

2. Два сокращенных автомата Мура эквивалентны тогда и только тогда, когда они Z-изоморфны.

Замечания 1. Эквивалентные сокращенные автоматы Мура практически одинаковы.

2. Для каждого автомата Мура существует единственный с точностью до изоморфизма эквивалентный сокращенный автомат Мура.

Доказательство теоремы. 1. Пусть A и A′ — автоматы Мура, заданные как в определении 3.6.1, и $\varphi = \varphi_Z$—Z-гомоморфизм из A на A′. Тогда X′=X и Y′=Y.

Покажем, что для каждого состояния z автомата A состояние $\varphi(z)$ является эквивалентным. Вследствие сюръективности φ это будет означать, что и для каждого состояния z′ автомата A′ существует эквивалентное z′ состояние z автомата A, т. е. что автоматы A и A′ эквивалентны. Эквивалентность состояний z и $\varphi(z)$ докажем полной индукцией по длине входных слов w.

Если $|w|=0$, т. е. $w=\Lambda$, то из определений 3.3.1 и 3.6.1 имеем $\varphi(f^*(z, w))=\varphi(z)=f'^*(\varphi(z), w)$ и $h_z(w)=h(z)=h'(\varphi(z))=h'_{\varphi(z)}(w)$.

Если $|w|=1$, т. е. $w=x$ для некоторого x из X, то из сказанного и из определений 3.3.1 и 3.6.1 получаем

$$\varphi(f^*(z, w))=\varphi(f(z, x))=f'(\varphi(z), x)=f'^*(\varphi(z), w);$$

$$h_z(w)=h_z(x)=h(z)h(f(z, x))=h'(\varphi(z))h'(\varphi(f(z, x)))=$$

$$=h'(\varphi(z))h'(f'(\varphi(z), x))=h'_{\varphi(z)}(x)=h'_{\varphi(z)}(w).$$

Предположение индукции: для каждого слова v длины n ($n\in\mathbf{N}$) выполняются равенства $\varphi(f^*(z, v))=f'^*(\varphi(z), v)$ и $h_z(v)=h'_{\varphi(z)}(v)$.

Пусть теперь w — слово из $F^+(X)$ длины $n+1$, т. е. $w=vx$, где $|v|=n$ и $x\in X$. Тогда из определений 3.3.1 и 3.6.1 и предположения индукции имеем

$$\varphi(f^*(z, w))=\varphi(f(f^*(z, v), x))=f'(\varphi(f^*(z, v)), x)=$$

$$=f'(f'^*(\varphi(z), v), x)=f'^*(\varphi(z), w);$$

$$h_z(w)=h_z(v)h(f^*(z, vx))=h'_{\varphi(z)}(v)h'(\varphi(f^*(z, vx)))=$$

$$=h'_{\varphi(z)}(v)h'(f'^*(\varphi(z), vx))=h'_{\varphi(z)}(vx)=h'_{\varphi(z)}(w).$$

Тем самым первая часть утверждения 1 теоремы доказана.

Вторая часть утверждения II будет доказана построением двух автоматов A и A′. Эти автоматы эквивалентны, имеют по три состояния. При этом реакции двух состояний автомата A и одного состояния автомата A′ равны отображению L_1, а реакции остальных состояний — отображению L_2. Отсюда вытекает, что любое отображение множеств состояний автоматов A и A′ друг на друга должно переводить по меньшей мере одно состояние в неэквивалентное, но из только что проведенного доказательства вытекает, что этого не должно быть, если отображение является Z-гомоморфизмом. Два таких автомата определяются графами, изображенными на рис. 3.6.2.

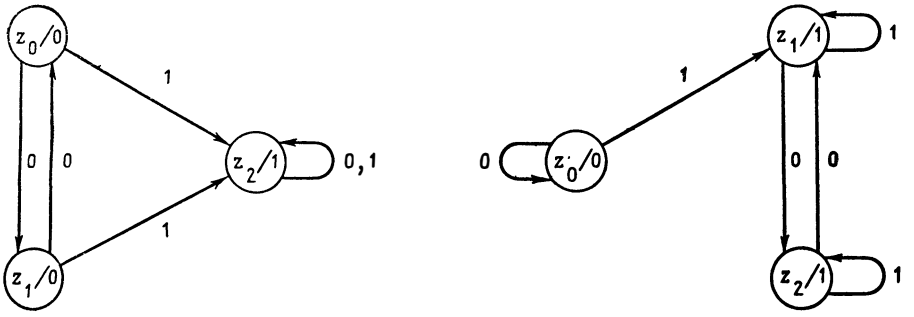


Рис. 3.6.2. Эквивалентные автоматы Мура, которые не могут быть гомоморфно отображены друг на друга

2. Пусть $A=(Z, X, Y, f, h)$ и $A'=(Z', X', Y', f', h')$ — два сокращенных автомата Мура.

Если автоматы A и A′ Z-изоморфны, то, как следует из п. 1, они эквивалентны.

Если же A и A′ эквивалентны, то множество $\{(z, z') \mid z \in Z,\ z' \in Z',\ h_z = h'_{z'}\}$ оказывается графиком биекции $\varphi: Z \to Z'$. Легко видеть, что $\varphi = \varphi_z$—Z-изоморфизм. ■

МИНИМАЛЬНЫЕ АВТОМАТЫ МУРА, ТЕОРЕМА ОБ ОДНОЗНАЧНОСТИ

Очевидно, что сокращенный автомат Мура имеет минимальное число состояний среди всех эквивалентных ему автоматов. Дадим соответствующее определение.

Определение 3.6.3. Автомат Мура A называется *минимальным,* если каждый эквивалентный ему автомат Мура имеет по меньшей мере столько же состояний, что и A.

Теорема 3.6.4 (теорема об однозначности минимального автомата Мура). Для каждого автомата Мура A существует единственный с точностью до изоморфизма эквивалентный минимальный автомат Мура A_m. Он может быть эффективно построен, является сокращенным, и каждый эквивалентный автомату A автомат Мура может быть (эффективно) Z-гомоморфно отображен на A_m. Каждый эквивалентный автомату A сокращенный автомат Мура Z-изоморфен автомату A_m.

Доказательство. Каждый минимальный автомат Мура является сокращенным, так как в противном случае для него по теореме 3.3.2 мог бы быть построен эквивалентный автомат с меньшим числом состояний. Вследствие этого и п. 2 теоремы 3.6.2 эквивалентные минимальные автоматы Мура Z-изоморфны.

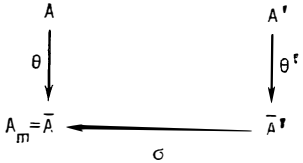


Рис. 3 6.3

Далее, каждый сокращенный автомат Мура является минимальным. Поэтому все эквивалентные некоторому автомату Мура A сокращенные или минимальные автоматы являются Z-изоморфными. Итак, чтобы получить A_m, достаточно (см. доказательство теоремы о сокращении) построить эквивалентный автомату A сокращенный автомат.

Пусть A′ — эквивалентный автомату A автомат Мура. По теореме о сокращении (теорема 3.3.2) для A′ можно построить эквивалентный сокращенный автомат Мура $\bar{A}'$. По утверждению 4 (см. с. 86) автомат $\bar{A}'$ является Z-гомоморфным образом автомата A′. Отсюда следует, что и Z-изоморфный автомату $\bar{A}'$ автомат Мура A_m оказывается Z-гомоморфным образом автомата A′, поскольку суперпозиция Z-гомоморфизмов является, очевидно, тоже Z-гомоморфизмом.

Рассматриваемая ситуация изображена на рис. 3.6.3, где θ

и θ' — определенные алгоритмом сокращения Z-гомоморфизмы, σ — существующий в силу п.2 теоремы 3.6.2 Z-изоморфизм и $\sigma\theta'$ — искомый Z-гомоморфизм A′ на A_m. ■

Дальнейшие определения и теоремы можно найти в упражнениях 3.7—3.10.

3.7. АППРОКСИМАЦИЯ ОТОБРАЖЕНИЙ

Не каждое сохраняющее длины слов отображение из $F^+(X)$ в $F^+(Y)$ может быть представлено как ограничение реакции некоторого состояния автомата Мура (это вытекает, например, из теоремы 2.2.3). Для отображения g из $X \cup X^2 \cup \ldots \cup X^n$ в $F^+(Y)$ (при $n \in \mathbf{N}$) такое представление, очевидно, возможно, если g является не только сохраняющим длину слов, но и последовательностным, т. е. если слова с одинаковым начальным отрезком u [1] отображаются в слова с одинаковым начальным отрезком g(u) (см. упражнение 2.7). Итак, для каждого сохраняющего длину слов последовательностного отображения g из $F^+(X)$ в $F^+(Y)$ и каждого натурального числа n существует автомат Мура A(g, n) с выделенным состоянием, реакция которого совпадает на $X \cup X^2 \cup \ldots \cup X^n$ с g, т. е. является аппроксимацией n-го порядка для отображения g. Возникает вопрос: сколько состояний (как минимум) должен иметь автомат A(g, n)? Иначе: как растет сложность автоматов A(g, n) с увеличением качества аппроксимации?

Определение 3.7.1. Пусть X и Y — конечные множества.

1. Отображение $g: F^+(X) \to F^+(Y)$ называется *полным,* если каждый элемент y множества Y встречается по меньшей мере в одном образе при отображении g, т. е. выполняется равенство

$Y = \{y \in Y \mid$ существуют $w \in F^+(X)$ и u, $v \in F(Y)$ такие, что $g(w) = uyv\}$.

Отображение g называется *сохраняющим длину слов,* если $|g(w)| = |w|$ для всех слов w из $F^+(X)$.

Отображение g называется *последовательностным,* если для любого u из $F^+(X)$ выполнено условие: для каждого v из $F^+(X)$ существует v′ из $F^+(Y)$ такое, что $g(uv) = g(u)v'$.

Множество всех сохраняющих длину слов последовательностных полных отображений из $F^+(X)$ в $F^+(Y)$ будет записываться как LSV(X, Y).

2. Отображение g из LSV(X, Y) называется *Mp-представимым,* если существует автомат Мура $A = (Z, X, Y, f, h)$, имеющий состояние z такое, что $\bar{h}_z = g$.

3. Пусть для каждого натурального числа n определено отношение $\overset{n}{\equiv}$ на LSV(X, Y): $g \overset{n}{\equiv} g'$ тогда и только тогда, когда для всех слов w из $F^+(X)$ длины, не большей n, выполнено ра-

[1] Т. е. слова вида uv, где $v \in F(X)$. — *Прим. перев.*

венство $g(w)=g'(w)$. Если $g \overset{n}{\equiv} g'$, то отображение g' называется *аппроксимацией n-го порядка* для отображения g.

4. Для каждого g из LSV(X, Y) отображение φ_g: $\mathbf{N} \to \mathbf{N}$ определяется следующим образом: $\varphi_g(n)$ есть минимум числа состояний по всем автоматам Мура A, удовлетворяющих условию: у A существует состояние z такое, что h является аппроксимацией n-го порядка для g.

Легко видеть, что отношение $\overset{n}{\equiv}$ при любом n является отношением эквивалентности на LSV(X, Y).

Очевидно также, что φ_g — монотонно возрастающее отображение и что $\varphi_g(n)$ с ростом n стремится к бесконечности тогда и только тогда, когда отображение g не Мр-представимо.

Нас будет интересовать скорость возрастания функций $\varphi_g(n)$ для не Мр-представимых отображений g из LSV(X, Y).

Теорема 3.7.2 (теорема Карпа об аппроксимации).

1. Пусть g — не Мр-представимое отображение из LSV(X, Y). Тогда для бесконечно многих n из **N** выполняется неравенство $\varphi_g(n) \geqslant (1/2)(n-1+|Y|)$.

2. Множитель 1/2 в п.1 не может быть заменен на больший. Константа $|Y|-1$ может быть увеличена не более чем на 2. Утверждение п. 1 становится ложным, если слова «для бесконечно многих» заменить на слова «для всех, кроме конечного числа».

Доказательство. 1. Следует показать, что для каждого достаточно большого r из **N** существует $n \in \mathbf{N}$ такое, что $n > r$ и выполнено неравенство $\varphi_g(n) \geqslant (1/2)(n-1+|Y|)$.

Поскольку отображение φ_g монотонно возрастает и не ограничено, для каждого r существует (причем единственное) n такое, что $n > r$ и $\varphi_g(r) = \varphi_g(n-1) < \varphi_g(n)$.

Пусть A и A′ — автоматы Мура соответственно с $\varphi_g(n-1)$ и $\varphi_g(n)$ состояниями и с выделенными состояниями z и z′ такими, что $\bar{h}_z \overset{n-1}{\equiv} g$ и $\bar{h}'_{z'} \overset{n}{\equiv} g$.

Так как $\varphi_g(n-1) < \varphi_g(n)$, то $\bar{h}_z \overset{n-1}{\equiv} \bar{h}'_{z'}$, но $\bar{h}_z \overset{n}{\not\equiv} \bar{h}'_{z'}$.

Допустим, что r настолько велико, что $\bar{h}_z$ является полным отображением из $F^+(X)$ в $F^+(Y)$, и положим $m = \varphi_g(n-1) + \varphi_g(n) - |Y| + 1$. Тогда $m > 0$ и $\bar{h}_z \overset{m}{\not\equiv} \bar{h}'_{z'}$, так как в противном случае для каждого x из X состояния $f(z, x)$ и $f'(z', x)$ были бы $(m-1)$-эквивалентны, а отсюда (см. теорему о сокращении 3.3.2 и следствие 2.3.5 для случая автоматов Мура) вытекало бы, что состояния $f(z, x)$ и $f'(z', x)$ эквивалентны и потому $\bar{h}_z$ и $\bar{h}'_{z'}$ равны.

Итак, имеем $\varphi_g(n-1) + \varphi_g(n) - |Y| + 1 > n-1$, т. е. $\varphi_g(n-1) + \varphi_g(n) > n-1+|Y|-1$.

Так как $\varphi_g(n-1) \leqslant \varphi_g(n)-1$, из предыдущего неравенства получаем $\varphi_g(n)-1+\varphi(n) > n-2+|Y|$, т. е. $\varphi_g(n) > (1/2)(n-1+|Y|)$.

2. Доказательство разбивается на две части, соответствующие двум частям утверждения п. 2.

Часть 1. Рассмотрим известный алгоритм проверки правильности расстановки скобок в так называемых скобочных выражениях. Ограничимся рассмотрением случая, когда используется только одна пара скобок: $X=\{[,]\}$. Скобочное выражение w, т. е. слово w из $F(X)$, называется, как известно, правильным, если последовательным удалением пар вида [,] (состоящих из открывающей и стоящей справа от нее закрывающей скобки) это выражение может быть преобразовано в пустое слово. Соответствующий алгоритм вычисляет следующее отображение:

$\hat{g}: F^+(X) \to Y$, где $Y=\{0, 1\}$; $\hat{g}(x_1x_2 \ldots x_n)=1$ при $x_1, \ldots, x_n \in X$ тогда и только тогда, когда

$$\sum_{i=1}^{k} r(x_i) \geqslant 0 \text{ для } k = 1, 2, \ldots, n \text{ и } \sum_{i=1}^{n} r(x_i) = 0,$$

где отображение $r: X \to \{-1, 1\}$ определено следующим образом:

$$r(x) = \begin{cases} -1, & \text{если } x =], \\ 1, & \text{если } x = [. \end{cases}$$

Легко видеть, что скобочное выражение $w=x_1x_2 \ldots x_n$ является правильным тогда и только тогда, когда $\hat{g}(w)=1$.

Пусть g — отображение из $F^+(X)$ в $F^+(Y)$, определенное для всех $x_1 \ldots x_n$ из $F^+(X)$ равенством $g(x_1 \ldots x_n)=\hat{g}(x_1)\hat{g}(x_1x_2) \ldots \hat{g}(x_1x_2 \ldots x_n)$.

Покажем, что

а) g не является Мр-представимым отображением;

б) $\varphi_g(m) \leqslant \frac{1}{2} m + 2$ для всех m.

Рассмотрим утверждение а). Если бы g было Мр-представимым, то для некоторого автомата Мура и некоторого состояния z этого автомата A было бы выполнено равенство $\bar{h}_z=g$. Пусть A′ (существующий по теореме 3.4.2) равносильный автомату A автомат Мили. Из теоремы о периодичности 2.6.8 вытекает, что для A′ существуют натуральные числа s и t такие, что слова $u=[^t]^t$ и $v=[^t]^{t+s}$ приводят к появлению одинаковых последних выходов, т. е. такие, что $\eta_1(\bar{h}_z(u))=\eta_1(\bar{h}_z(v))$. Отсюда на основании равенства $\bar{h}_z=g$ получаем $\hat{g}(u)=\hat{g}(v)$, что неверно, поскольку $\hat{g}(u)=1$ и $\hat{g}(v)=0$.

Рассмотрим теперь утверждение б). Покажем сначала, что $\varphi_g(2s+1) \leqslant s+2$ для каждого $s \geqslant 0$. С этой целью построим для каждого s автомат Мура $A_s = (Z, X, Y, f, h)$ такой, что

$Z = \{z_0, z_1, ..., z_{s+1}\}$

и $f(z_i, [) = z_{i+1}$ при $i = 0, 1, ..., s$;

$f(z_{s+1}, [) = z_{s+1}$;

$f(z_i,]) = z_{i-1}$ при $i = 1, 2, ..., s$;

$f(z_0,]) = f(z_{s+1},]) = z_{s+1}$;

$h(z_0) = 1$; $h(z_i) = 0$ при $i = 1, 2, ..., s+1$.

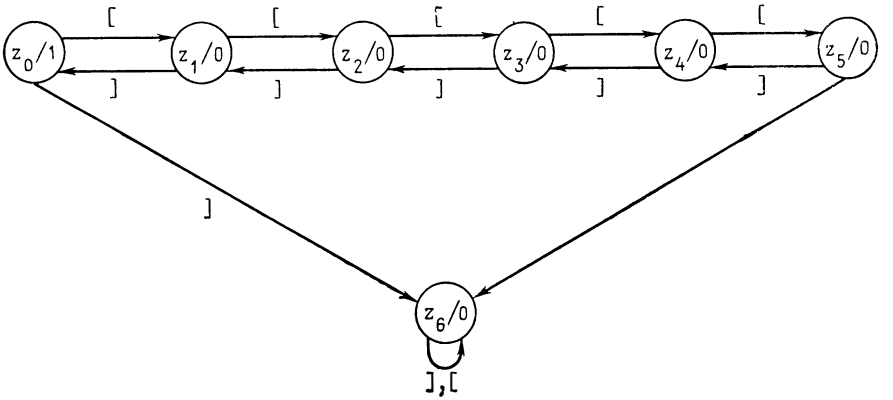


Рис. 3.7.1. Автомат Мура A_5

Граф автомата A_s при $s=5$ изображен на рис. 3.7.1.

Сразу видно, что при $n = 2s+1$ выполнено условие $\bar{h}^{n}_{z_0} \equiv g$. Итак, существует автомат Мура с $s+2$ состояниями, обеспечивающий аппроксимацию $(2s+1)$-го порядка для отображения g[1], т. е. $\varphi_g(n) \leqslant \frac{1}{2}(n+3)$.

Из $\varphi_g(n-1) \leqslant \varphi_g(n)$ вытекает теперь, что $\varphi_g(n-1) \leqslant \frac{1}{2}(n+3) = \frac{1}{2}(n-1+4)$, так что при произвольном m имеем $\varphi_g(m) \leqslant \frac{1}{2}(m+4)$, т. е. утверждение б) доказано.

Итак, для бесконечно многих m может быть выполнено лишь неравенство $\varphi_g(m) > \frac{1}{2}(m+|Y|+1)$, так что константа $|Y|-1$ в п. 1) может быть увеличена не более чем на 2.

---

[1] Т. е. автомат Мура, имеющий состояние z_0 такое, что $\bar{h}^{2s+1}_{z_0} \equiv g$. — *Прим. перев.*

Предположим теперь, что существует $b > 1/2$ такое, что $\varphi_g(n) > b(n-1+|Y|) = b(n+1)$ для бесконечно многих n. В этом случае существует и n_0 такое, что для всех $n \geqslant n_0$ выполнено $(b-1/2)n \geqslant 2-b$. Но тогда для бесконечно многих $n > n_0$ выполнено и неравенство $\varphi(n) > b(n+1) \geqslant \frac{1}{2}n + 2 = \frac{1}{2}(n+4)$, что противоречит полученной выше границе.

Часть 2. Для доказательства рассмотрим следующее отображение $\hat{g}$ из $F^+(\{a\})$ в $Y = \{0, 1\}$:

$$\hat{g}(a^r) = \begin{cases} 1, & \text{если } r = 2^{2^t} \text{ для некоторого } t \text{ из } \mathbf{N}_0, \\ 0 & \text{в противном случае.} \end{cases}$$

Пусть $g(a) = \hat{g}(a)$ и $g(wa) = g(w)\hat{g}(wa)$ для w из $F^+(\{a\})$.

Отображение $g: F^+(\{a\}) \to F^+(Y)$ не является Мр-представимым. Действительно, если бы существовал автомат Мура, представляющий g, то, как следует из теоремы о периодичности, существовали бы натуральные числа i и j такие, что a^k и a^{k+j} при каждом $k \geqslant i$ порождали бы одинаковые последние выходы, отсюда вытекало бы равенство $\hat{g}(a^k) = \hat{g}(a^{k+j})$, противоречащее определению $\hat{g}$.

Нетрудно проверить, что при каждом натуральном числе t следующий автомат Мура B_t обеспечивает аппроксимацию порядка $(2^{2^t} - 1)$ для отображения g:

$B_t = (\{z_0, z_1, \ldots, z_s\}, \{a\}, Y, f, h)$ где $s = 2^{2^t - 1} + 1$;

$f(z_i, a) = z_{i+1}$ при $i = 0, 1, \ldots, s-1$;

$f(z_s, a) = z_s$,

$h(z_r) = 1$ при $r = 2^{2^k}$ для подходящего k из $\mathbf{N}_0$ и

$h(z_r) = 0$ в остальных случаях.

Итак, $\varphi_g(2^{2^t} - 1) \leqslant 2^{2^t - 1} + 2$ при $t = 0, 1, 2, \ldots$

Если предположить, что существует m такое, что $\varphi_g(n) > \frac{1}{2} \times (n+1)$ для всех $n \geqslant m$, то получим также, что $\varphi_g(2^{2^t} - 1) > \frac{1}{2}(2^{2^t} - 1 + 1) = 2^{2^t - 1}$ для всех $t \geqslant m$.

При $t \geqslant 2$, очевидно, выполнено неравенство $2^{2^t - 1} > 2^{2^t - 1} + 2$.

Из сказанного получаем при $t \geqslant m \geqslant 2$ противоречие:

$2^{2^t - 1} + 2 < 2^{2^t - 1} < \varphi_g(2^{2^t} - 1) \leqslant 2^{2^t - 1} + 2$. ■

Дополнение к п.2) теоремы 3.7.2 содержится в упражнении 3.11.

Из частей 1 и 2 доказательства утверждения 2 теоремы 3.7.2 немедленно получаем следствие.

Следствие 3.7.3. 1. Не существует (конечного) автомата Мура (или автомата Мили) с входным алфавитом $\{[,]\}$, с помощью которого можно установить для произвольного конечного скобочного выражения w, является ли оно правильным скобочным выражением, т. е. не существует автомата, порождающего после введения слова w выход 1 тогда и только тогда, когда w — правильное скобочное выражение.

2. Не существует автомата Мура (или автомата Мили) с входным алфавитом $\{a\}$, с помощью которого можно установить, состоит ли входное слово из 2^{2^k} символов.

В общем случае вычисление значений функции φ_g для заданного отображения g является весьма сложной задачей. Следующая теорема дает точные верхнюю и нижнюю границы для φ. При этом используется обозначение $\eta_1(w)$ для последнего символа слова w (см. определение 2.6.6).

Теорема 3.7.4. Пусть g — отображение из LSV(X, Y) и n — натуральное число.

1. Пусть подмножество T множества $F^+(X)$ таково, что для любых двух различных слов x и y из T существует (вообще говоря, зависящее от x и y) слово w в $F^+(X)$ такое, что:

а) $\eta_1(g(xw)) \neq \eta_1(g(yw))$;

б) $\max(|x|, |y|) + |w| \leqslant n$,

тогда $\varphi_g(n) \geqslant |T|$.

Данная нижняя граница точна, т. е. существуют g, n и T такие, что $\varphi_g(n) = |T|$.

2. $$\varphi_g(n) \leqslant \begin{cases} (|X|^{n+1} - 1)/(|X| - 1), & \text{если } |X| \neq 1, \\ n + 1, & \text{если } |X| = 1. \end{cases}$$

Данная верхняя граница точна.

Доказательство. 1. 1) Пусть g, n, T, x, y и w удовлетворяют условиям а) и б) и пусть A — автомат Мура, имеющий состояние z такое, что $\bar{h}_z$ является аппроксимацией n-го порядка для g.

Если бы выполнялось равенство $f^*(z, xw) = f^*(z, yw) = z'$, то по условию б) мы бы имели

$$\eta_1(g(xw)) = \eta_1(\bar{h}_z(xw)) = h(z') = \eta_1(\bar{h}_z(yw)) = \eta_1(g(yw)),$$

что противоречит условию а).

Итак, $f^*(z, x) \neq f^*(z, y)$ для всех различных x и y из T, так что $|Z| \geqslant |\{f^*(z, x) \mid x \in T\}| = |T|$ и потому $\varphi_g(n) \geqslant |T|$.

2) Пусть $X = \{[,]\}$, $Y = \{0, 1\}$, g — отображение, определенное в ч. 1 доказательства п. 2 теоремы 3.7.2, n — нечетное натуральное число, $n = 2t - 1$.

Положим $T = \{[], [, [[, ..., [^t\}$, так что $|T| = t + 1$.

Пусть x и y — слова из T, причем $x \neq y$. Если $x = [\,]$ или $y = [\,]$, то положим $w = \Lambda$. Если же $x = [^i$ и $y = [^j$, то положим $w =]^m$, где $m = \min(i, j)$. В любом случае условия а) и б) будут выполнены. Итак, $\varphi_g(n) \geqslant T = t + 1 = \frac{1}{2}(n+1) + 1 = \frac{1}{2}(n+3)$.

В то же время в доказательстве п.2 теоремы 3.7.2 получена граница $\varphi_g(n) \leqslant (1/2)(n+3)$, так что $\varphi_g(n) = |T|$.

2. Для каждого отображения g из LSV(X, Y) может быть построен автомат Мура A, обеспечивающий аппроксимацию n-го порядка для g:

$$A = (\{z_0, z_1, \ldots, z_t\}, X, Y, f, h), \text{ где } X = \{x_1, \ldots, x_k\};$$

$$t = \begin{cases} n+1, & \text{если } |X| = 1, \\ 1 + |X| + |X^2| + \ldots + |X^n| = (|X|^{n+1} - \\ -1)/(|X| - 1) - \text{в противном случае;} \end{cases}$$

$$f(z_j, x_i) = \begin{cases} z_{jk+i}, \text{ если } jk + i \leqslant t, \\ \qquad\qquad\qquad\qquad \text{для } 0 \leqslant j \leqslant t,\ 1 \leqslant i \leqslant k; \\ z_j - \text{в противном случае,} \end{cases}$$

$h(z_0) = g(x_1)$, $h(z_j) = \eta_1(g(w))$ для слова w длины, не большей n, и такого, что $f^*(z_0, w) = z_j$ при $1 \leqslant j \leqslant t$.

Чтобы показать, что автомат A определен правильно, мы должны доказать, что правильно определено отображение h. Для этого нужно показать существование для каждого j, где $1 \leqslant j \leqslant t$, слова w длины, не большей n, такого, что $f^*(z_0, w) = z_j$. Поскольку t в точности совпадает с числом слов длины, не большей n, над алфавитом X, то любые такие различные слова должны переводить автомат из состояния z_0 также в различные состояния.

Итак, пусть задано j $(1 \leqslant j \leqslant t)$. Представим его в виде $j = j_p k^p + j_{p-1} k^{p-1} + \ldots + j_1 k + j_0$, где $1 \leqslant j_q \leqslant k$ при $0 \leqslant q \leqslant p$, и обозначим p через p(j). Тогда, в частности, $p(t) = n-1$. Теперь полной индукцией по p(j) докажем следующее, более сильное утверждение: существует слово w в $F^+(X)$ такое, что $|w| = p(j)+1$, $f^*(z_0, w) = z_j$ и $\bar{h}_{z_0}(w) = g(w)$. При $p(j) = 0$ в силу $j = j_0 \leqslant t$ из определения имеем: $f(z_0, x_{j_0}) = z_{j_0}$ и $\bar{h}_{z_0}(x_{j_0}) = h(z_{j_0}) = g(x_{j_0})$.

Допустим, теперь, что утверждение верно для каждого j такого, что $p(j) = m-1$, $m \geqslant 1$. Для j с $p(j) = m$ тогда справедливо равенство $j = qk + j_0$, где $q = j_m k^{m-1} + \ldots + j_2 k + j_1$, так что $p(q) = m-1$. По предположению имеется w с $|w| = p(q) + 1 = m$ такое, что $f^*(z_0, w) = z_q$ и $\bar{h}_{z_0}(w) = g(w)$. Из определения f в этом случае получаем $f^*(z_0, wx_{j_0}) = f(z_q, x_{j_0}) = z_j$. Далее, $|wx_{j_0}| = m + 1 =$

$=p(j)+1$. Из предположения индукции теперь получаем $\bar{h}_{z_0}(wx_{j_0}) = \bar{h}_{z_0}(w)\bar{h}_{z_q}(x_{j_0}) = \bar{h}_{z_0}(w)h(z_j) = g(w)\eta_1(g(wx_{j_0})) = g(wx_{j_0})$.

Итак, мы показали, что $\bar{h}_{z_0}$ является аппроксимацией n-го порядка для отображения g, так что $\varphi_g(n) \leqslant t$.

Из утверждения 1 данной теоремы следует, далее, что $\varphi_g(n) = t$, если $\eta_1(g(u)) \neq \eta_1(g(v))$ для всех $u \neq v$ из $X \cup X^2 \cup \ldots \cup X^n$. ■

Пункт 1 теоремы 3.7.4 позволяет во многих случаях доказывать, что некоторое определенное отображение не является Мр-представимым.

Следствие 3.7.5. Не существует автомата Мура с входным алфавитом X, где $|X| \geqslant 2$, и выходным алфавитом $Y = \{0, 1\}$, способного устанавливать, имеет ли входное слово вид vv, т. е. автомата Мура, представляющего отображение

$$g : F^+(X) \to F^+(Y).$$

$$\eta_1(g(w)) = \begin{cases} 1, \text{ если существует } v \text{ такое, что } w = vv; \\ 0 \text{ в противном случае.} \end{cases}$$

Доказательство. Пусть k — произвольное натуральное число и $n = 2k$. Для любых слов u и v из X^k, где $u \neq v$, тогда имеем $\eta_1(g(uv) = 0$ и $\eta_1(g(vv)) = 1$. Из п.1 теоремы 3.7.4 получаем в этом случае $\varphi_g(n) \geqslant |X|^k$.

Предположим, что существует автомат Мура A, представляющий g и имеющий t состояний. Тогда $\varphi_g(n) \leqslant t$ для всех натуральных чисел n.

Пусть из **N** выбрано k такое, что $t < |X|^k$. Тогда из сказанного выше получаем противоречие:

$$t < |X|^k \leqslant \varphi_g(2k) \leqslant t. \blacksquare$$

Другие приложения теорем 3.7.2 и 3.7.4 содержатся в упражнениях 3.12 и 3.13.

3.8. ЭКСПЕРИМЕНТЫ

ИГРА «МЫСЛИТЕЛЬ» КАК ДИАГНОСТИЧЕСКИЙ ЭКСПЕРИМЕНТ

Настольная игра «Мыслитель» может быть описана на языке автоматов Мура как диагностический эксперимент для соответствующего автомата S. В этом эксперименте должно быть определено состояние, в котором S находится перед его началом, причем известны правила функционирования автомата, т. е. его формальное описание в виде $S = (Z, X, Y, f, h)$ или эквивалентное представление S графом или таблицей, и можно задавать автомату S входы и наблюдать соответствующие выходы.

Описание автомата-«мыслителя» S начинается с задания множества цветов $F = \{$зеленый, желтый, красный, оранжевый, голу-

бой, синий}. Входами для S являются четверки $x=(f_1, f_2, f_3, f_4)$, где f_i — цвета из F при $i=1,...,4$, причем допускается, что $f_i=f_j$ при $i\neq j$. Состояниями автомата S являются четверки пар $z=((\varphi_1, \varphi_1'), (\varphi_2, \varphi_2'), (\varphi_3, \varphi_3'), (\varphi_4, \varphi_4'))$, где φ_i и φ_i' — цвета из F при $i=1,...,4$. Выходом в любом таком состоянии z является пара целых чисел (s, w), где s — число пар (φ_i, φ_i') с $\varphi_i=\varphi_i'$ в z, а w — число индексов j из множества $\{1,...,4\}$ таких, что $\varphi_j\neq\varphi_j'$, но существует индекс k из $\{1,...,4\}$ такой, что $\varphi_k\neq\varphi_k'$ и $\varphi_j=\varphi_k'$. При входе (f_1, f_2, f_3, f_4) автомат S переходит из состояния z в состояние $((\varphi_1, f_1), (\varphi_2, f_2), (\varphi_3, f_3), (\varphi_4, f_4))$.

В начале игры один из игроков выбирает некоторое начальное состояние автомата, оставляя свой выбор в тайне от другого игрока. При этом в качестве начального разрешается выбирать только состояния с $\varphi_i=\varphi_i'$ при $i=1,...,4$, т. е. состояния с выходом (4, 0).

Другой игрок задает один за другим входы, пытаясь получить на выходе (4, 0), а первый игрок производит изменения состояний автомата (в уме) и сообщает второму выходы.

Ситуации, подобные ситуациям в «Мыслителе», часто встречаются на практике. Скажем, на экзаменах (в школе, институте), в медицинской диагностике, при экспериментировании в естественных науках, при проверке технических устройств (например, компьютерная диагностика технического состояния автомобилей), при отладке программ.

КЛАССИФИКАЦИЯ ЭКСПЕРИМЕНТОВ

Будем исходить из того, что имеется некий реальный автомат, для которого известно его формальное описание. Этот автомат может воспринимать входы и порождать соответствующие выходы. Автомат должен быть исследован экспериментатором, который может наблюдать только его входно-выходное поведение.

Можно рассматривать следующие различные типы экспериментов.

1а) **Многократные эксперименты,** где используется набор идентичных копий одного автомата (прибора), с которыми можно одновременно проводить ряд экспериментов.

1б) **Однократные эксперименты,** в которых данный автомат используется только один раз.

2а) **Адаптивные эксперименты,** в которых экспериментатор может выбирать следующий вход в зависимости от предыстории, т. е. от ранее полученных в процессе работы результатов.

2б) **Автономные эксперименты,** в которых входная последовательность должна быть определена перед началом эксперимента, и только после окончания работы автомата может быть проанализирована вся полученная выходная последовательность.

3а) **Диагностические эксперименты по определению начального состояния,** целью которых является определение состояния автомата перед началом эксперимента.

3б) **Диагностические эксперименты по определению финального состояния,** целью которых является определение состояния автомата после окончания эксперимента.

4а) **Синхронизирующие эксперименты,** целью которых является перевод автомата в некоторое определенное состояние независимо от (неизвестного) начального состояния.

4б) **Эксперименты по проверке состояний,** в ходе которых автомат независимо от начального состояния должен побывать по меньшей мере по одному разу в каждом из состояний.

4в) **Эксперименты по проверке переходов,** в ходе которых автомат независимо от начального состояния должен по меньшей мере по одному разу совершить каждый возможный переход из состояния в состояние (пройти каждую стрелку на графе).

5) **Эксперименты с дополнительной информацией** — в частности, часто вместе с формальным описанием автомата задается, что рассматриваемый автомат Мура в начале эксперимента находится в одном (неизвестном) состоянии из фиксированного (известного) подмножества всех состояний.

Следующим классом экспериментов является класс так называемых **экспериментов по идентификации автоматов.** В этом случае задается некоторое множество формальных описаний (пятерок, графов или таблиц) автоматов Мура и множество реальных устройств, о которых известно, что их описания принадлежат заданному множеству. Экспериментатор должен идентифицировать данные реальные устройства («черные ящики»), т. е. найти их формальные описания. Здесь также встречаются эксперименты типов 1) и 2).

Пример 3.8.1. 1) Игра «Мыслитель» состоит в однократном диагностическом адаптивном эксперименте по определению начального состояния.

2) Из теоремы Мура о неопределенности (теорема 3.3.3) следует, что не существует автономного диагностического эксперимента по определению начального состояния для произвольного сокращенного автомата Мура. В упражнении 3.3 утверждается, что такой эксперимент существует для любого автомата Мура, имеющегося не более трех состояний. Из доказательства теоремы 3.3.3 следует, что для автомата Мура, граф которого изображен на рис. 3.3.1, не существует даже адаптивного диагностического эксперимента по определению начального состояния.

В то же время финальное состояние автомата Мура из доказательства теоремы 3.3.3 может быть легко определено с помощью адаптивного диагностического эксперимента. Действительно, если первый выход автомата (при пустом входе) равен 1, то уже известно, что финальное состояние есть z_4. В противном случае подаем на вход 0. Если после этого получен выход 0, то финальное состояние — z_1, если выход равен 1, то финальное состояние — z_4. Из сказанного следует, что рассматриваемый автомат может быть адаптивно синхронизирован, поскольку каждое его состояние достижимо из любого другого.

3) Для последовательностного сумматора из примера 3.2.2 каждый вход (каждая пара цифр 0 и 1) порождает автономный диагностический эксперимент по определению начального состояния.

4) Для автоматов Мура справедливо утверждение, аналогичное лемме 2.7.3. Отсюда вытекает, что для сокращенного автомата Мура с конечной памятью всегда существует автономный диагностический эксперимент по определению финального состояния — из п.2) теоремы 2.7.2 следует, что уже слово длины $\frac{1}{2}|Z|(|Z|-1)$ порождает такой эксперимент. В то же время получающийся из автомата Мили, не обладающего конечной памятью (см. рис. 2.7.1), автомат Мура $A=(\{1, 2, 3\}, \{0, 1\}, \{0, 1\}, f, h)$, где $f(1, 0)=f(1, 1)=2$, $f(2, 0)=f(3, 0)=1$ и $f(2, 1)=f(3, 1)=3$, а $h(1)=h(2)=0$ и $h(3)=1$, является автоматом, для которого существует не только автономный диагностический эксперимент по определению финального состояния, но даже и автономный синхронизирующий эксперимент: вход 11 переводит каждое состояние в состояние 3.

ПРОБЛЕМЫ СУЩЕСТВОВАНИЯ, СЛОЖНОСТИ И ПОСТРОЕНИЯ

В связи со сказанным возникают по меньшей мере три проблемы.

Проблема существования: существуют ли для автоматов из некоторого класса эксперименты определенного типа?

Проблема сложности: если эксперимент существует, то какой максимальной длины входные последовательности могут потребоваться и какую минимальную длину должны они иметь?

Проблема построения: как можно регулярным образом проводить требуемые эксперименты?

Для большинства возможных постановок задач только что сформулированные проблемы неразрешимы. В разд. 3.9 и следующих главах будут рассматриваться только некоторые из таких постановок и будут решены только некоторые из проблем.

Приведем теперь некоторые простые утверждения, сокращающие многообразие возможных постановок.

Утверждение 3.8.2. 1. Каждый автономный эксперимент является также и адаптивным экспериментом, так что для проведения адаптивных экспериментов не могут требоваться входные последовательности, более длинные, чем для проведения автономных экспериментов.

2. Каждый диагностический эксперимент по определению начального состояния является также и диагностическим экспериментом по определению финального состояния. Действительно, если известны начальное состояние z и входное слово w, использованное для эксперимента, то нужно лишь вычислить состояние $f^*(z, w)$.

3. Для автомата Мура, у которого ни один вход не объединяет состояния, т. е. у которого $f(z, x) \neq f(z', x)$ при $z \neq z'$ и любом x из X, каждый диагностический эксперимент по определению финального состояния является также и диагностическим экспериментом по определению начального состояния. Действительно, в данном случае для каждого состояния z и любого входного слова w существует не более одного состояния z′ такого, что $f^*(z', w) = z$.

4. При синхронизирующем эксперименте определяется и финальное состояние.

5. Каждый сокращенный автомат Мура обладает (как следует из теоремы о сокращении 3.3.2) адаптивным диагностическим многократным экспериментом по определению начального состояния. Опишем его.

Если рассматриваемый автомат A имеет n состояний, то для эксперимента понадобится не более n—1 копии A (все копии должны иметь, конечно, одно начальное состояние).

Выберем два состояния z и z′ автомата A. По теореме 3.3.2 существует входное слово w длины не большей, чем $n-|Y|$, различающее состояния z и z′, т. е. такое, что $g^*(z, w) \neq g^*(z', w)$. Введем это слово в одну из имеющихся копий автомата A. При этом реализуется одна из трех возможностей.

1) Выход равен $g^*(z, w)$. Вывод: исходным состоянием было не z′.

2) Выход равен $g^*(z', w)$. Вывод: исходным состоянием было не z.

3) Выход не равен ни $g^*(z, w)$, ни $g^*(z', w)$. Вывод: ни z, ни z′ не были начальным состоянием A.

После проведения описанной части эксперимента известно, что начальное состояния A принадлежит (n—1)-элементному (в худшем случае) подмножеству множества состояний. Теперь можно выбрать следующие два состояния (из множества потенциально возможных начальных состояний), соответствующее (различающее эти слова) входное слово и повторить описанный шаг. После не более чем n—1 шага останется только одно потенциально возможное начальное состояние, которое и является искомым.

В качестве дополнения читателю рекомендуется выполнить упражнение 3.14, п. 1).

6. Из предыдущего вытекает, что каждый сокращенный автомат Мура A с n состояниями имеет диагностический автономный многократный эксперимент по определению начального состояния, для которого требуется C_n^2 [1)] копий рассматриваемого автомата: для каждого двухэлементного подмножества $\{z, z'\}$ множества состояний автомата A выбираем различающее эти состояния входное слово, используем одну копию данного автомата и действуем далее, как и выше.

[1)] C_n^2 — число сочетаний из n по 2. — *Прим. перев.*

Для лучшего понимания рекомендуется выполнить упражнение 3.14, п. 2).

7. Для автомата Мура, не являющегося сокращенным, не существует диагностического эксперимента по определению начального состояния.

8. Сильно связный автомат Мура (см. упражнение 3.9), обладающий диагностическим экспериментом по определению финального состояния, всегда обладает адаптивным синхронизирующим экспериментом, адаптивным экспериментом по проверке состояний и адаптивным экспериментом по проверке переходов. Действительно, если автомат требуется перевести в некоторое состояние z, то при известном финальном состоянии z′, полученном в результате исходного эксперимента, для этого достаточно использовать существующее вследствие сильной связности входное слово w такое, что $f^*(z', w)=z$. Остальное очевидно.

9. Для того чтобы автомат Мура имел адаптивный эксперимент по проверке состояний (или адаптивный эксперимент по проверке переходов), необходимо, чтобы он был сильно связным, так как в процессе такого эксперимента автомат должен быть последовательно переведен из произвольного начального состояния во все состояния.

3.9. ОДНОКРАТНЫЕ АВТОНОМНЫЕ ДИАГНОСТИЧЕСКИЕ ЭКСПЕРИМЕНТЫ С ДОПОЛНИТЕЛЬНОЙ ИНФОРМАЦИЕЙ

ПРОБЛЕМЫ СУЩЕСТВОВАНИЯ, СЛОЖНОСТИ И ПОСТРОЕНИЯ ДЛЯ ЭКСПЕРИМЕНТОВ ПО ОПРЕДЕЛЕНИЮ НАЧАЛЬНОГО ИЛИ КОНЕЧНОГО СОСТОЯНИЯ

Мы будем рассматривать только однократные диагностические эксперименты с дополнительной информацией о состояниях. Везде в данном разделе A — автомат Мура с n состояниями и m выходами.

Определение 3.9.1. Пусть Z′ — некоторое по меньшей мере двухэлементное подмножество множества состояний автомата A. Слово w из F(X) называется автономным диагностическим экспериментом для A по определению начального состояния из Z′ (*экспериментом по определению начального состояния для* (A, Z′)), если отображение $h_w: Z' \to F(Y)$, где $\bar{h}_w(z)=h_z(w)$ для z из Z′ является инъективным т. е. если из $z \neq z'$ всегда вытекает, что $h_w(z) \neq \bar{h}_w(z')$. Длина слова w называется длиной эксперимента.

Теорема 3.9.2. Для каждого сокращенного автомата Мура A и любого подмножества Z′ (где $p=|Z'| \geqslant 2$) множества состояний автомата A с помощью описываемого ниже метода можно установить, существует ли эксперимент по определению состояний для (A, Z′). В случае, если эксперимент существует, такой эксперимент может быть построен с длиной, не превышающей $(p-m'+1)n^p$, при $p>m'$, где $m'=|\{h(z) \mid z \in Z'\}|$ (если $p=m'$, то, очевидно, пустое слово Λ оказывается требуемым экспериментом).

Метод состоит из следующих шагов.

1. Построить для каждого y из Y множество

$$N(Z', \Lambda, y) = \{z \in Z' \mid h(z) = y\}.$$

2. Положить $\bar{N}(Z', \Lambda) = \{N(Z', \Lambda, y) \mid y \in Y\}$ и $k = -1$.

3. До тех пор, пока не будет найдено k такое, что:

либо существует w в X^k, при котором все множества, входящие в $\bar{N}(z', w)$, являются одноэлементными,

либо для любого w из X^k множество $\bar{N}(Z', w)$ пусто,

выполнять следующие шаги.

4. Увеличить k на 1.

5. Для каждого w из X^k и каждого x из X сделать следующее:

Если выполнены условия а)—в), то положить $\bar{N}(Z', wx) = \{N(Z', wx, vy) \mid y \in Y, N(Z', w, v) \in \bar{N}(Z', w)\}$.

В противном случае положить $\bar{N}(Z', wx) = \varnothing$.

а) $\bar{N}(Z', w) \neq \varnothing$;

б) для каждого $N(Z', w, v) \in \bar{N}(Z', w)$ и любых z и $z' \in N(Z', w, v)$ из $z \neq z'$ вытекает, что $f(z, x) \neq f(z', x)$;

в) не существует слова w′ длины, меньшей $|w|+1$, такого, что для любого y из Y и каждого $N(Z', w, v)$ соответствующее множество

$N(Z', wx, vy) = \{f(z, x) \mid z \in N(Z', w, v), h(f(z, x)) = y\}$ лежит в $\bar{N}(Z', w')$.

Замечание. Если $\bar{N}(Z', w) \neq \varnothing$, то $N(Z', w, v) = \{f^*(z, w) \mid z \in Z', h_z(w) = v\}$, т. е. если, скажем, $h_w(z) = h_w(z') = v$ для z и z′ из Z′, то состояния $f^*(z, w)$ и $f^*(z', w)$ различны и принадлежат оба множеству $N(Z', w, v)$.

Любое слово w, для которого в результате применения метода получается множество $\bar{N}(Z', w)$, содержащее в качестве элементов только одноэлементные множества, является экспериментом по определению начального состояния для (A, Z′). Если же такого слова не существует, то не существует и эксперимента по определению начального состояния для (A, Z′).

Доказательство. а) Метод дает результат (сходится) при рассмотрении слов длины, не превышающей $(p-m'+1)n^p$.

Действительно, при $m > p$ верно следующее. Пусть при фиксированном w выполнены равенства $\bar{N}(Z', w) = \{N_1, N_2, \ldots, N_q\}$ и $n_j = |N_j|$ для $j = 1, \ldots, q$. Упорядоченный набор $(n_1, \ldots, n_q)$ назовем типом множества $\bar{N}(Z', w)$. Тогда для любого x из X либо $|\bar{N}(Z', wx)| \geqslant |\bar{N}(Z', w)| + 1$, либо множества $\bar{N}(Z', w)$ и $\bar{N}(Z', wx)$ имеют одинаковый тип. Максимальное число множеств $\bar{N}(Z', w)$ типа $(n_1, \ldots, n_q)$ при произвольном слове w из F(X) есть $n^{n_1} n^{n_2} \ldots n^{n_q} = n^p$, поскольку $n_1 + n_2 + \ldots + n_q = p$, а n^{n_j} является числом всех подмножеств множества состояний Z, имеющих по n_j элементов [т. е. числом всех возможных n_j-элементных множеств $N(Z', w, v)$]. Поскольку $|\bar{N}(Z', \Lambda)| = m'$ и при $q = p$ все элементы множества $\bar{N}(Z', w)$ типа $(n_1, \ldots, n_q)$ должны быть одноэлементными множествами, то q может принимать лишь значе-

ния m', $m'+1, \ldots, p$. Итак, при использовании рассматриваемого метода может встретиться не более $(p-m'+1)n^p$ непустых множеств $\bar{N}(Z', w)$.

При $m'=p$ уже множество $\bar{N}(Z', \Lambda)$ состоит только из одноэлементных множеств.

б) Метод корректен, т. е. приводит к правильному результату.

Если применение метода привело к построению множества $\bar{N}(Z', w)$, содержащего в качестве элементов только одноэлементные множества, то для любых двух различных сотояний z и z' из Z' выполнено условие $h_w(z) \neq h_w(z')$, т. е. отображение h_w является в этом случае инъективным на Z'.

Далее, при выполнении цикла «до тех пор, пока» остается справедливым следующее высказывание: если существует эксперимент по определению начального состояния для (A, Z'), то существует и слово w с $\bar{N}(Z', w) \neq \varnothing$, которое может быть продолжено до такого эксперимента. Это высказывание истинно перед началом цикла «до тех пор, пока», и его истинность сохраняется при выполнении цикла.

Действительно, если существует слово w' такое, что $|w'| \leqslant |w|$, и такое, что при некотором x из X все множества $N(Z', wx, vy)$ (где $y \in Y$ и $N(Z', w, v) \in \bar{N}(Z', w)$) являются уже элементами множества $\bar{N}(Z', w')$, то слово w' может быть продолжено до эксперимента по определению начального состояния тогда и только тогда, когда до такого эксперимента может быть продолжено слово wx. Если в то же время для некоторой пары различных состояний z и z' из некоторого $N(Z', w, v)$ и для какого-то x из X выполнено равенство $f(z, x)=f(z', x)$, то слово wx не может быть продолжено до эксперимента по определению начального состояния для (A, Z'). Итак, в обоих случаях можно положить $\bar{N}(Z', wx)=\varnothing$, сохраняя истинность рассматриваемого высказывания.

Так как высказывание остается справедливым в момент окончания работы, для (A, Z') не может существовать эксперимента по определению начального состояния, если не получено множество $\bar{N}(Z, w)$, содержащее в качестве элементов только одноэлементные множества. ■

В качестве дополнения читателю рекомендуется выполнить упражнение 3.15.

Замечание. Для наглядного представления описанного в теореме метода и для работы с простыми задачами полезно использовать так называемое *А-диагностическое дерево*, являющееся ориентированным графом, вершины которого — множества $\bar{N}(Z', w)$, а ребра, помеченные входом x, ведут из $\bar{N}(Z', w)$ в $\bar{N}(Z', wx)$.

Пример 3.9.3. Рассматривая А-диагностическое дерево для автомата Мура, граф которого изображен на рис. 3.7.1, находим, что слово]]]]] является автономным диагностическим экспериментом по определению начального состояния этого автомата (рис. 3.9.1). Для того чтобы найти это слово, достаточно построить

дерево только до пятого уровня (показанного штриховой линией). Отметим, что начальным является состояние z_i, если входная последовательность]]]]] приводит к появлению выхода $0^i 1\, 0^{5-i}$.

Для исследования проблемы определения финального состояния очень полезно приведенное ниже уточнение первой части теоремы о сокращении (теорема 3.3.2). Для доказательства нам понадобятся утверждения и понятия из доказательства теоремы Хаффмана — Мили (теорема 2.3.3), в частности, понятие k-эквивалентности.

Теорема 3.9.4. Пусть Z_1, ..., Z_q — попарно дизъюнктные (непересекающиеся) подмножества множества состояний автомата A,

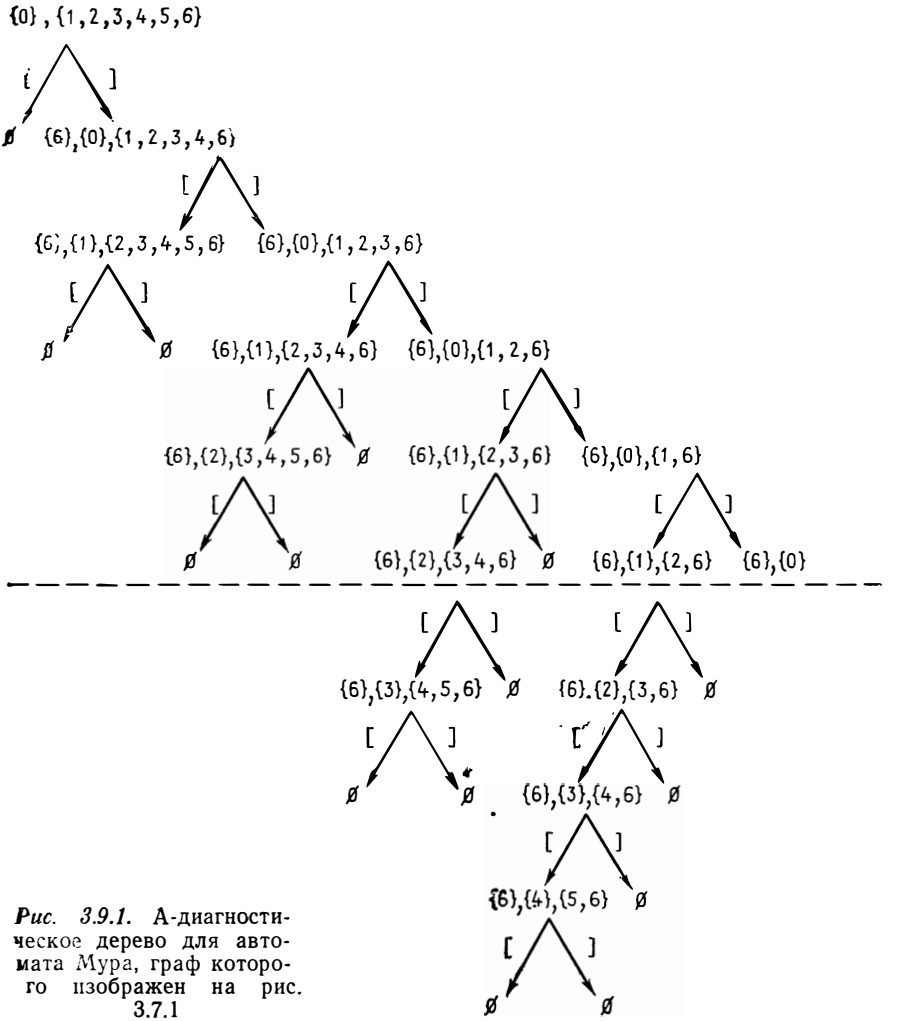


Рис. 3.9.1. A-диагностическое дерево для автомата Мура, граф которого изображен на рис. 3.7.1

причем такие, что по меньшей мере одно из множеств содержит по крайней мере два неэквивалентных состояния.

Пусть далее $p=|Z_1|+|Z_2|+\ldots+|Z_q|-q+1$ (поэтому при $q=1$ имеем $p=|Z_1|$) и $\bar{p}=\max(0, n-m-p+2)$.

Тогда по меньшей мере одно из множеств Z_i содержит минимум два не $\bar{p}$-эквивалентных состояния, т. е. существуют индекс j (где $1\leqslant j\leqslant q$), два состояния z и z' из Z_j и входное слово w длины, не большей $\bar{p}$, такие, что $h_z(w)\neq h_{z'}(w)$.

Граница $\bar{p}$ для длины слова w точна.

Доказательство. а) Пусть $\bar{k}$ — наименьшее из натуральных чисел k со следующим свойством: классы k-эквивалентных состояний автомата A являются также классами $(k+1)$-эквивалентных состояний, т. е. просто классами эквивалентных состояний. Будем различать следующие три случая.

1. Если $\bar{p}\geqslant\bar{k}$, то неэквивалентные состояния оказываются и не $\bar{p}$-эквивалентными, так что по предположению хотя бы одно из множеств Z_i содержит два не $\bar{p}$-эквивалентных состояния.

2. Если $\bar{p}=0$, то $p\geqslant n-m+2$.

В этом случае не может быть выполнено неравенство $q\geqslant m$, так как иначе мы бы имели $n\geqslant p+q-1\geqslant p+m-1\geqslant n+1$. Итак, $q<m$. Предположим, что при каждом i, где $1\leqslant i\leqslant q$, для любых двух состояний z и z' из Z_i выполнено равенство $h(z)=h(z')$. Тогда $m-q>0$ выходов «остаются свободными», что из-за сюръективности отображения h означает, что по меньшей мере $m-q$ состояний из Z не лежат в объединении множеств Z_i $(1\leqslant i\leqslant q)$. Отсюда получаем противоречие: $n\geqslant(p+q-1)+(m-q)=p+m-1\geqslant n+1$. Итак, должно существовать множество Z_i $(1\leqslant i\leqslant q)$, содержащее два состояния, порождающие различные выходы, т. е. не являющиеся $\bar{p}$-эквивалентными.

3. Пусть теперь $0<\bar{p}<\bar{k}$. Тогда $\bar{p}=n-m-p+2$ и выполнено неравенство $q<\bar{p}+m$, поскольку иначе мы имели бы $p+q-1\geqslant p+\bar{p}+m-1=n+1$. Из доказательства теоремы 2.3.3 и наброска доказательства теоремы 3.3.2 вытекает, что автомат A имеет не менее $\bar{p}+m$ различных классов $\bar{p}$-эквивалентности. Если бы каждое множество Z_i при $i=1, \ldots, q$ целиком входило в некоторый класс $\bar{p}$-эквивалентности, то имелось бы $(\bar{p}+m)-q>0$ классов $\bar{p}$-эквивалентности, не содержащих состояний из множеств Z_i. Это снова приводит к противоречию $n\geqslant(p+q-1)+(\bar{p}+m)-q=n+1$, так что по меньшей мере одно из множеств Z_i должно содержать пару не $\bar{p}$-эквивалентных состояний.

б) Описываемая ниже серия автоматов Мура показывает, что граница $\bar{p}$ точна.

Пусть $n, m\geqslant 2$. Тогда

$$A_{n,m}=(Z_n, X, Y_m, f_{n,m}, h_{n,m}),$$

где $Z_n=\{z_1, \ldots, z_n\}$, $Y_m=\{1, \ldots, m\}$, множество X — произвольно, $f_{n,m}(z_j, x)=z_{i+1}$ при $i=1, \ldots, n-1$ и любом x из X;

$f_{n,m}(z_n, x)=z_n$ при произвольном x из X;

$h_{n,m}(z_i)=\max(1, i-n+m)$ при $i=1, \ldots, n$.

Легко проверить, что все автоматы $A_{n,m}$ сокращенные.

Пусть теперь p и q — натуральные числа такие, что $p \leqslant n-m+1$ и $p+q-1 \leqslant n$. Тогда положим $Z_1=\{z_1, \ldots, z_p\}$ и $Z_i=\{z_{p+i-1}\}$ для $i=2, 3, \ldots, q$.

Множества Z_i, $1 \leqslant i \leqslant q$, удовлетворяют условию теоремы. Кратчайшее слово, различающее состояния z и z′ из Z_1, является кратчайшим словом, переводящим z_p в z_{n-m+2}. Такое слово имеет длину $n-m+2-p=\bar{p}$, так что приведенная в теореме граница точна. ■

АДАПТИВНЫЙ МЕТОД

Следствие 3.9.5. Пусть A — сокращенный автомат Мура и Z′ — некоторое p-элементное множество состояний автомата A, где $p \geqslant 2$. Тогда описанным ниже способом можно с помощью адаптивного диагностического эксперимента определить, в каком состоянии находится A в момент окончания эксперимента, если известно, что в момент начала эксперимента A находился в одном из состояний из множества Z′. При этом длина эксперимента, т. е. число последовательно выбираемых входов x из X, не превышает $(\tilde{p}-1)\left(n-m-\frac{1}{2}(\tilde{p}-2)\right)$, где $\tilde{p}=\min(p, n-m+1)$. Эта граница точна при условии, что величина (число элементов) множества X не ограничена сверху.

Метод проведения эксперимента. 1. Множество Z′ разбивается на подмножества $Z_y'=\{z \in Z' \mid h(z)=y\}$ при y из Y, и на основе первого выхода определяется, в каком множестве Z_y' содержится состояние, в котором A находится в момент начала эксперимента. Это множество обозначается Z_E'.

2. До тех пор, пока не будет выполнено условие $|Z_E'|=1$, выполняется следующее: выбирается слово w из F(X) длины, не большей, чем $n-m-|Z_E'|+2$, различающее по меньшей мере два состояния из Z_E'. Пусть v — выходная последовательность без первого символа, полученная при слове w. Тогда строятся множества $Z_v'=\{z \in Z_E' \mid \bar{h}_z(w)=v\}$ и $Z_E'=\{f^*(z, w) \mid z \in Z_v'\}$.

3. Если $Z_E'=\{z'\}$, то z′ — искомое финальное состояние.

Доказательство. а) Из теоремы 3.9.4 при q=1 вытекает существование слова w, необходимого для выполнения цикла «до тех пор, пока». Действительно, никакие два состояния автомата A не эквивалентны, а получающееся на первом шаге множество Z_E' имеет не более $\tilde{p}=\min(p, n-m+1)$ элементов. Все же получающиеся на следующих шагах множества Z_E' содержат меньшее число элементов.

б) Цикл «до тех пор, пока» выполняется конечное число раз, так как при каждом его выполнении число элементов в множестве Z_E' уменьшается по меньшей мере на 1.

в) Рассмотрим момент начала любого цикла «до тех пор, пока». Если w — введенная к этому моменту входная последовательность, а v — соответствующая полученная выходная последовательность, то в этот момент

$Z_E' = \{f^*(z, w) \mid z \in Z', h_z(w) = v\}$.

Отсюда следует, что если $Z_E' = \{z'\}$, то z' — искомое финальное состояние.

г) Общая длина эксперимента не превышает

$$(n - m - \tilde{p} + 2) + (n - m - (\tilde{p} - 1) + 2) + \ldots + (n - m) =$$

$$= ((n - m) - (\tilde{p} - 2)) + ((n - m) - (\tilde{p} - 2) + 1) + \ldots + ((n - m) -$$

$$- (\tilde{p} - 2) + (\tilde{p} - 2)) = (\tilde{p} - 1)((n - m) - (\tilde{p} - 2)) + 1 + 2 + \ldots$$

$$\ldots + (\tilde{p} - 2) = (\tilde{p} - 1)(n - m - (\tilde{p} - 2)) + \frac{1}{2}(\tilde{p} - 1)(\tilde{p} - 2) =$$

$$= (\tilde{p} - 1)\left(n - m - \frac{1}{2}(\tilde{p} - 2)\right).$$

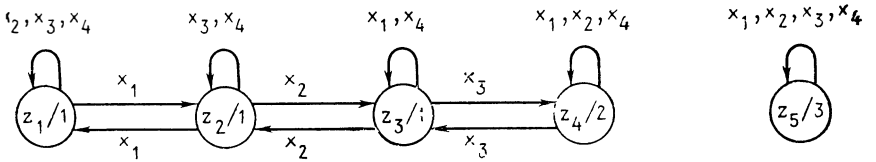


Рис. 3.9.2. Автомат Мура $A_{5,3,4}$

д) Описываемая ниже серия автоматов Мура показывает, что полученная граница является точной. Для $1 < m \leqslant n$ и $n - m + 1 \leqslant r$ пусть:

$t = (n, m, r)$,

$A_t = (\{z_1, \ldots, z_n\}, \{x_1, \ldots, x_r\}, \{1, 2, \ldots, m\}, f_t, h_t)$;

$h_t(z_i) = \max(1, i - n + m)$ для $i = 1, \ldots, n$;

$f_t(z_j, x_j) = z_{j+1}$, $f_t(z_{j+1}, x_j) = z_j$ для $j = 1, \ldots, n - m + 1$;

$f_t(z_i, x_k) = z_1$ для $i = 1, \ldots, n$ и всех k из множества $\{n - m + 2, \ldots, r\}$ и всех k из $\{1, \ldots, n - m + 1\}$ таких, что $k \neq i$ и $k \neq i - 1$.

Легко проверяется, что автоматы A_t — сокращенные. Граф автомата $A_{(5,3,4)}$ изображен на рис. 3.9.2.

Пусть, далее, $Z_t' = \{z_i \in Z_t \mid h_t(z_i) = 1\}$, так что $p = n - m + 1$. Покажем, что не существует входной последовательности длины, меньшей $1 = (p - 1)\left(n - m - \frac{1}{2}(p - 2)\right) = (p - 1)\left(p - 1 - \frac{1}{2}p + 1\right) = \frac{1}{2}p(p - 1)$, которая могла бы использоваться в качестве (адаптивного) эксперимента по определению финального состояния при наличии информации о том, что начальное состояние принадлежит множеству Z_t'.

Очевидно, каждая входная последовательность, в которую не входит x_p, приводит для автомата, находящегося в состоянии из

Z_t', к выходной последовательности вида 1 1 ... 1 и переводит автомат в некоторое состояние из Z_t'. При этом разные состояния из Z_t' переходят в разные состояния, так как каждый вход $x_i \neq x_p$ либо сохраняет все состояния из Z_t', либо переводит два состояния из Z_t' одно в другое и сохраняет остальные.

Итак, финальное состояние можно определить только тогда, когда на вход по меньшей мере один раз будет подано x_p. Другие входы перед первым x_p бесполезны. Если вход x_p порождает выход 2, то все ясно. В противном случае ясно, что автомат находится в одном из состояний из множества $Z_t' - \{z_p\}$.

Аналогичные рассуждения приводят к выводу, что входное слово $x_{p-1}x_p$, порождающее отличный от 1 последний выход, так же позволяет определить финальное состояние. Если же после использования входной последовательности $x_p x_{p-1} x_p$ финальное состояние не определилось, то ясно, что автомат находится в одном из состояний из множества $Z_t' - \{z_{p-1}, z_p\}$.

Методом полной индукции теперь нетрудно получить, что только при использовании (самой короткой) входной последовательности $x_p x_{p-1} x_p x_{p-2} x_{p-1} x_p$ ... x_p во всех случаях может быть определено финальное состояние, если выход 2 появился после i-го входа x_p, то начальным состоянием было состояние z_{p-i+1}, если же все выходы равны 1, то начальным было состояние z_1.

Длина рассматриваемой входной последовательности равна $1+2+ \ldots +(p-1) = (1/2)\,p\,(p-1)$. ■

Замечание. Если в следствии 3.9.5 предположить, что $|X| \leqslant n-m$, то приведенная в нем граница не может быть достигнута с помощью автоматов $A_{n,m}$. Упражнение 3.16 показывает, однако, что в таком случае эта граница оказывается завышенной только на постоянный множитель.

Автоматы Мура A_t позволяет также установить нижнюю границу для длины экспериментов по определению начального состояния. Из теоремы 3.9.2 получается следствие.

Следствие 3.9.6. Пусть $\alpha(n, m, r)$ — максимум длин всех экспериментов по определению начального состояния для автоматов Мура с $n \geqslant 2$ состояниями, m выходами и r входами. Тогда

$$\frac{1}{2}(n-m)\,(n-m+1) \leqslant \alpha(n, m, r) \leqslant (n-m+1) \cdot n^n.$$

Замечание. Верхняя граница для α очень велика. До сих пор остается неизвестным, насколько α может быть велико в действительности (см. также упражнение 3.15).

Определение 3.9.7. Пусть Z' — некоторое множество состояний автомата A. Слово w из $F(X)$ называется автономным диагностическим экспериментом для A по определению финального состояния при старте в Z' [коротко: *экспериментом по определению финального состояния для* (A, Z')], если существует отображение t: $F(Y) \to Z$ такое, что $t(h_z(w)) = f^*(z, w)$ для всех z из Z', т. е. если для всех z и z' из Z' выполнено условие: из $h_z(w) = h_{z'}(w)$ вытекает, что $f^*(z, w) = f^*(z', w)$.

Замечание. Данное определение соответствует интуитивному представлению об экспериментах по определению финального состояния. Покажем это. Если с помощью автономного эксперимента, т. е. путем задания входного слова w, можно определить финальное состояние при старте в состоянии из множества Z′ на основе анализа полученного выходного слова, то определено и отображение t, которое каждому возможному выходному слову $h_z(w)$ сопоставляет финальное состояние $f^*(z, w)$.

Имея же, с другой стороны, описанное в определении отображение t и выходное слово v, полученное при обработке автоматом входного слова w, получаем искомое финальное состояние: t(v).

Для того чтобы из теоремы 3.9.4 вывести утверждение о существовании и длине автономного диагностического эксперимента по определению финального состояния, нам понадобится довольно сложная лемма.

Лемма 3.9.8. Пусть $Q=\{M_i \mid i\in I\}$ — конечная система конечных непустых множеств. Будем говорить, что множества M и M′ из Q взаимно сцеплены, если в Q существуют множества $M_1, \ldots, M_n$ такие, что $M=M_1$, $M'=M_n$ и $M_j \cap M_{j+1}\neq\varnothing$ при $j=1, \ldots, n-1$.

Определим далее для каждого M из Q множество [M] равенством

$$[M]=\cup\{M'\in Q \mid M \text{ и } M' \text{ взаимно сцеплены}\}$$

и положим $\bar{Q}=\{[M] \mid M\in Q\}$.

Тогда

1. $\bar{Q}$ является разбиением множества $V_Q=\cup\{M \mid M\in Q\}$, т. е. $\cup\{[M] \mid M\in Q\}=V_Q$ и $[M]\cap[M']=\varnothing$ при $[M]\neq[M]'$;

2. $\sum\limits_{i\in I} |M_i| - |V_Q| \geqslant |I| - |\bar{Q}|$.

Доказательство. Так как каждое множество M из Q сцеплено с самим собой, то всегда $M\subseteq[M]$. Далее, конечно, всегда $[M]\subseteq V_Q$. Поэтому $\cup\{[M] \mid M\in Q\}=V_Q$.

Предположим, что $[M]\cap[M']\neq\varnothing$ для некоторой пары множеств M и M′ из Q. Тогда должны существовать в Q множества: M_i, сцепленное с M, и M_j, сцепленное с M′, такие, что $M_i\cap M_j\neq\varnothing$. Но тогда и множества M и M′ оказываются взаимно сцепленными, т. е. $[M]=[M']$.

Пусть M — произвольное множество из Q и $I_M=\{i\in I \mid M_i\subseteq [M]\}$.

Поскольку элементы множества $\bar{Q}$ попарно дизъюнктны, то утверждение 2 немедленно вытекает из следующего промежуточного утверждения:

2′. $\sum\limits_{i\in I_M} |M_i| - |[M]| \geqslant |I_M| - 1$ для любого M из Q.

Пусть теперь M — произвольное, но фиксированное множество из Q. Чтобы иметь возможность провести доказательство по индукции, занумеруем множество индексов I_M, т. е. положим

$I_M = \{i_1, i_2, \ldots, i_m\}$, причем выберем нумерацию так, чтобы при $k = 1, \ldots, m-1$ выполнялось соотношение $M_{i_{k+1}} \cap (M_{i_1} \cup \ldots \cup M_{i_k}) \neq \varnothing$. Это всегда возможно, так как все множества M_i при $i \in I_M$ взаимно сцеплены.

Докажем теперь полной индукцией по k, что $|M_{i_1}| + \ldots + |M_{i_k}| - |M_{i_1} \cup \ldots \cup M_{i_k}| \geqslant k-1$ при $k = 1, \ldots, m$. Отсюда при $k = m$ получим утверждение 2′.

При $k = 1$ утверждение очевидно.

Нам понадобится теперь следующий очевидный факт: для произвольных конечных пересекающихся множеств U и V выполняется неравенство $|U| + |V| - |U \cup V| \geqslant 1$, так что, в частности,

$$|M_{i_1} \cup \ldots \cup M_{i_k}| + |M_{i_{k+1}}| - |M_{i_1} \cup \ldots \cup M_{i_{k+1}}| \geqslant 1.$$

Из сказанного и из предположения индукции (предполагается истинность утверждения для k) получаем

$$|M_{i_1}| + \ldots + |M_{i_k}| + (|M_{i_{k+1}}| - |M_{i_1} \cup \ldots \cup M_{i_{k+1}}|) \geqslant$$

$$\geqslant |M_{i_1}| + \ldots + |M_{i_k}| + 1 - |M_{i_1} \cup \ldots \cup M_{i_k}| \geqslant (k-1) + 1 = k. \blacksquare$$

Теорема 3.9.9 (Хиббард). Пусть A — сокращенный автомат Мура и $Z_1, \ldots, Z_q$ — попарно дизъюнктные и не все одноэлементные подмножества состояний автомата A, а m_i — число различных выходов, порождаемых состояниями из Z_i: $m_i = |h(Z_i)|$ при $i = 1, \ldots, q$. Пусть также $r = |Z_1| + \ldots + |Z_q|$, $d = r - q$, $q' = m_1 + \ldots + m_q$ и $d' = r - q'$.

Если $d' \neq 0$, то существует входное слово w длины, не большей $(n-m-d'+1) + (n-m-d'+2) + \ldots + (n-m)$, которое для каждого $i = 1, \ldots, q$ является экспериментом по определению финального состояния для (A, Z_i) (при $d' = 0$ уже Λ оказывается таким экспериментом).

Доказательство. Сначала разложим Z_i на m_i дизъюнктных множеств $Z_{i,y}$ так, чтобы в каждом таком множестве содержались все состояния из Z_i, порождающие выход y:

$$Z_{i,y} = \{z \in Z_i \mid h(z_i) = y\}.$$

Таким образом получаем q' дизъюнктных множеств $Z_1', \ldots, Z_{q'}'$. Если все эти множества одноэлементны, то Λ является экспериментом по определению финального состояния для любой пары (A, Z_i). Это в точности тот случай, когда $r = q'$, так что $d' = 0$.

Предположим теперь, что $d' \geqslant 1$. Для этого случая мы докажем теорему полной индукцией по d' (используя Z_i' вместо Z_i). Легко видеть, что входное слово w, являющееся экспериментом по определению финального состояния для каждой пары (A, Z_i') при $i = 1, \ldots, q'$, оказывается таковым и для каждой пары (A, Z_i) при $i = 1, \ldots, q$. Это следует из того, что первый элемент полу-

чающейся при вводе слова w выходной последовательности однозначно определяет, в каком из подмножеств $Z_{i,y}$ множества Z_i находится состояние автомата перед началом работы.

Пусть $d'=1$. Тогда в точности одно из множеств Z_i', например множество Z_k', является двухэлементным, а все остальные множества одноэлементны. Поскольку автомат A сокращенный, то по теореме 3.3.2 существует слово длины, не превышающей $n-m$, различающее оба состояния из Z_k'. Это слово оказывается, очевидно, экспериментом по определению финального состояния для всех пар (A, Z_i') при $i=1, \ldots, q'$.

Пусть теперь $d'>1$. Тогда вследствие сокращенности автомата A и теоремы 3.9.4 существуют слово w длины, не большей $n-m-\bar{p}+2=n-m-(d'+1)+2=n-m-d'+1$, и множество Z_k' с двумя, по меньшей мере, состояниями z и z′ такими, что $h_z(w) \neq h_{z'}(w)$. . Положим тогда

$$P=\{(i, v) \mid 1 \leqslant i \leqslant q',\ v=h_z(w) \text{ для подходящего } z \in Z_i'\}.$$

Из неравенства $d'>1$ имеем $|P| \geqslant q'+1$. Для каждой пары (i, v) из P положим далее

$$Z'_{i,v}=\{f^*(z, w) \mid z \in Z_i',\ h_z(w)=v\}.$$

Теперь возможны два случая.

1. $|Z'_{i,v}|=1$ для каждой пары (i, v) из P.

В этом случае слово w оказывается экспериментом по определению финального состояния для любой пары (A, Z_i') при $i=1, \ldots, q'$. Действительно, из равенств $h_z(w)=h_{z'}(w)=v$ вытекает, что для любых z и z′ из Z_i' пара (i, v) содержится в P, а состояния $f^*(z, w)$ и $f^*(z', w)$ — в $Z'_{i,v}$, так что $f^*(z, w)=f^*(z', w)$.

2. Существует пара (i, v) в P такая, что $|Z'_{i,v}| \geqslant 2$.

Множество $Q=\{Z'_{i,v} \mid (i, v) \in P\}$ удовлетворяет предположению леммы 3.9.8, поскольку множества $Z'_{i,v}$ непусты и конечны, P — тоже конечно, так как для каждого i число слов v, удовлетворяющих условию $h_z(w)=v$ для подходящих z из Z_i', конечно (слово w фиксировано!). Пусть $\bar{Q}$ — существующее по лемме 3.9.8 разбиение множества V_Q, $\bar{q}=|\bar{Q}|$ и $\bar{r}=|V_Q|$. По предположению тогда $\bar{q}<\bar{r}$, так что $\bar{d}=r-\bar{q}>0$. Чтобы использовать предположение индукции для множеств из $\bar{Q}$ (вместо Z_i'), следует сначала показать, что $\bar{d} \geqslant d_1$.

Из леммы вытекает, что $\sum_{(i, v) \in P} |Z'_{i,v}| - \bar{r} \geqslant |P| - \bar{q}$. Из того, что множества Z_i' попарно дизъюнктны, следует далее

$$\sum_{(i, v) \in P} |Z'_{i,v}| \leqslant \sum_{1 \leqslant i \leqslant q'} |Z_i'| = r.$$

Из сказанного вытекает, что $r-\bar{r} \geqslant |P|-\bar{q} \geqslant q'+1-\bar{q}$, откуда получаем $r-q'-1 \geqslant \bar{r}-\bar{q}$, что и требовалось.

По предположению индукции существует слово w' длины, не большей $s=(n-m-\bar{d}+1)+(n-m-\bar{d}+2)+\ \ldots\ +(n-m)$, являющееся для каждой пары $(A, \bar{Z})$, где $\bar{Z}$ — множество из $\bar{Q}$, экспериментом по определению финального состояния. Нам остается показать, что слово ww' оказывается экспериментом по определению финального состояния для пар (A, Z_i') при $1\leqslant i\leqslant q'$, поскольку тогда мы получаем такой эксперимент длины

$$(n-m-d'+1)+s\leqslant(n-m-d'+1)+(n-m-d'+2)+\ \ldots$$
$$\ldots+(n-m).$$

Итак, рассмотрим произвольное i, где $1\leqslant i\leqslant q'$, и два произвольных состояния z и z' из Z_i', для которых выполнено равенство $h_z(ww')=h_{z'}(ww')$. Следует показать, что в этом случае $f^*(z, ww')=f^*(z', ww')$. Пусть $h_z(w)=v$. Тогда $h_{z'}(w)=v$, а состояния $s=f^*(z, w)$ и $s'=f^*(z', w)$ принадлежат множеству $Z_{i,v}$. По построению множества $\bar{Q}$ в нем существует множество $\bar{Z}$ такое, что $Z'_{i,v}\subseteq\bar{Z}$, а слово w' является экспериментом по определению финального состояния для $(A, \bar{Z})$. Поскольку из предположения о z и z' следует, что $h_s(w')=h_{s'}(w')$, то из сказанного имеем

$$f^*(z, ww')=f^*(s, w')=f^*(s', w')=f^*(z', ww'). \blacksquare$$

Следствие 3.9.10. Каждый сокращенный автомат Мура с n состояниями и m выходами обладает при каждом подмножестве $Z'(p=|Z'|\geqslant 2)$ множества состояний экспериментом по определению финального состояния для (A, Z') длины, не большей $(\tilde{p}-1)(n-m-(1/2)(\tilde{p}-2))$, где $\tilde{p}=\min(p, n-m+1)$. Граница для длины точна, если величина множества входов X не ограничена.

Доказательство. Утверждение непосредственно вытекает из теоремы 3.9.9 (случай $q=1$) и доказательства следствия 3.9.5, поскольку при $q=1$ выполнены равенства $d=p-1$ и $d'=\tilde{p}$.

Замечания. 1. Отметим, что адаптивные эксперименты по определению финального состояния не являются, вообще говоря, более короткими, чем автономные (см. следствия 3.9.5 и 3.9.10).

2. При рассмотрении простых примеров очень удобно, как и в случае экспериментов по определению начального состояния (см. пример 3.9.3), строить так называемые *E-диагностические деревья* — см. упражнение 3.17.

Некоторые высказывания об экспериментах по идентификации автоматов содержатся в упражнении 3.18.

УПРАЖНЕНИЯ

3.1. (Мур.) Пусть X — конечное множество. Задайте для каждого слова w из F(X) автомат Мура K(w) со следующим свойством: K(w) имеет два выхода 0 и 1 и выделенное (начальное) состояние z_0; если автомату K(w) на вход подается слово v, не содержащее w в качестве подслова ($v\neq swt$ при всех s и t

из $F(X)$), а $K(w)$ находится в состоянии z_0, то выход должен состоять из одних нулей, если v содержит w в качестве подслова, то последний выход должен быть равен 1.

3.2. (Мур) Покажите, что приведенная в теореме о сокращении (теорема 3.3.2) граница $n-m$ точна, т. е. постройте для любых m и n автомат Мура $D_{n,m}$ с n состояниями и m выходами такой, что $D_{n,m}$ имеет два (по меньшей мере) различных не эквивалентных состояния с реакциями, совпадающими на всех входных последовательностях длины, меньшей $n-m$.

3.3. Докажите, что не существует автомата Мура с менее чем четырьмя состояниями, удовлетворяющего условию теоремы Мура о неопределенности (теорема 3.3.3). Покажите далее, что можно использовать автоматы с тремя (но не с меньшим числом) состояниями, если условие теоремы ослабить до требования $\overline{h}_z(w) \neq \overline{h}_{z'}(w)$ для всех $z \neq z'$.

3.4. 1. Для всех рассмотренных в разд. 3.1—3.3 и в упражнениях 3.1—3.3 автоматов Мура постройте равносильные автоматы Мили.

2. Докажите аналог теоремы 2.3.2 для автоматов Мура как непосредственно (т. е. используя только определение 3.3.1), так и применяя теорему 3.4.2 к теореме 2.3.2. [Указание. Заметьте, что для $z' = f^*(z, w)$ выполнено условие

$$h_z(w)h_{z'}(v) \neq h_z(wv) = h_z(w)\overline{h}_{z'}(v).]$$

3.5. (Ибарра.) Покажите, что в формулировке теоремы 3.4.3 нельзя поменять местами понятия «автомат Мили» и «автомат Мура», т. е. что два равносильных некоторому автомату Мили автомата Мура не обязательно эквивалентны. Какое дополнительное условие должно быть выполнено, чтобы обращение в указанном смысле теоремы 3.4.3 было истинно? Покажите далее, что методом, использованным в доказательстве теоремы 3.4.4, для данного автомата Мили могут быть построены два не эквивалентных между собой равносильных автомата Мура. Как должно быть изменено доказательство теоремы 3.4.4, чтобы такое не было возможным?

3.6. (Блох, Глушков.) Пусть $A=(Z, X, Y, f, g)$ — автомат Мили. Покажите, что следующий автомат Мура A' равносилен автомату A:

$A' = (Z', X, Y, f', h)$, где $Z' = Z \cup Z \times X$,

$f'(z, x) = (z, x)$, $f'((z, x), x') = (f(z, x), z')$,

$h(z) = y_0$, $h((z, x)) = g(z, x)$ для всех z из Z и всех x из X, где y_0 — некоторый произвольный, но фиксированный элемент множества Y.

Сравните этот автомат Мура с построенным в теореме 3.4.4. Когда A' имеет меньше состояний?

3.7.* (Спивак.) По аналогии с определением 3.4.1 назовем два состояния некоторого автомата Мура равносильными, если совпадают ограничения их реакций на входные слова из соответствующей свободной полугруппы. Назовем, далее, два автомата Мура с одинаковыми множествами входов X и выходов равносильными, если совпадают ограничения их реакций на $F^+(X)$. Будем называть автомат Мура g-сокращенным, если у него нет двух различных равносильных состояний. Состояние z автомата Мура A называется достижимым, если существуют состояние z' и вход x из X такие, что $f(z', x) = z$. Пусть $E(A)$ — множество всех достижимых состояний автомата A.

Автомат Мура называется сокращенным по Мили, если любые два его различных состояния из $E(A)$ неэквивалентны, а любое его недостижимое состояние

[т. е. состояние из Z—E(A)] не равносильно никакому другому состоянию из Z.

Теперь докажите следующее.

1. Каждый g-сокращенный автомат Мура является сокращенным по Мили, но не наоборот. В то же время сокращенный по Мили автомат Мура, полученный (методом из теоремы 3.4.4) из некоторого «представимого как автомат Мура», автомата Мили, является также g-сокращенным.

2. Каждый сокращенный по Мили автомат Мура является сокращенным, но не наоборот (так что и каждый g-сокращенный автомат Мура оказывается сокращенным, но не наоборот). Для автомата Мура, у которого все состояния достижимы, понятия «сокращенный по Мили» и «сокращенный» равносильны

3. Для произвольного автомата Мура не существует, вообще говоря, равносильного g-сокращенного автомата. Если, как в доказательствах теорем о сокращении (теоремы 2.3.5 и 3.3.2), используя классы равносильных состояний некоторого автомата Мура A, строить равносильный автомат, то нужно строить автомат Мили; при этом ни один равносильный автомату A автомат Мили не будет иметь меньше состояний, чем полученный в результате такого построения.

4. Для каждого автомата Мура A существует равносильный сокращенный по Мили автомат Мура $\tilde{A}$. Такой автомат, если абстрагироваться от выходов недостижимых состояний, определен однозначно с точностью до изоморфизма. Ни один равносильный автомату A автомат Мура не может иметь меньше состояний, чем автомат $\tilde{A}$.

5. Если A′ — автомат Мили и A — равносильный автомату A′ автомат Мура, то $\tilde{A}$ имеет минимальное число состояний среди всех равносильных автомату A′ автоматов Мура.

3.8. Автомат Мура A называется Z-гомоморфно сокращенным (коротко ZH-сокращенным), если каждый Z-гомоморфизм A на некоторый автомат Мура A′ является изоморфизмом. Докажите, что для каждого автомата Мура существует однозначно с точностью до изоморфизма определенный эквивалентный ZH-сокращенный автомат Мура, причем сокращенный и минимальный.

3.9.* (Мур.) Автомат Мура A=(Z, X, Y, f, g) называется сильно связным, если для любых его двух состояний z и z′ существует входное слово w из F(X) такое, что f*(z, w)=z′.

1. Постройте сокращенный автомат Мура, все состояния которого достижимы (т. е. для которого f(Z, X)=Z, см. упражнение 3.7), не являющийся сильно связным.

2. Пусть A — сильно связный автомат Мура и A′ — эквивалентный автомату A сокращенный автомат Мура. Докажите, что тогда и автомат A′ сильно связный. Покажите далее, что этого может и не быть, если автомат A′ не является сокращенным.

3. Докажите, что два сильно связных автомата Мура A и A′ эквивалентны уже тогда, когда существуют состояния z автомата A и z′ автомата A′, являющиеся эквивалентными.

4. Как можно в п. 3 ослабить требование сильной связности для автоматов A и A′, чтобы все же эквивалентность двух состояний влекла за собой эквивалентность автоматов?

3.10.* (Фальк.) Инициальным автоматом Мура называется шестерка A=(Z, X, Y, f, h, I) такая, что A′=(Z, X, Y, f, h) — автомат Мура и I⊆Z; элементы множества I называются инициальными состояниями. Реакцией инициаль-

ного автомата Мура A называется множество $L_I(A)=\{h_z \mid z\in I\}$; последовательностным отношением, определенным автоматом A (см. упражнение 2.8), — множество $T_I(A)=\cup\{\mathrm{gr}\, h_z \mid z\in I\}$.

A называется неизбыточным, если не существует такого состояния z в I, что для $I'=I-\{z\}$ выполняется равенство $T_I(A)=T_{I'}(A)$, т. е. если ни одно состояние не может быть исключено из I без изменения последовательностного отношения. A называется сокращенным, если таковым является A′. A называется инициально связным, если для каждого состояния z′ из Z существуют инициальное состояние z в I и входное слово w такие, что $f^*(z, w)=z'$. A называется сильно связным, если таковым является A′ (см. упражнение. 3.9). Два инициальных автомата Мура A_1 и A_2 изоморфны, если изоморфны соответствующие автоматы Мура A'_1 и A'_2 и если множества инициальных состояний при изоморфизме отображаются друг на друга.

Покажите следующее.

1. Пусть A_1 и A_2 — сокращенные инициально связные инициальные автоматы Мура с одинаковыми реакциями. Тогда A_1 и A_2 изоморфны.

2. Существует бесконечно много неизоморфных неизбыточных инициально связных сокращенных инициальных автоматов Мура с одинаковым последовательностным отношением.

3. Пусть A_1 и A_2 — неизбыточные сильно связные сокращенные инициальные автоматы Мура с одинаковым последовательностным отношением. Тогда A_1 и A_2 изоморфны.

[Указание к п. 2. Постройте бесконечную последовательность инициальных автоматов Мура $A_m=(Z, X, Y, f_m, h_m, I)$ с $|Z_m|=4m+2$, $X=Y=\{0, 1\}$, $I=\{z, z'\}$ и с двумя выделенными состояниями t и t′, так что

$h_{mt}=\{(w, 1\bar{w}) \mid w\in F(X)\}$, где $\bar{w}$ получается из w заменой 0 на 1 и наоборот (т. е., например, $w=011$, $\bar{w}=100$); $h_{mt'}=\{(w, 10^{|w|}) \mid w\in F(X)\}$;

$h_{mz}=\{(0^i 1w, 0^{2i+1}1\bar{w}) \mid i\geqslant 2m-1,\ w\in E(X)\}\cup\{(0^{2i}1w, 0^{2i+1}1\bar{w}) \mid 0\leqslant i\leqslant m-1,\ w\in F(X)\}\cup\{(0^{2i+1}1w, 0^{2i+2}10^{|w|}) \mid 0\leqslant i\leqslant m-2,\ w\in F(X)\}$;

$h_{mz'}=\{(0^i 1w, 0^{i+1}10^{|w|}) \mid i\geqslant 2m-1,\ w\in F(X)\}\cup\{(0^{2i}1w, 0^{2i+1}10^{|w|}) \mid 0\leqslant i\leqslant m-1,\ w\in F(X)\}\cup\{(0^{2i+1}1w, 0^{2i+2}1\bar{w}) \mid 0\leqslant i\leqslant m-2,\ w\in F(X)\}$.]

3.11. (Карп.) Покажите, что не существует натурального числа k такого, чтобы высказывание 1) теоремы 3.7.2 могло быть заменено на следующее: существует натуральное число m такое, что $\varphi_g(n)>\frac{1}{k}(n-1+|Y|)$ для всех $n\geqslant m$.

3.12.*. (Эвен.) Пусть r — вещественное число $(0<r<1)$ и $d(r)=0.\, r_1r_2\ldots$ — представление r в виде бесконечной двоичной дроби ($r_i\in\{0, 1\}$), которая тогда и только тогда является периодической, когда число r рационально.

Пусть g_r — отображение из $F^+(\{0, 1\})$ в $F(\{0, 1\})$, определенное условием $\eta_1(g_r(x_1x_2\ldots x_n))=1$ тогда и только тогда, когда двоичная дробь $0.x_1x_2\ldots x_n$ не превышает r. Докажите, что g_r является Мр-представимым тогда и только тогда, когда число r рационально.

3.13. Пусть X — конечный алфавит и $Y=\{0, 1\}$. Пусть, далее, для каждого слова w из F(X) зеркальное слово $\tilde{w}$ определяется следующим образом: $\tilde{x}=x$

для x из X, $\widetilde{uv}=\widetilde{v}\widetilde{u}$ для всех u и v из F(X). Пусть, наконец, отображение g из $F^+(X)$ в $F^+(Y)$ определяется условием: $g(w)=1$ тогда и только тогда, когда существует слово v такое, что $w=v\widetilde{v}$. Докажите, что g не является Мр-представимым.

3.14. 1. Докажите (методом полной индукции), что каждый сокращенный автомат Мура обладает адаптивным многократным диагностическим экспериментом по определению начального состояния, для которого нужно меньше копий автомата, чем число его состояний [см. утверждение 3.8.2, п. 5].

2. Докажите с использованием п.1, что для сокращенного автомата Мура с n состояниями всегда существует диагностический многократный автономный эксперимент по определению начального состояния, для которого требуется $\frac{1}{2}n(n-1)$ копий автомата (используйте п. 6 утверждения 3.8.2).

3.15. 1. Напишите программу, реализующую метод из теоремы 3.9 2, и проверьте для «не слишком больших» автоматов Мура, является ли полученная для длины эксперимента граница точной.

2. Покажите, что в случае $Z'=Z$ могут потребоваться входные последовательности длины самое большее n!

3.16. (Мур.) Определите длины кратчайших экспериментов по определению конечного состояния для (A_n, Z_n) при $n\in\mathbf{N}$, где

$A_n=(Z_n, \{0, 1\}, \{0, 1\}, f_n, h_n)$, $Z_n=\{z_1, \ldots, z_{2n+1}\}$;

$f_n(z_1, 0)=z_{n+2}$, $f_n(z_1, 1)=z_{n+1}$,

$f_n(z_i, 0)=z_{i+1}$ для $i=2, \ldots, 2n$,

$f_n(z_{2n+1}, 0)=z_2$, $f_n(z_{2n+1}, 1)=z_1$,

$f_n(z_i, 1)=z_i$ для $i=2, \ldots, n+1$,

$f_n(z_{n+j}, 1)=z_j$ для $j=2, \ldots, n$,

$h_n(z_1)=1$, $h_n(z_i)=0$ для $i=2, \ldots, 2n+1$.

3.17. Из доказательства теоремы 3.9.9 выведите определение E-диагностического дерева (по аналогии с A-диагностическим деревом из замечания после теоремы 3.9.2 и из примера 3.9.3) и постройте E-диагностические деревья для автоматов, графы которых изображены на рис. 3.2.1, 3.3.1 и 3.5.2, полагая (в обозначениях теоремы 3.9.9), что $q=1$ и $Z_1=Z$.

3.18.* (Мур, Штарке.) Пусть A и A′ — автоматы Мура с общим входным множеством X. Положим для w из F(X), что $h_A(w)=\{h_z(w)\mid z\in Z\}$. Автоматы A и A′ называются различимыми, если в F(X) существует слово w такое, что $h_A(w)\neq h_{A'}(w)$. Они называются сильно различимыми, если в F(X) существует слово w такое, что $h_A(w)\cap h_{A'}(w)=\varnothing$.

1. Постройте два автомата Мура, являющихся неразличимыми, но не эквивалентными.

2. Постройте два автомата Мура, являющихся различимыми, но не сильно различимыми.

3. Докажите, что два сильно связных автомата Мура эквивалентны, если они неразличимы. [Указание. Используйте упражнение 3.9.]

4. Пусть $M=\{A_1, \ldots, A_n\}$ — конечное семейство автоматов Мура с общим входным множеством X. Слово w из F(X) называется идентифицирующим экспериментом для M, если существует отображение α_w из $h_{A_1}(w)\cup\ldots\cup h_{A_n}(w)$

в {1, ..., n} такое, что $\alpha_w(v) = i$ для каждого i из {1, . . , n} и каждого v из $h_{A_i}(w)$.

Докажите, что идентифицирующий эксперимент для M существует тогда и только тогда, когда все автоматы A_i из M попарно сильно различимы.

3.19. 1. Перенесите как можно больше теорем и упражнений об автоматах Мили из гл. 2 на случай автоматов Мура, как это было сделано с теоремой о сокращении. В частности, перенесите теорему 2.2.3 и упражнения 2.1—2.4 и 2.6—2 10.

2. Перенесите как можно больше теорем и упражнений об автоматах Мура из гл. 3 на случай автоматов Мили, в частности теоремы 3.3.3 и 3.6.4 (упражнение 2.6) и упражнения 3.1, 3.3, 3.8—3.10.

ОБЗОР ЛИТЕРАТУРЫ

Описанная в данной главе модель конечных автоматов была первоначально описана Муром в работе [12]. В этой работе (впрочем, чрезвычайно трудной для чтения) получены в основном теоремы 3.3.2, 3.3.3 и 3.6.4 и результаты, вошедшие в упражнения 3.1, 3.2 и 3.9. Из этой же работы Мура берет начало теория экспериментов с автоматами; там получены частный случай ($p=n$, $m=2$) следствия 3.9.5, результат из упражнения 3.16 и пп. 1 и 3 из упражнения 3.18.

Пример 3.1.1 взят из области синтаксического анализа языков программирования, см. по этому поводу [13].

Равносильность автоматов Мили и Мура исследовалась первоначально в [3, 2, 7]. См. по этому поводу также важную работу [8] из списка литературы к гл. 2 (и ее же по поводу упражнения 3.6) работы [11] (и ее же по поводу упражнения 3.5) и [14] и (ее же по поводу упражнения 3.7).

Входно-независимые автоматы Мили исследовались в основном до 1962 г, (например в [9, 10], там же даны дальнейшие ссылки на литературу). Однако в этих работах еще считалось, что входно-независимые автоматы Мили соответствуют автоматам Мура (см. по этому поводу цитированную в гл. 2 книгу Гинзбурга [7, с. 42]). В [9] рассматривались частичные автоматы Мили (см. гл. 4), в связи с этим см. также [1].

По воводу примера 3.5.1 см. работу [5].

Понятие гомоморфизма автоматов было введено в работах [6, 8] из списка литературы к гл. 2. В обеих этих работах доказана теорема 3.6.4.

Содержание разд. 3.7 и упражнения 3.11 в основном соответствует работе Карпа (1967 г.).

По поводу упражнения 3.12 см. [6].

Понятия из разд. 3.8 близки к рассмотренным в [12]. См. также литературу к разд. 3.9, прежде всего цитированную в гл. 2 книгу [25], из которой взяты определения 3.9.1 и 3.9.7. Отметим, однако, что везде, кроме работы Мура, рассматривались автоматы Мили.

Теорема 3.9.2 взята из [8], см. также [5] из списка литературы к гл. 2.

Теоремы 3.9.4 и 3.9.8, лемма 3.9.7 и следствия 3.9.5 и 3.9.10 в основном соответствуют работе [10], см. также [4, 7] из списка литературы к гл. 2.

Упражнение 3.18, п. 4 основано на работе [15], см. также [25] из списка литературы к гл. 2.

ГЛАВА 4.

ЧАСТИЧНЫЕ АВТОМАТЫ МИЛИ

4.1. ВВОДНЫЕ ПРИМЕРЫ

На практике, особенно часто в тех случаях, когда входы для автомата поступают от некоторой технической системы (от другого автомата), определенные комбинации входов вообще не встречаютоя, т. е. автомат, находящийся в некотором состоянии, никогда не получает определенные входы. Часто также и не все выходы автомата представляют интерес, например могут использоваться только выходы, получаемые в определенные моменты времени, или только выходы, порождаемые автоматом, находящимся в определенном состоянии. Поэтому полезно рассматривать модели автоматов, в которых допускается, что определенные переходы из состояния в состояние или определенные выходы остаются незаданными.

Поскольку по результатам разд. 3.4 автоматы Мили и Мура равносильны, то мы ограничимся в этой главе рассмотрением автоматов Мили.

СУММАТОР С ЛИНЕЙНЫМ ВХОДОМ

Пример 4.1.1. Требуется построить автомат для сложения двоичных чисел, который получает на вход не параллельно записи слагаемых, как двоичные сумматоры из предыдущих глав, а одну входную последовательность, в которой цифры слагаемых записаны попеременно (см. ниже).

Итак, требуется построить автомат Мили $A=(Z, X, Y, f, g)$ со следующими свойствами:

1) $X=Y=\{0, 1\}$;

2) A имеет выделенное состояние s (начальное состояние);

3) пусть $w=a_1b_1a_2b_2 \ldots a_kb_k$ — входная последовательность длины 2k (k из **N**, a_i и b_i при $i=1, \ldots, k$ — элементы множества X) и пусть $g_s(w)=d_1c_1d_2c_2 \ldots d_kc_k$. Тогда двоичное число $c=c_kc_{k-1} \ldots c_1$ должно быть суммой по модулю 2^k двоичных чисел $a=a_ka_{k-1} \ldots a_1$ и $b=b_kb_{k-1} \ldots b_1$, т. е. c_i должно быть i-й цифрой (справа) суммы a и b;

4) A имеет минимальное число состояний, т. е. не существует автомата Мили со свойствами 1)—3), имеющего меньше состояний, чем A.

Очевидно, что только каждый второй знак в выходной последовательности имеет значение, т. е. знаки d_i при построении автомата могут не приниматься во внимание.

Построим сначала автомат Мили, удовлетворяющий только требованиям 1)—3). Выберем для него следующие пять состояний:

$z_0=s$. Это состояние автомат может принимать после введения четного числа знаков, скажем, после входа b_i и выхода c_i, если

при вычислении c_i не произошел перенос 1 в следующий разряд.

z_1. Это состояние автомат может принимать после введения нечетного числа знаков, скажем, после входа a_i, если из предыдущих вычислений вытекает, что $c_i = b_i$.

z_2. Это состояние автомат принимает после входа b_i, если при вычислении c_i произошел перенос 1 в следующий разряд.

z_3. Это состояние автомат принимает после входа a_i, если при вычислении c_i произошел перенос 1 в следующий разряд и если $c_i = b_i$.

z_4. Это состояние автомат принимает после входа a_i, если $c_i = \bar{b}_i$, где $\bar{0}=1$ и $\bar{1}=0$.

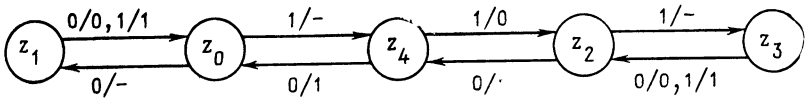


Рис. 4.1.1. Не полностью определенный последовательностный сумматор А с попеременным вводом цифр слагаемых

Автомат А имеет граф, изображенный на рис. 4.1.1, где не имеющие значения выходы обозначены тире. Таким образом, автомат А определен не полностью, только после замены всех тире на знаки 0 или 1 получается граф полностью определенного автомата Мили [причем так можно получить графы многих автоматов, удовлетворяющих, очевидно, условиям 1)—3)].

По состоянию, в которое автомат переходит после введения последовательности длины 2k, можно установить, является ли выходная последовательность в точности суммой a+b (в вышеописанном смысле) или нет: если последним оказывается состояние z_0, то c_i являются цифрами суммы a+b, если же финальное состояние — z_2, то выходная последовательность представляет число $a+b-2^k$.

Легко видеть, что А становится сокращенным автоматом Мили при любой расстановке цифр 0 или 1 вместо тире. Например, входная последовательность 010 показывает, что состояния z_0 и z_1 не могут быть эквивалентны (независимо от того, какой выход выбран для перехода из z_0 в z_4). Далее, например, входная последовательность 00 переводит пары состояний z_0, z_4 и z_2, z_4, а входная последовательность 000 — пары z_0, z_3 и z_2, z_3 в пару z_0, z_1; отсюда вытекает, что все эти пары состоят из неэквивалентных состояний (так как состояния z_0 и z_1 неэквивалентны). Остальное доказывается аналогично.

Между тем существует автомат Мили A′ (его граф изображен на рис. 4.1.2), который функционирует так же, как А, т. е. удовлетворяет требованиям 1)—3) и, однако, имеет меньше состояний, чем автомат А.

Автомат A′ имеет два состояния, которые могут служить начальными в смысле требования 2): z_0' и z_1'.

Используя автомат A′, также можно по состоянию, в которое этот автомат переходит после введения входной последовательности длины 2k, определить, соответствует ли выходная последовательность сумме a+b или a+b—2^k: если финальным является состояние z_0' или z_1', то вычислено выражение a+b, если же нет, то a+b—2^k.

Отметим, что A′ не эквивалентен никакому доопределению автомата A (получающемуся при замене тире на символы 0 или 1) в смысле определения 2.3.1, поскольку иначе такое доопределение не могло бы быть сокращенным автоматом (на основании аналога теоремы 3.6.4 для автоматов Мили, см. упражнение 3.19).

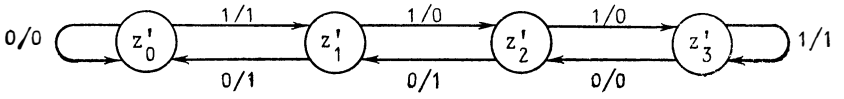


Рис. 4.1.2. Минимальный последовательностный сумматор A′ с попеременным вводом цифр слагаемых

Минимальность автомата A′, т. е. выполнение требования 4), мы докажем, показав, что любой автомат, удовлетворяющий требованиям 1)—3), должен иметь не менее четырех состояний. Пусть z_0 — начальное состояние автомата Мили B=(Z, X, Y, f, g), удовлетворяющего условиям 1)—3). Рассмотрим входные последовательности 1111, 0111 и 0110. Нам известны реакции автомата B, находящегося изначально в состоянии z_0, на эти последовательности: —0—1, —1—0 и —1—1 соответственно, где знак «—» означает, что на его месте может стоять и 0, и 1.

Пусть теперь $z_{i+1}=f(z_i, 1)$ при i=0, 1, 2. Тогда $g(z_1, 1)=0$ и $g(z_3, 1)=1$, т. е. $z_1 \neq z_3$. Если бы выполнялось равенство $z_0=z_2$, то мы бы имели $z_1=f(z_0, 1)=f(z_2, 1)=z_3$, а из $z_1=z_2$ следовало бы $z_1=z_2=f(z_1, 1)=f(z_2, 1)=z_3$. Итак, $z_0 \neq z_2$ и $z_1 \neq z_2$. Аналогично получаем $z_0 \neq z_1$. Таким образом, B имеет по меньшей мере три различных состояния: z_0, z_1 и z_2.

Пусть $z_4=f(z_0, 0)$. Тогда $g(z_4, 1)=1$, т. е. $z_4 \neq z_1$. Предположим, что $z_4=z_2$, так что $g(z_2, 1)=1$. Если бы также z_3 было равно z_2, то должно бы было выполняться равенство $z_3=f(z_2, 1)=f(z_3, 1)$, так что входная последовательность 0111 порождала бы последовательность состояний z_0, $z_4=z_2$, z_3, z_3 и выполнялось бы равенство $g(z_3, 1)=0$, что противоречит сказанному. Итак, равенство $z_3=z_2$ невозможно. Равным образом невозможно и равенство $z_3=z_0$, поскольку иначе входная последовательность 0110, порождающая последовательность состояний z_0, z_2, z_0, z_2, приводила бы к равенству $g(z_2, 0)=1$, а в то же время входная последовательность 00 — к $g(z_2, 0)=g(z_4, 0)=0$. Итак, если $z_4=z_2$, то состояния z_0, z_1, z_2, z_3 попарно различны.

Допустим, теперь, что $z_4=z_0$. Входные последовательности 00 и 0111 показывают, что тогда должно быть $g(z_0, 0)=0=g(z_2, 1)$, так что состояние z_3 должно отличаться не только от z_1, но и от z_2.

Далее, должно быть и $z_3 \neq z_0$, так как иначе входная последовательность 111001 приводила бы к неверной выходной последовательности 100001. Итак, снова состояния z_0, z_1, z_2, z_3 должны быть попарно различны.

Если, наконец, состояние z_4 отлично от всех состояний z_0, z_1 и z_2, то B снова имеет четыре различных состояния.

АНАЛИЗАТОР СИНТАКСИСА

Пример 4.1.2. Требуется построить автомат, с помощью которого для слова w из F({a, b}) можно установить, имеет ли это слово вид a^ib^j, где $j > i \geqslant 0$.

С этой целью будем считать, что множество слов $M = \{a^ib^j \mid i, j \in \mathbf{N}_0,\ j > i \geqslant 0\}$ описано с помощью металингвистических формул в форме Бэкуса — Наура (у читателя предполагается умение обращаться с этой конструкцией — см. введение к разд. 3.1):

1. ⟨слово⟩ : : = ⟨левое слово⟩⟨правое слово⟩
2. ⟨левое слово⟩ : : = Λ
3. ⟨левое слово⟩ : : = a⟨левое слово⟩b
4. ⟨правое слово⟩ : : = b
5. ⟨правое слово⟩ : : = ⟨правое слово⟩b.

Например, слова b и aabbbb получаются следующим образом:

⟨слово⟩ : : = ⟨левое слово⟩⟨правое слово⟩ : : = ⟨левое слово⟩ b : : = b

⟨слово⟩ : : = ⟨левое слово⟩⟨правое слово⟩ : : = ⟨левое слово⟩⟨правое слово⟩ b : : = ⟨левое слово⟩ bb : : = a⟨левое слово⟩ bbb : : = aa⟨левое слово⟩bbbb : : = aabbbb.

Легко видеть, что каждое слово из M получается однозначным образом, если расписывать формулу 1, заменяя самую правую металингвистическую переменную в соответствии с формулами 2—5. Таким образом, каждому слову w из M отвечает в точности одна правосторонняя расшифровка формулы 1 (в смысле примера 3.1.1). Очевидно, что и каждая правосторонняя расшифровка формулы 1 порождает некоторое слово из M. Чтобы определить, является некоторое слово w над {a, b} словом из M, можно, таким образом, пытаться построить порождающую слово w правостороннюю расшифровку формулы 1 (в обратном порядке).

Ради простоты введем следующие сокращенные обозначения металингвистических переменных: W — для ⟨слово⟩, L — для ⟨левое слово⟩, R — для ⟨правое слово⟩.

Теперь задача может быть поставлена таким образом: требуется построить автомат A, который при введении в него слова v из F({a, b, W, L, R}), причем правый конец слова отмечается особым знаком &, т. е. при введении v&, прочитывает это слово слева направо и устанавливает, получено ли оно в результате правосторонней расшифровки из некоторого другого слова v′; если это действительно так, то автомат A должен выдавать номер формулы, применение которой порождает из v′ слово v; в противном случае на выходе должен появляться сигнал ошибки (f); если на

вход подается слово W (односимвольное), то A должен порождать выход 0. Итак, автомат A должен, просматривая входную последовательность слева направо, находить первое вхождение в нее следующих «ключевых подслов»: b, Lb, ab, aLb, Rb, LR&, W.

Процесс анализа с использованием автомата A протекает следующим образом. В A вводится исследуемое слово w&. Если автомат A выдает число i, $1 \leqslant i \leqslant 5$, то в слове w производится изменение, соответствующее применению i-й формулы, и получившееся слово w′ снова вводится в A. Процесс продолжается до тех пор, пока не появится выход f (тогда w не является словом из M) или выход 0 (тогда $w \in M$).

Если, скажем, w=aabbbb, то автомат A должен прочитать начальный отрезок aab этого слова и установить, что может быть «в обратном направлении» (слева от первого b) применена формула 2, так что w′=aaLbbbb.

Чтобы учесть, что после выдачи номера некоторой формулы в автомат всегда должно быть введено новое (измененное) слово, используется «состояние покоя» r, в которое автомат может перейти из любого другого состояния и из которого он переходит в начальное состояние только при появлении специального входа (знака «+»).

Остальные состояния автомата A опишем следующим образом (здесь v& — подходящее входное слово).

z_0: Начальное состояние. Если v=W, то порождается выход 0. Если слово v начинается с символа b, то это слово должно быть с использованием формулы 2 преобразовано в слово Lv, т. е. порождается выход 2. Если $v=\Lambda$, то анализируемое слово не принадлежит M, т. е. порождается выход f.

z_1: Слово v начинается с по меньшей мере одного символа a. Во входной последовательности должно быть найдено первое вхождение символа b или символа L. Если $v=a^ibu$, то это слово может получиться из слова $v'=a^iLbu$ и на выходе должно появиться 2. Если $v=a^i$, то анализируемое слово не принадлежит M, выход равен f.

z_2: Известно, что $v=a^iLu$. Тогда должно быть выполнено равенство $v=a^iLbu'$, а слово v может быть получено из $v'=a^{i-1}Lu'$ с помощью формулы 3.

z_3: Должно быть v=Lbu, при этом v может быть получено из v′=LRu с помощью формулы 4.

z_4: v=LRu. Если u начинается с символа b, то v получается с помощью формулы 5, если $u=\Lambda$, т. е. v&=LR&, то выход равен 1.

Очевидно, нам не нужно для каждого состояния и каждого входного символа задавать, каким образом должен реагировать автомат A, так как определенные комбинации при правильном использовании A встретиться не могут. Если в некотором состоянии автомат получает на вход не рассмотренный выше символ, то можно считать, что произошла ошибка; чтобы доопределить A,

можно заставить его подавать на выход f и переходить в таких случаях в состояние r.

Заметим, однако, что при определенных входах (например, при входе R) не может быть порожден никакой выход — он должен быть тогда некоторым новым символом. Так что автомат не может быть доопределен так же, как автомат из примера 4.1.1.

Граф автомата A изображен на рис. 4.1.3, на котором показаны только представляющие интерес входы и выходы.

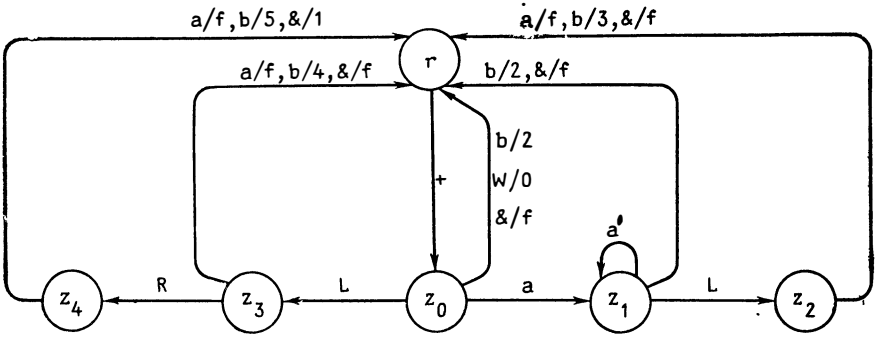


Рис. 4.1.3. Граф автомата A

ДЕКОДЕР

Пример 4.1.3. Требуется построить декодер для следующего кодирования: $h(a)=0$, $h(b)=11$, $h(c)=2$, $h(d)=10$, $h(e)=121$.

Если B и C — два алфавита, то, как известно, кодирование h есть инъективный гомоморфизм $h: F^+(B) \to F^+(C)$ [т. е. отображение со свойствами $h(u)=h(v)$ тогда и только тогда, когда $u=v$ и $h(uv)=h(u)h(v)$ для всех u и v из $F^+(B)$; из последнего свойства вытекает, что всегда достаточно определять h только на алфавите B].

Итак, искомый автомат должен для каждого слова w из $F^+(\{0, 1, 2\})$ вычислять его прообраз $h^{-1}(w)$.

Для того чтобы построить A, рассмотрим сначала так называемое кодовое дерево для h (рис. 4.1.4).

Этот граф преобразовывается в граф автомата A, причем идущие к листьям (т. е. к обозначенным символами a, b, c, d, e вершинам) стрелки направляются в корень, метки на листьях используются как выходные символы. Таким образом получается граф автомата A, изображенный на рис. 4.1.5.

Отметим, что доопределение автомата A не может быть проведено таким же образом, как в примерах 4.1.1 или 4.1.2, так как, с одной стороны, при переходах из z_0 в z_1 и из z_1 в z_2 ничего не должно появляться на выходе (или же некоторый новый символ n) и, с другой стороны, вход 0 или 2 для автомата, находящегося в состоянии z_2, не может приводить к переходу в z_0. (Если же мы хотим определить, что должно происходить в такой ситуации, нам следует ввести новое состояние z_3, в которое автомат пе-

реходит из z_2 при входах 0 и 2 и в котором остается, выдавая сигнал ошибки f.) Только так можно получить доопределение автомата A, граф которого изображен на рис. 4.1.6.

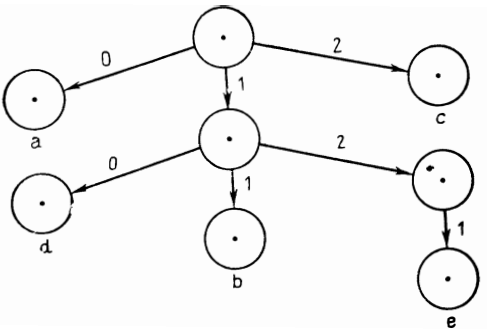


Рис. 4.1.4. Кодовое дерево для h

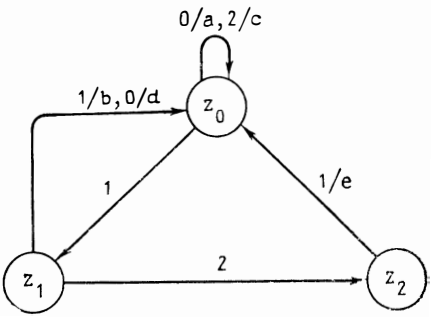


Рис. 4.1.5. Граф декодера

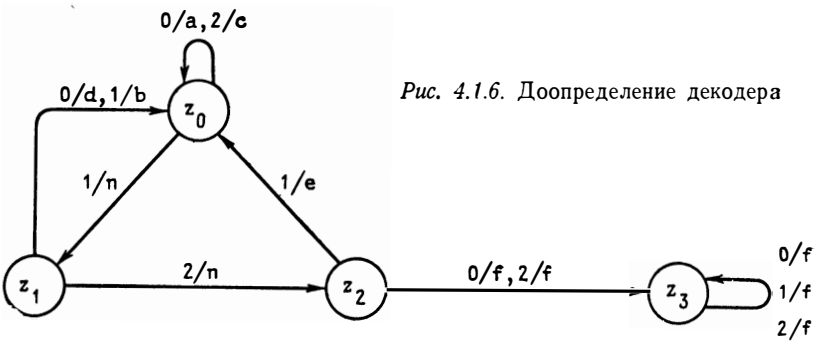


Рис. 4.1.6. Доопределение декодера

Замечание. При технической реализации автоматов Мили или Мура используются обычно входы и выходы 0 и 1 и память с двумя различными состояниями. В таком случае приходится представлять входы, выходы и состояния упорядоченными наборами из k, m и соответственно n нулей и единиц, причем в лучшем случае $2^{k-1} < |X| \leqslant 2^k$, $2^{m-1} < |Y| \leqslant 2^m$ и $2^{n-1} < |Z| \leqslant 2^n$. Поскольку при этом потенциально возможны все входы, представленные последовательностями из нулей и единиц длины k, все выходы, представленные последовательностями длины m, и могут использоваться n ячеек памяти с двумя состояниями, то такая реализация оказывается, вообще говоря, частичным автоматом. Действительно, здесь не встречаются определенные входные и выходные комбинации и определенные состояния (если $|X|$, $|Y|$ и $|Z|$ не являются степенями двойки).

Для более глубокого понимания и в качестве дополнения читателю рекомендуется выполнить связанные с примерами 4.1.1—4.1.3 упражнения 4.1—4.3 и упражнение 4.4. Важным дополнением упражнения 4.3 является упражнение 4.5.

4.2. ОПРЕДЕЛЕНИЕ, РАЗЛИЧНЫЕ ПОНЯТИЯ РЕАКЦИИ И ЭКВИВАЛЕНТНОСТИ, СОВМЕСТНОСТЬ

Чтобы иметь возможность рассматривать упомянутые в разд. 4.1 проблемы, нужно формализовать понятие не полностью определенного автомата (часто коротко называемого частичным автоматом) и определить, что понимается под его поведением.

ОПРЕДЕЛЕНИЕ ЧАСТИЧНОГО АВТОМАТА МИЛИ И ПОДАВТОМАТОВ

Пусть h — частичное (т. е. не всюду определенное) отображение множества U в множество V; тогда используется запись $h: (U) \dashrightarrow V$.

D(h) или, короче, D_h обозначает область определенности отображения h.

Определение 4.2.1. *Частичным автоматом Мили* называется пятерка $A = (Z, X, Y, f, g)$, где Z, X и Y — конечные множества (как в определении 2.2.1), называемые множествами *состояний, входов* и *выходов* соответственно, а f и g — *частичные отображения* из $Z \times X$ в Z и Y соответственно. При этом должны выполняться равенства

$$pr_1(gr\, f) \cup pr_3(gr\, f) \cup pr_1(gr\, g) = Z;$$

$$pr_2(gr\, f) \cup pr_2(gr\, g) = X \text{ и } pr_3(gr\, g) = Y.$$

Как и в случае автоматов Мили, f называется *функцией переходов*, а g — *функцией выходов.*

Ограничения на графики функций f и g должны гарантировать, что у автомата нет заведомо избыточных состояний, входов и выходов.

Следствие 4.2.2. Каждый автомат Мили (в смысле определения 2.2.1) является также частичным автоматом Мили (в смысле определения 4.2.1), а каждый частичный автомат Мили, имеющий всюду определенные функции переходов и выходов, является автоматом Мили.

Автоматы Мили при необходимости отличать их от частичных автоматов Мили будут именоваться иногда полностью определенными автоматами Мили.

Замечание. Множества D_f и D_g для некоторого частичного автомата Мили могут быть, вообще говоря, различны. Если пара (z, x) принадлежит D_f, но не D_g, то это означает, что, хотя вход x вызывает переход автомата из состояния z в некоторое (иное) состояние, при этом не возникает никакой выход или выход может быть произвольным. Если, напротив, пара (z, x) принадлежит D_g, но не D_f, то вход x для автомата, находящегося в состоянии z, приводит к появлению определенного выхода, но не определяет перехода в следующее состояние.

Пример 4.2.3. Автомат A из примера 4.1.1 описывается с использованием определения 4.2.1 следующим образом:

$A=(\{z_0, z_1, z_2, z_3, z_4\}, \{0, 1\}, \{0, 1\}, f, g)$,

где $D_f=\{z_0, ..., z_4\}\times\{0, 1\}$, $D_g=\{z_1, z_3, z_4\}\times\{0, 1\}$,

а отображения f и g задаются таблицей (рис. 4.2.1), в которой не определенные выходы обозначены, как и ранее, тире.

Замечание. Из примеров 4.1.1—4.1.3 легко понять, как частичные автоматы Мили могут быть описаны графами и таблицами. Как и в случае автоматов Мили, для частичных автоматов Мили также можно использовать переходно-выходные матрицы.

	z_0	z_1	z_2	z_3	z_4
0	$z_1/-$	$z_0/0$	$z_4/-$	$z_2/0$	$z_0/1$
1	$z_4/-$	$z_0/1$	$z_3/-$	$z_2/1$	$z_2/0$

Рис. 4.2.1. Таблица последовательностного сумматора A из разд. 4.1

Анализ примеров приводит к следующей конструкции.

Лемма 4.2.4. Для каждого частичного автомата Мили $A=(Z, X, Y, f, g)$ существует частичный автомат Мили $A'=(Z', X, Y, f', g')$ такой, что:

1) $D_g=D_{g'}\subseteq D_{f'}$;

2) $Z'=Z\cup z'$, $z'\notin Z$, $f'/Z=f$, $g'/Z=g$.

Доказательство. Полагаем $f'(z, x)=z'$ для всех (z, x) из D_g-D_f. ■

Замечание. 1. Условие 1) леммы может быть усилено до $D_{f'}=Z'\times X$ — достаточно просто положить $f'(z, x)=z'$ для всех (z, x) из $Z'\times X-D_f$.

2. В то же время не всегда целесообразно расширять D_g, скажем, используя новый дополнительный выход (см. пример 4.1.1).

Конструкция, использованная в лемме, приводит к следующему определению.

Определение 4.2.5. Пусть автомат A задан, как в определении 4.2.1. Частичный автомат Мили $A'=(Z', X, Y', f', g')$ называется *подавтоматом* автомата A, если $Z'\subseteq Z$, $Y'\subseteq Y$, $\mathrm{gr}\, f'=\mathrm{gr}\, f\cap(Z'\times X\times Z')$ и $\mathrm{gr}\, g'=\mathrm{gr}\, g\cap(Z'\times X\times Y')$.

Лемма 4.2.6. Каждое подмножество[1] Z' множества состояний Z частичного автомата Мили A однозначно определяет подавтомат автомата A, имеющий множество Z' в качестве множества состояний.

Доказательство. Пусть $A=(Z, X, Y, f, g)$, $Z'\subseteq Z$. Положим $\mathrm{gr}\, f'=\mathrm{gr}\, f\cap(Z'\times X\times Z')$, $\mathrm{gr}\, g'=\mathrm{gr}\, g\cap(Z'\times X\times Y)$ и $Y'=\mathrm{pr}_3(\mathrm{gr}\, g')$. ■

---

[1] Непустое. — *Прим. перев.*

В отличие от случаев автоматов Мили и Мура, формальное описание реакции частичного автомата Мили на последовательность входов не лишено сложностей: здесь возможны многие существенно различные определения (каждое из которых полезно при соответствующем подходе), причем эти определения оказываются равносильными для случая полностью определенных автоматов (см. упражнение 2.10).

Замечание. В дальнейшем всегда будем считать, что A — частичный автомат Мили в смысле определения 4.2.1.

Определение 4.2.7. 1. Частичное отображение $f^*: (Z \times F(X)) \dashrightarrow Z$ — это отображение, определяемое условиями:

$f^*(z, \Lambda) = z$ для всех z из Z;

$f^*(z, wx) = f(f^*(z, w), x)$ тогда и только тогда, когда определены $f^*(z, w) = z'$ и $f(z', x)$,— для всех z из Z, всех x из X и всех w из $F(X)$.

2. Для определения расширения функции выходов существуют три возможности.

1) $g^*: (Z \times F(X)) \dashrightarrow F(Y)$ определяется условиями:

$g^*(z, \Lambda) = \Lambda$ для всех z из Z;

$g^*(z, wx) = g^*(z, w)\, g(f^*(z, w), x)$ тогда и только, когда определены $g^*(z, w)$, $f^*(z, w)$ и $g(f^*(z, w), x)$,— для всех z из Z, всех x из X и всех w из $F(X)$.

Реакцией состояния z (для любого z из Z) называется частичное отображение $g_z: (F(X)) \dashrightarrow F(Y)$, где $g_z(w) = g^*(z, w)$.

2) Пусть $\bar{Y} = Y \cup \{-\}$, где $- \notin Y$. Тогда $\bar{g}^*: (Z \times F(X)) \dashrightarrow F(\bar{Y})$ — это отображение, определяемое условиями:

$\bar{g}^*(z, \Lambda) = \Lambda$ для всех z из Z;

$\bar{g}^*(z, x) = g(z, x)$ для всех (z, x) из D_g;

$\bar{g}^*(z, x) = -$ для всех (z, x) из $Z \times X - D_g$;

$\bar{g}^*(z, wx) = \bar{g}^*(z, w)\, \bar{g}^*(f^*(z, w), x)$ тогда и только тогда, когда определено состояние $f^*(z, w)$[1],— для всех z из Z, всех x из X и всех w из $F(X)$.

Частичной реакцией (коротко: U-реакцией) состояния z называется частичное отображение $\bar{g}_z: (F(X)) \dashrightarrow F(\bar{Y})$, где $\bar{g}_z(w) = \bar{g}^*(z, w)$.

3) *Поведением* состояния z называется следующее частичное отображение $\widehat{g}_z: (F(X)) \dashrightarrow F(Y)$:

$\widehat{g}_z(\Lambda) = \Lambda$;

$\widehat{g}_z(x) = g(z, x)$ тогда и только тогда, когда определено $g(z, x)$,— для всех x из X,

$\widehat{g}_z(w) = g(f^*(z, w), x)$ тогда и только тогда, когда определены $f^*(z, w) = z'$ и $g(z', x)$,— для всех x из X и w из $F(X)$.

---

[1] Отметим, что тогда определено и слово $\bar{g}^*(z, w)$. — *Прим. перев.*

Замечание. Очевидно, что $D(\hat{f}^*) \subseteq D(\bar{g}^*)$ и $D(g^*) \subseteq D(\bar{g}^*)$. Равенство в обоих случаях[1] выполняется только тогда, когда автомат A полностью определен. Далее $D(g^*) = \{z, w) \mid \bar{g}^*(z, w) \in F(Y)\}$. Если $D_f \subseteq D_g$, то для любого z из Z имеем $D(g_z) = D(\hat{g}_z)$ и выполняется включение $D(\hat{f}^*) \subseteq D(g^*)$. Ясно, что утверждение теоремы 2.3.2 остается справедливым для частичных отображений $\hat{f}^*$, g^*, $\bar{g}^*$ и $\hat{g}_z$.

Понятие реакции не имеет смысла использовать при рассмотрении примеров из разд. 4.1. Его следует применять, если функции переходов и выходов обладают одинаковыми областями определенности (т. е. если $D_f = D_g$). Это условие выполняется всегда в тех случаях, когда «частичность» автомата вытекает из того, что определенные входы не могут встретиться при определенных состояниях автомата (см., например, упражнение 4.5).

Для примера 4.1.1 в наибольшей степени подходит понятие U-реакции, поскольку знак «—», введенный в определении U-реакции, может интерпретироваться так же, как и в примере 4.1.1: как знак резервирования места для произвольного выхода.

При рассмотрении примеров 4.1.2 и 4.1.3 наиболее разумно использовать понятие поведения.

Читателю рекомендуется еще раз рассмотреть упражнения 4.1—4.4 и выполнить упражнение 4.6, в котором вводится специальный тип частичных автоматов Мили.

L-, U- и V-эквивалентность

Для обобщения понятий эквивалентности состояний и автоматов существует несколько возможностей. Исходя из частичных отображений g_z, $\bar{g}_z$ и $\hat{g}_z$, получаем по аналогии с определением 2.3.1 три понятия эквивалентности, замечая, что два частичных отображения равны тогда и только тогда, когда совпадают их области определенности и совпадают значения, которые они принимают на этих областях.

Определение 4.2.8. Два состояния z и z′ автомата A называются L-эквивалентными, если $g_z = g_{z'}$, U-эквивалентными, если $\bar{g}_z = \bar{g}_{z'}$, и V-эквивалентными, если $\hat{g}_z = \hat{g}_{z'}$.

Замечание. Легко видеть, что отношения L-, U- и V-эквивалентности являются отношениями эквивалентности на множестве Z.

Теорема 4.2.9. 1. Два состояния частичного автомата Мили являются V-эквивалентными тогда и только тогда, когда они U-эквивалентны.

2. Из U-эквивалентности состояний частичного автомата Мили вытекает их L-эквивалентность. Обратное верно тогда и только

---

[1] Но не в каждом в отдельности. — *Прим. перев.*

тогда, когда область определенности функции переходов содержится в области определенности функции выходов.

Доказательство. Пусть z и z′ — состояния автомата A и $w=x_1x_2\ldots x_n$ — слово из $F(X)$, $n\geqslant 1$.

1. 1) Пусть состояния z и z′ — V-эквивалентны. Для $i=1,\ldots,n$ пусть $w_i=x_1\ldots x_i$. Тогда при $i=1,\ldots,n$ значения $\hat{g}_z(w_i)$ и $\hat{g}_{z'}(w_i)$ либо оба определены и равны, либо оба не определены. Пусть индексы $i_1, i_2, \ldots, i_k$ выбраны так, что значение $\hat{g}_z(w_j)$ определено в точности тогда, когда $j=i_m$ для некоторого m при $1\leqslant m\leqslant k$.

Тогда $\bar{g}_z(w)=y_1\ldots y_n$, причем $y_{i_m}=\hat{g}_z(w_{i_m})$ для $m=1,\ldots,k$ и $y_i=-$ в остальных случаях. То же имеем и для $\bar{g}_{z'}(w)$. Итак, $\bar{g}_z(w)=\bar{g}_{z'}(w)$.

2) Пусть состояния z и z′ — U-эквивалентны. Если $\eta_1(\bar{g}_z(w))\in Y$ (η_1 — окончание длины 1, см. определение 2.6.6), то $\hat{g}_z(w)=\eta_1(\bar{g}_z(w))=\eta_1(\bar{g}_{z'}(w))=\hat{g}_{z'}(w)$. В противном случае $\hat{g}_z$ и $\hat{g}_{z'}$ не определены.

2. 1) Если состояния z и z′ U-эквивалентны и определено значение $g^*(z, w)$, то

$$g^*(z, w)=\bar{g}^*(z, w)=\bar{g}^*(z', w)=g^*(z', w).$$

2) Пусть $D_f\subseteq D_g$ и $g_z=g_{z'}$. Из замечания к определению 4.2.7 в таком случае следует $D(\hat{g}_z)=D(g_z)=D(g_{z'})=D(\hat{g}_{z'})$. Далее $\hat{g}_z(w)=\eta_1(g_z(w))=\eta_1(g_{z'}(w))=\hat{g}_{z'}(w)$, откуда с учетом п.1 получаем нужное утверждение.

3) Рассмотрим частичный автомат Мили

$B=(\{z_1, z_2, z_3\}, \{0, 1\}, \{0, 1\}, f, g)$ с $f(z_1, 1)=z_2$, $f(z_i, 0)=f(z_2, 1)=z_3$ при $i=1,2$, $g(z_i, 0)=0$ при $i=1,2,3$. У этого автомата состояния z_1 и z_2 L-эквивалентны, но не U-эквивалентны[1]. ▫

Следствие 4.2.10. Два состояния полностью определенного автомата Мили L-эквивалентны (т. е. эквивалентны в смысле определения 2.3.1) тогда и только тогда, когда они V-эквивалентны.

СОВМЕСТИМОСТЬ СОСТОЯНИЙ

Из анализа примера 4.1.1 вытекает разумность обобщения понятия U-эквивалентности, при котором допускается, чтобы выделенному знаку «—» сопоставлялись различные выходы.

---

[1] Доказано на самом деле следующее утверждение: если область определенности функции переходов некоторого частичного автомата Мили не содержится в области определенности функции выходов, то из L-эквивалентности состояний не вытекает, вообще говоря, их U-эквивалентность. — *Прим. перев.*

Определение 4.2.11. 1. Пусть множество $\bar{Y}$ задано как в 4.2.7, п.2, 2). Отношение $\sim$ (совместность) определяется на $F(Y)$ следующим образом:

1) $\Lambda \sim \Lambda$, $y \sim -$ и $- \sim y$ для всех y из $\bar{Y}$.

2) Для всех w и w' из $F(\bar{Y})$ соотношение $w \sim w'$ выполняется тогда и только тогда, когда существуют u и u' в $F(\bar{Y})$, а также y и y' в $\bar{Y}$ такие, что $w = uy$, $w' = u'y'$, $u \sim u'$ и $y \sim y'$.

2. Пусть A — частичный автомат Мили в обычных обозначениях. Два состояния z и z' этого автомата называются *совместными*, если для всех w из $D(\bar{g}_z) \cap D(\bar{g}_{z'})$ имеет место соотношение $\bar{g}_z(w) \sim \bar{g}_{z'}(w)$.

Замечание. Отметим, что отношение совместности (как на $F(\bar{Y})$, так и на Z) не является отношением эквивалентности, поскольку, например, $a—b \sim aab$ и $a—b \sim abb$, но при $a \neq b$ не выполнено $aab \sim abb$.

Следствие 4.2.12. 1. Если состояния z и z' совместны и пары (z, x) и (z', x) принадлежат D_f, то и состояния $f(z, x)$ и $f(z', x)$ совместны.

2. Состояния z и z' совместны тогда и только тогда, когда $\hat{g}_z(w) = \hat{g}_{z'}(w)$ для всех w из $D(\hat{g}_z) \cap D(\hat{g}_{z'})$.

3. U- или L-эквивалентные состояния совместны. Поэтому для полностью определенных частичных автоматов Мили понятия эквивалентности и совместности совпадают.

Доказательство. 1. Пусть $z_1 = f(z, x)$, $z_2 = f(z', x)$ и w — слово из $D(\bar{g}_{z_1}) \cap D(\bar{g}_{z_2})$. По предположению $xw \in D(\bar{g}_z) \cap D(\bar{g}_{z'})$ и существуют y и y' в $\bar{Y}$ такие, что $y \sim y'$ и $yg_{z_1}(\bar{w}) = \bar{g}_z(xw) \sim \sim \bar{g}_{z'}(xw) = y'\bar{g}_{z_2}(w)$.

2. Утверждение 2 вытекает из доказательства теоремы 4.2.9.

3. Утверждение 3 очевидно.■

Пример 4.2.13. В автомате A из примера 4.1.1 состояния z_0 и z_1 совместны, поскольку для всех x из $\{0, 1\}$ и всех w из $F(\{0, 1\})$ выполняется равенство $\bar{g}^*(z_1, xw) = x\bar{g}^*(z_0, w)$, а знак «—» стоит в $\bar{g}^*(z_1, xw)$ в точности на $(2i)$-х местах, а в $\bar{g}^*(z_0, w)$ — на $(2i-1)$-х $(i = 1, 2, \ldots)$.

В то же время состояния z_0 и z_1 не являются ни L-, ни U-эквивалентными, что сразу видно из рассмотрения, проведенного в разд. 4.1.

В разд. 4.3 будет показано, что вопрос о том, можно ли за конечное число шагов установить, являются ли два состояния некоторого частичного автомата Мили L- либо U-эквивалентными, может быть решен простым сведением к соответствующему вопросу для автоматов Мили (см. теорему 2.3.3).

Каким образом может быть решен вопрос о совместности состояний (за конечное число шагов), видно из доказательства сле-

дующей теоремы. Полученная при этом граница точна (см. упражнение 4.8). Другие методы содержатся в упражнениях 4.9 и 4.10.

Теорема 4.2.14 (Гинзбург). Два состояния z и z′ частичного автомата Мили с n состояниями совместны уже тогда, когда для всех слов w из F(X) длины, не превышающей $\frac{1}{2}n(n-1)$, выполнено: $\bar{g}_z(w) \sim \bar{g}_{z'}(w)$. Таким образом, проблема совместности состояний разрешима.

Доказательство. Будем вести доказательство данной теоремы так же, как и теоремы 2.3.3. Вместо отношения k-эквивалентности введем отношение k-совместности. Поскольку отношение совместности не является отношением эквивалентности, мы можем рассматривать не «классы совместных состояний», но только лишь множество всех неупорядоченных пар k-совместных состояний. Пусть A — частичный автомат Мили и k — неотрицательное целое число. Два состояния z и z′ автомата A будем называть k-совместными (обозначение: $z \underset{k}{\sim} z'$), если $\bar{g}_z(w) \sim \bar{g}_{z'}(w)$ для всех слов w из пересечения $D(\bar{g}_z) \cap D(\bar{g}_{z'})$ таких, что $|w| \leqslant k$.

Пусть V_k — множество всех неупорядоченных пар k-совместных состояний автомата A. Тогда V_0 является множеством всех двухэлементных подмножеств множества Z, так что $|V_0| = \frac{1}{2}n(n-1)$.

Из определения вытекает, что $V_{k+1} \subseteq V_k$ при любом k.

Множество $\{z_1', z_2'\}$ из V_0 будем называть последующим для $\{z_1, z_2\}$, если $\{z_1, z_2\} \neq \{z_1', z_2'\}$ и существует x в X такое, что $f(z_i, x) = z_i'$ при $i = 1, 2$.

Промежуточное утверждение 1. При $k \geqslant 1$ множество V_{k+1} является множеством элементов из V_k таких, что их последующие множества также принадлежат V_k.

Доказательство. а) Пусть $\{z_1, z_2\}$ — пара из V_k, причем такая, что все ее последующие множества также лежат в V_k. Пусть, далее, x — вход из X и $w = xu$ — слово из $X^{k+1} \cap D(\bar{g}_{z_1}) \cap D(\bar{g}_{z_2})$. Так как $z_1 \underset{k}{\sim} z_2$, выполнено $\bar{g}(z_1, x) \sim g(z_2, x)$. Если $f(z_1, x) = f(z_2, x)$, то, конечно, $\bar{g}^*(z_1, w) \sim \bar{g}^*(z_2, w)$. В противном случае по предположению $f(z_1, x) \underset{k}{\sim} f(z_2, x)$, так что, в частности, $\bar{g}^*(f(z_1, x), u) \sim \bar{g}^*(f(z_2, x), u)$ и $\bar{g}^*(z_1, w) \sim \bar{g}^*(z_2, w)$. Итак, пара $\{z_1, z_2\}$ принадлежит V_{k+1}.

б) Пусть $\{z_1, z_2\}$ — пара из V_{k+1}. Тогда, очевидно, при каждом x из X таком, что состояния $f(z_1, x)$ и $f(z_2, x)$ оба определены и различны, пара $\{f(z_1, x), f(z_2, x)\}$ принадлежит V_k.

Промежуточноее утверждение 2. Если при некотором k имеем $V_k = V_{k+1}$, то при всех i также $V_{k+i} = V_k$.

Доказательство. Доказательство получается из промежуточного утверждения 1 применением полной индукции по i, поскольку в этом случае V_{k+i+1} оказывается множеством элементов из $V_{k+i} (= V_k)$ таких, что их последующие множества принадлежат $V_{k+i} (= V_k)$.

Промежуточное утверждение 3. Если для всех i из N выполняется равенство $V_k = V_{k+i}$, то любые два состояния z и z′ из V_k совместны.

Доказательство. Если z и z′ — состояния из V_k, то при всех i из $\mathbf{N}_0$ имеет место $z \underset{k+1}{\sim} z'$. Отсюда вытекает, что $z \underset{n}{\sim} z'$ при всех n из **N**.

Поскольку, как следует из промежуточного утверждения 1, имеется цепочка включений $V_0 \supseteq V_1 \supseteq V_2 \supseteq \ldots$, то при $k_0 = |V_0|$, очевидно, $V_{k_0} = V_{k_0+i}$ для всех i из **N**. Чтобы установить, являются ли два состояния совместными, нужно, таким образом, только проверить, лежат ли эти состояния в одном элементе множества V_{k_0}■

Замечание. Понятие совместности состояний без труда может быть перенесено на состояния различных частичных автоматов Мили, если только оба таких автомата имеют одинаковые множества входов и выходов. А именно, пусть $A = (Z, X, Y, f, g)$ и $A' = (Z', X, Y, f', g')$ — два частичных автомата Мили, причем $Z \cap Z' = \varnothing$. Состояние z автомата A совместно с состоянием z′ автомата A′ тогда и только тогда, когда эти состояния оказываются совместными, если рассматривать их как состояния «объединенного» частичного автомата $A'' = (Z \cup Z', X, Y, f'', g'')$ такого, что $f''/Z \times X = f$, $f''/Z' \times X = f'$, $g''/Z \times X = g$ и $g''/Z' \times X = g'$.

4.3. ДООПРЕДЕЛЕНИЕ И СОКРАЩЕНИЕ

В этом разделе переносятся на случай частичных автоматов Мили понятия эквивалентности и сокращенности автоматов Мили (см. разд. 2.3), понятия гомоморфизма, изоморфизма и минимальности автоматов Мура (см. разд. 3.6) и соответствующие теоремы.

U-РЕАКЦИЯ, U-ГОМОМОРФИЗМ

Поскольку понятие реакции уже, чем понятие U-реакции и поведения, мы ограничимся при рассмотрении частичных автоматов Мили только изучением их U-реакций. Аналогичные результаты для реакции (и поведения) легко получить с помощью несложных модификаций приведенных ниже построений (см. упражнение 4.11).

Для входно-выходного поведения частичных автоматов Мили оказываются существенными (релевантными) только такие состояния, которые по меньшей мере при одной входной последовательности приводят к появлению выхода из множества Y.

Определение 4.3.1. Пусть A — частичный автомат Мили в обычных обозначениях. Состояние z автомата A называется *релевантным*, если в F(X) существует слово w такое, что $\hat{g}_z(w) \in Y$.

Множество всех релевантных состояний автомата A будем обозначать Z^r.

Однозначно определенный **множеством Z^r (по лемме 4.2.6)** подавтомат $A^r = (Z^r, X, Y, f^r, g^r)$ автомата A называется *релевантным подавтоматом автомата A*.

Замечание. Если выполняется включение $pr_1(gr\, f) \cup \cup pr_3(gr\, f) \subseteq pr_1(gr\, g)$, то $A = A^r$.

При перенесении этих понятий на случай автоматов Мили будем учитывать только релевантные состояния и релевантные подавтоматы.

Определение 4.3.2. 1. *U-реакцией* частичного автомата Мили A называется множество U-реакций его релевантных состояний.

2. Два частичных автомата Мили A и A′ называются *U-эквивалентными* (обозначение: $A \equiv A'$), если их U-реакции равны.

3. Частичный автомат Мили называется *U-сокращенным*, если все его состояния релевантны и попарно не U-эквивалентны.

4. Частичный автомат Мили A называется *U-минимальным*, если не существует U-эквивалентного A частичного автомата Мили с меньшим числом состояний.

Замечания. 1. Частичный автомат Мили A и его релевантный подавтомат A^r всегда имеют равные U-реакции, т. е. всегда $A \equiv A^r$.

2. U-сокращенный (соответственно U-минимальный) частичный автомат Мили совпадает со своим релевантным подавтоматом.

При перенесении на случай частичных автоматов Мили понятия гомоморфизма также будем исходить из того, что интерес представляет только множество U-реакций релевантных состояний.

Определение 4.3.3. Пусть $A = (Z, X, Y, f, g)$ и $A' = (Z', X, Y, f', g')$ — частичные автоматы Мили.

1. Отображение h из Z^r в Z'^r называется *U-гомоморфизмом* из A в A′, если для всех z из Z^r и всех x из X выполнены следующие условия.

1) Состояние f(z, x) определено тогда и только тогда, когда определено состояние f′(h(z), x). Если определено состояние f(z, x), то h(f(z, x)) = f′(h(z), x).

2) Выход g(z, x) определен тогда и только тогда, когда определен выход g′(h(z), x). Если определен выход g(z, x), то g(z, x) = g′(h(z), x).

Если отображение h является, кроме того, сюръективным, то h называется *U-эпиморфизмом* A на A′, а A′ — *U-гомоморфным образом* A (обозначение: $A \overset{h}{\twoheadrightarrow} A'$).

2. Инъективный U-эпиморфизм A на A′ называется *U-изоморфизмом* A на A′. Если существует U-изоморфизм A на A′, то автоматы A и A′ называются *U-изоморфными* (обозначение: $A \simeq A'$).

3. A называется *U-гомоморфно сокращенным*, если каждый U-эпиморфизм из A оказывается U-изоморфизмом и $A = A^r$.

Замечание. Для полностью определенных частичных автоматов Мили понятия U-эпиморфизма (U-изоморфизма) и Z-эпиморфизма (Z-изоморфизма) совпадают (см. разд. 3.6).

Лемма 4.3.4. 1. Если h есть U-изоморфизм A на A′, то h^{-1} есть U-изоморфизм A′ на A.

2. Если $A \rightsquigarrow A'$, то для любого релевантного состояния z автомата A выполняется равенство $\bar{g}_z = \bar{g}_{h(z)}$, так что, в частности, $A \equiv A'$.

3. Любой U-минимальный частичный автомат Мили является U-гомоморфно сокращенным.

4. Любой U-сокращенный частичный автомат Мили является U-минимальным.

Доказательство. Утверждения 1 и 2 вытекают непосредственно из определений.

3. Пусть A есть U-минимальный, но не U-гомоморфно сокращенный автомат. Тогда должен существовать автомат A′ такой, что $A' \not\rightsquigarrow A$ и $A \rightsquigarrow A'$. При этом автомат A′ должен иметь меньше состояний, чем A, а по утверждению 2 должно выполняться соотношение $A \equiv A'$. Это противоречит предположению о U-минимальности автомата A.

4. Пусть A есть U-сокращенный, но не U-минимальный автомат. Тогда должен существовать автомат A′ с меньшим, чем у A, числом состояний, такой что $A \equiv A'$. Поэтому по меньшей мере два состояния автомата A должны иметь равные U-реакции (совпадающие с реакцией одного из состояний автомата A′). Противоречие! ■

ПРОБЛЕМА U-МИНИМИЗАЦИИ, ДООПРЕДЕЛЕНИЕ

Будем рассматривать следующую проблему. Пусть задан некоторый частичный автомат Мили A. Спрашивается:

1. Существует ли а) U-сокращенный частичный автомат Мили A_r такой, что $A_r \equiv A$; б) U-гомоморфно сокращенный частичный автомат Мили A_h такой, что $A_h \equiv A$; в) U-минимальный частичный автомат Мили A_m такой, что $A_m \equiv A$?

2. Определены ли в случае их существования автоматы A_r, A_h и A_m однозначно и какие между ними существуют связи?

3. Существует ли алгоритм построения A_r, A_h и A_m?

Ответ на вопросы 1,б) и 1,в), очевидно, положителен. Действительно, множество всех U-эквивалентных автомату A не U-изоморфных частичных автоматов Мили с меньшим, чем у A, числом состояний конечно (поскольку конечно Z и фиксировано X).

Мы получим ниже положительные ответы на все вопросы. При этом мы (приблизительно так же, как в примере 4.1.3) частичному автомату Мили A будем однозначным образом сопоставлять полностью определенный частичный автомат Мили A^0 (т. е. просто автомат Мили), причем так, что будут сохраняться свойства U-сокращенности, U-гомоморфной сокращенности или U-минимальности. После этого будут использованы теорема об однозначности минимального автомата Мура и равносильность автоматов Мура и Мили.

Лемма 4.3.5. Для каждого частичного автомата Мили $A=(Z, X, Y, f, g)$ существует единственный полностью определенный частичный автомат Мили $A^0=(Z^0, X, Y, f^0, g^0)$ со следующими свойствами:

1) $Z^0=Z^r$, если $Z^r\times X\subseteq D_f$ и $f(z^r, X)\subseteq Z^r$; в противном случае $Z^0=Z^r\cup 0$, где $0\notin Z$;

2) $g^{0*}(z, w)=\bar{g}^*(z, w)$ для всех (z, w) из $D(\bar{g}^*)$;

3) $g^0(z, x)$ является элементом множества Y тогда и только тогда, когда пара (z, x) принадлежит D_g;

4) $f^{0*}(z, w)\in Z^r$ тогда и только тогда, когда $(z, w)\in D(f^*)$ и $f^*(z, w)\in Z^r$.

Автомат A^0 называется при этом 0-доопределением автомата A.

Доказательство. Для задания автомата A^0 должны быть определены лишь функции f^0 и g^0:

$$f^0(z, x)=\begin{cases} f(z, x), \text{ если } (z, x)\in D_f \text{ и } f(z, x)\in Z^r, \\ 0 \text{ в противном случае;}\end{cases}$$

$$g^0(z, x)=\begin{cases} \bar{g}(z, x), \text{ если } (z, x)\in D(\bar{g}), \\ — \text{ в противном случае.}\end{cases}$$

Легко видеть, что автомат A^0 полностью определен, условия 1)—4) выполнены и функции f^0 и g^0 не могут быть определены иначе, если требуется, чтобы автомат A^0 был определен полностью. ■

Пример 4.3.6. На рис. 4.1.6 изображен граф изоморфного образа $\bar{0}$-доопределения частичного автомата Мили, граф которого приведен на рис. 4.1.5 (нужно только заменить z_3 на 0 и f и n на —).

Следствие 4.3.7. 1. Каждый частичный автомат Мили U-изоморфен своему 0-доопределению.

2. Пусть A и B — частичные автоматы Мили и A^0 и B^0 — их $\bar{0}$-доопределения. В этом случае:

1) $A\tilde{\to}B$ тогда и только тогда, когда $A^0\tilde{\to}B^0$;

2) $A\approx B$ тогда и только тогда, когда $A^0\simeq B^0$;

3) $A\equiv B$ тогда и только тогда, когда $A^0\equiv B^0$;

4) автомат A является U-сокращенным тогда и только тогда, когда таковым является автомат A^0.

Лемма 4.3.8. Если A — частичный автомат Мили, $(A^0)_m$ (определенный однозначно с точностью до Z-изоморфизма) — эквивалентный автомату A^0 минимальный автомат Мили и A_m — некоторый U-минимальный U-эквивалентный автомату A частичный автомат Мили, то для $\bar{0}$-доопределения автомата A_m справедливо соотношение $(A_m)^0\simeq(A^0)_m$.

Доказательство. Из п.3 следствия 4.3.7 вытекают соотношения $(A^0)_m\equiv A^0\equiv(A_m)^0$. Поэтому из теоремы об однозначности минимального автомата (теорема 3.6.4) следует существование Z-гомоморфизма h $(A_m)^0$ на $(A^0)_m$. Пусть Z_m — множество состояний автомата A_m, B—определенный множеством $h(Z_m)$ подавтомат автомата $(A^0)_m$. Тогда $(A^0)_m\simeq B^0$ и $A_m\tilde{\to}B$, так что $A_m\equiv B$.

Из-за U-минимальности автомата A_m отсюда вытекает, что $A_m \simeq \simeq B$. Из п. 2) следствия 4.7.3 теперь получаем $(A^0)_m \simeq B^0 \simeq (A_m)^0$. ■

РЕШЕНИЕ ПРОБЛЕМЫ U-МИНИМИЗАЦИИ

Теперь мы можем получить ответы на поставленные выше вопросы.

Теорема 4.3.9 (теорема об U-сокращении). Для каждого частичного автомата Мили A существует единственный с точностью до U-изоморфизма U-эквивалентный U-минимальный частичный автомат Мили A_m. Этот автомат является U-сокращенным и U-гомоморфно сокращенным.

Каждый U-эквивалентный автомату A частичный автомат Мили, являющийся U-сокращенным или U-гомоморфно сокращенным, оказывается и U-минимальным.

Доказательство. Уже отмечалось, что для частичного автомата Мили A всегда существует U-эквивалентный автомату A U-минимальный частичный автомат Мили A_m. По лемме 4.3.8 $(A_m)^0 \simeq (A^0)_m$, так что по теореме 3.6.4 $(A_m)^0$ с точностью до U-изоморфизма определен однозначно. Отсюда (см. п. 2 следствия 4.3.7) вытекает, что и A_m определен с точностью до U-изоморфизма единственным образом. Из п.3 леммы 4.3.4 получаем, что A_m является также U-гомоморфно сокращенным. Поскольку по теореме 3.6.4 автомат $(A^0)_m$, а потому и U-изоморфный ему автомат $(A_m)^0$ является U-сокращенным, то A_m в силу п. 4 следствия 4.7.3 тоже U-сокращенный автомат.

Пусть, далее, B есть U-сокращенный (или U-гомоморфно сокращенный) U-эквивалентный автомату A частичный автомат Мили. Тогда из п. 4) [или 1)] следствия 4.3.7 получаем, что автомат $B^0 \equiv A^0$ является U-сокращенным (U-гомоморфно сокращенным). По теореме 3.6.4 и на основе вышесказанного $B^0 \simeq (A^0)_m \simeq (A_m)^0$ и потому из п. 2 следствия 4.7.3 вытекает, что $B \simeq A_m$. ■

Следствие 4.3.10. Пусть A — частичный автомат Мили, A_m — соответствующий U-минимальный автомат и B—U-эквивалентный автомату A частичный автомат Мили. Тогда существует U-эпиморфизм B на A_m.

Для доказательства следует заметить, что U-минимальный U-гомоморфный образ автомата B изоморфен A_m, а суперпозиция U-эпиморфизма и U-изоморфизма является U-эпиморфизмом.

Следствие 4.3.11. Следующий набор инструкций определяет алгоритм для нахождения U-минимального автомата, соответствующего автомату A (для любого частичного автомата Мили A).

1. Найти релевантные состояния автомата A.
2. Построить $\bar{0}$-доопределение A^0 автомата A.
3. Построить сокращенный автомат Мили $(A^0)_m$ из A^0, используя доказательство теоремы о сокращении (теорема 2.3.6).
4. Построить определенный множеством состояний Z_m автомата A_m подавтомат автомата $(A_m)^0 \simeq (A^0)_m$. Этот автомат — искомый.

Как показывает пример 4.1.1, когда ставится задача поиска частичного автомата Мили с наименьшим возможным числом состояний, решающего определенную задачу, построение U-минимального частичного автомата Мили может оказаться недостаточным. Действительно, частичный автомат Мили A (см. рис. 4.1.1) является U-минимальным, а автомат A′ (см. рис. 4.1.2) имеет меньше состояний, чем A, и потому не U-эквивалентен A. В примере 4.1.1 было, далее, показано, что не существует частичного автомата Мили, решающего рассмотренную в этом примере задачу и обладающего меньшим, чем автомат A′, числом состояний.

Ниже будет исследован вопрос о том, как могут быть охарактеризованы подобного рода минимальные автоматы, «решающие ту же задачу», при каких условиях они существуют, однозначно ли они определены, как они могут быть построены и так далее.

ПОНЯТИЕ ПОКРЫТИЯ, ПРОБЛЕМА МИНИМИЗАЦИИ

Для последующих рассуждений полезно отсутствие некоторого последующего состояния или выхода в описании конкретного автомата интерпретировать как «пропуск» соответствующих входов, поскольку они несущественны для задания способа функционирования данного автомата. Будем, кроме того, считать, что вместо отсутствующих состояний или выходов могут использоваться только имеющиеся в исходном описании состояния или выходы.

Рассматривая вопрос о соотношении между автоматами A и A′ из примера 4.1.1, нетрудно заметить, что для каждого состояния z_i автомата A существует по меньшей мере одно совместное с ним состояние z_j' автомата A′, поведение которого определено всюду, где определено поведение состояния z_i. Так, например, состояния z_0 и z_1 совместны с состоянием z_0' (см. также пример 4.2.13).

Сказанное оправдывает введение следующего определения.

Определение 4.4.1. Пусть $A=(Z, X, Y, f, g)$ и $A'=(Z', X, Y, f', g')$ — частичные автоматы Мили.

1. Состояние z' автомата A′ *покрывает* состояние z автомата A (обозначение: $z' \geqslant z$), если состояния z' и z совместны (ср. замечание в конце разд. 4.2) и $D(\widehat{g}_z) \subseteq D(\widehat{g}'_{z'})$.

2. Автомат A′ *покрывает* автомат A (обозначение: $A' \geqslant A$), если для каждого состояния z автомата A существует покрывающее его состояние z' автомата A′.

3. Автомат A′ называется *минимальным* для A, если $A' \geqslant A$ и любой покрывающий автомат A частичный автомат A″ имеет не меньше состояний, чем A′.

4. Автомат A′ называется *доопределением* автомата A, если он является автоматом Мили, $Z=Z'$, $\operatorname{gr} f \subseteq \operatorname{gr} f'$ и $\operatorname{gr} g \subseteq \operatorname{gr} g'$.

Итак, в примере 4.1.1 автомат A′ является минимальным для автомата A.

Разрешимость вопроса о том, покрывает ли одно состояние другое, требуется доказать в упражнении 4.12.

Отметим, что покрывающий автомат A частичный автомат Мили «в большей степени, чем A» реагирует на входы, т. е. порождает выходы, отличные от выходов автомата A (вообще говоря), в то время как U-эквивалентный частичный автомат Мили обладает в точности такой же реакцией, как и A.

Следствие 4.4.2. Пусть A и A′ полностью определенные частичные автоматы Мили. Тогда автомат A покрывает A′ в том и только в том случае, когда A и A′ эквивалентны.

Соответствующая проблеме минимизации числа состояний автоматов Мили (или Мура) проблема для частичных автоматов Мили (называемая просто *проблемой минимизации)* формулируется следующим образом.

1. Существует ли для каждого частичного автомата Мили минимальный?

2. Является ли минимальный автомат (если он существует) единственным?

3. Если вопрос 2 имеет отрицательный ответ, то как можно описать множество всех автоматов, минимальных для некоторого частичного автомата Мили (аналогично тому, как это было сделано в случае полностью определенных автоматов при помощи понятий гомоморфизма и изоморфизма)?

4. Существует ли алгоритм построения всех минимальных для некоторго частичного автомата Мили автоматов?

Следствие 4.4.3. Если существует частичный автомат Мили A′, минимальный для автомата A, то существует и полностью определенный частичный автомат Мили, минимальный для A.

Доказательство. Если, скажем, в A′ не определено состояние $f'(z', x)$ и состояние z' покрывает состояние z автомата A, то не определено и $f(z, x)$. Поэтому и любое доопределение автомата A′ будет покрывать автомат A. Поскольку такое доопределение имеет столько же состояний, сколько их у автомата A′, то оно равным образом будет автоматом, минимальным для A. ■

Замечание. При ответе на первый вопрос проблемы минимизации достаточно, таким образом, ограничиться рассмотрением только полностью определенных автоматов.

В противоположность результатам, полученным в разд. 4.3 и для полностью определенных автоматов, верна следующая теорема.

Теорема 4.4.4. Существуют частичные автоматы Мили A, которые обладают многими не U-эквивалентными минимальными автоматами, имеющими меньше состояний, чем соответствующие U-минимальные автоматы. Эти минимальные автоматы не могут быть найдены путем доопределения A и последующего сокращения на основе теоремы о сокращении.

В качестве доказательства рассмотрим следующий пример.

Пример 4.4.5. Пусть частичные автоматы Мили A, A′ и A″ определены таблицами, приведенными на рис. 4.4.1.

Автомат A является U-сокращенным, а по теореме об U-сокращении — и U-минимальным. Каждое доопределение этого автомата (выходы 0 или 1 при входе 1 в состоянии z_2) оказывается

сокращенным автоматом. Имеют место соотношения $A' \geqslant A$ и $A'' \geqslant A$. Автоматы A' и A'' не эквивалентны. Теорема тем самым доказана.

Отметим, что состояния z_1 и z_2, а также z_2 и z_3 совместны, но состояния z_1 и z_3 — нет. ■

Простым, но требующим большого перебора способом построения минимального автомата для данного частичного автомата Мили является так называемый метод *расщепления состояний*. Объясним его на примере автомата A из последнего доказатель-

A	z_1	z_2	z_3
0	$z_1/0$	$z_2/0$	$z_2/0$
1	$z_3/0$	$z_2/-$	$z_1/1$

A'	z_1'	z_2'
0	$z_1'/0$	$z_1'/0$
1	$z_2'/0$	$z_1'/1$

A''	z_1''	z_2''
0	$z_1''/0$	$z_2''/0$
1	$z_2''/0$	$z_1''/1$

Рис. 4.4.1. Частичный автомат Мили с двумя различными U-эквивалентными минимальными автоматами

ства. Идея метода состоит в замене состояния z_2 двумя состояниями z_2' и z_2'', различающимися выходами при входе 1, причем каждое из них эквивалентно одному из двух оставшихся состояний. При этом должна быть обеспечена возможность перехода из состояния z_2' в состояние z_2'' и из z_2'' в z_2'; для этого есть много возможностей.

Пусть в результате применения метода получены автоматы Мили $\bar{A}'$ и $\bar{A}''$, описанные таблицами, приведенными на рис. 4.4.2. Производя сокращение этих автоматов в духе теоремы о сокращении (теорема 2.3.5), получаем из $\bar{A}'$ автомат A' и из $\bar{A}''$ — автомат A'' (из примера 4.4.5).

$\bar{A}'$	z_1	z_2'	z_2''	z_3
0	$z_1/0$	$z_2'/0$	$z_2'/0$	$z_2'/0$
1	$z_3/0$	$z_2''/0$	$z_2'/1$	$z_1/1$

$\bar{A}''$	z_1	z_2'	z_2''	z_3
0	$z_1/0$	$z_2'/0$	$z_2''/0$	$z_2''/0$
1	$z_3/0$	$z_2''/0$	$z_2'/1$	$z_1/1$

Рис. 4.4.2. Доопределения автомата A, полученные расщеплением состояний

Замечание. Теорема 4.4.4 и пример 4.4.5 показывают, что проблема минимизации для частичных автоматов Мили существенно сложнее, чем аналогичная проблема для полностью определенных автоматов Мили.

Общее предположение. С настоящего момента будет считаться, что у всех рассматриваемых частичных автоматов Мили все состояния релевантны.

Данное предположение не является по сути ограничением, так как не релевантные состояния ничего не вносят во входно-выходное поведение рассматриваемых автоматов.

Теперь будем в основном рассматривать третий из поставленных выше четырех вопросов. Будут получены и ответы на вопросы первый и третий, хотя первый вопрос будет подробнее изучаться в разд. 4.5. Ответ на второй вопрос уже получен.

ПРЕОБРАЗОВАНИЯ И ПОКРЫТИЯ

Очень полезным является следующее обобщение понятия гомоморфизма.

Определение 4.4.6. Пусть $A=(Z, X, Y, f, g)$ и $A'=(Z', X, Y, f', g')$ — частичные автоматы Мили. Назовем t *преобразованием* из A в A', если t — соответствие (т. е. многозначное отображение) из Z в Z' со следующими свойствами:

1) при каждом z из Z, каждом z' из $t(z)$ и каждом x из X значение $g'(z', x)$ определено, если определено $g(z, x)$;

2) для всех (z, x) из D_g и всех z' из $t(z)$ выполняется равенство $g(z, x)=g'(z', x)$;

3) для каждой пары (z, x) из D_f выполнено условие: $t(z)\neq\varnothing$, для каждого z' из $t(z)$ пара (z', x) принадлежит $D_{f'}$ и выполняется включение $t(f(z, x))\supseteq f'(t(z), x)$.

Преобразование t называется *однозначным,* если при любом z из Z выполнено $|t(z)|=1$.

Замечание. Если h является U-эпиморфизмом A на A', то h — однозначное преобразование из A в A', а h^{-1} — преобразование из A' в A.

Теорема 4.4.7 (теорема Мюнтеферинга о преобразованиях). Частичный автомат Мили A' покрывает частичный автомат Мили A тогда и только тогда, когда существует преобразование t из A в A'.

Доказательство. 1. Пусть t — преобразование из A в A'. Полной индукцией по длине слова w из п.3) определения 4.4.6 немедленно получаем, что $f'^*(t(z), w)\subseteq t(f^*(z, w))$ для всех пар (z, w) из D_{f^*}.

Отсюда вытекает, что для каждого состояния z автомата A и каждого z' из $t(z)$ выполнено соотношение $z'\geqslant z$. Действительно, используя п.1) определения 4.4.6, получаем, что $D(\widehat{g}_z)\subset D(\widehat{g}'_{z'})$, а из п. 2) определения 4.4.6, используя полную индукцию по длине входного слова, находим $\bar{g}'^*(z', v)\sim\bar{g}^*(z, v)$ для всех слов v из $(D\bar{g}_z^*)$, это означает совместимость состояний z и z'.

2. Пусть A' покрывает A. Определим преобразование t из A в A', сопоставив каждому состоянию z автомата A множество всех покрывающих его состояний автомата A': $t(z)=\{z'\in Z' \mid z'\geqslant z\}$.

Свойства 1) и 2) определения 4.4.6 оказываются при этом очевидным образом выполненными.

Пусть теперь $(z, x)\in D_f$ и $z_1'\in f'(t(z), x)$. Тогда в $t(z)$ сущест-

вует состояние z_2' такое, что z покрывается состоянием $z_1'=f'(z_2', x)$. Из п.1 следствия 4.2.12 и того факта, что из $D(\widehat{g}_z)\subseteq D(\widehat{g}'_{z_2'})$ немедленно вытекает $D(\widehat{g}_{f(z,\,x)})\subseteq D(\widehat{g}'_{z_1'})$, получаем $z_1'\geqslant f(z, x)$. Итак, z_1' принадлежит $t(f(z, x))$.

Чтобы показатель справедливость свойства 3) определения 4.4.6, нужно еще доказать, что в $t(z)$, существует z', для которого определено состояние $f'(z', x)$.

По предположению в $t(z)$ существует z' такое, что $z'\geqslant z$. Поскольку по общему предположению состояние $f(z, x)$ релевантно, то в $F(X)$ существует слово w, для которого определено значение $\bar{g}_z(xw)$. Но тогда определено и значение $\widehat{g}'_{z'}(x, w)=\eta_1(\bar{g}'^{*}(z, xw))=$ $=\eta_1(\bar{g}'^{*}(f'(z', x), w))$ (см. п. 1 в 4.4.1), и потому должно быть определено $f'(z', x)$. ■

Замечания. 1. Определенное в п. 2 доказательства преобразование из A в A′ будем называть *каноническим преобразованием*.

2. Читателю рекомендуется выполнить упражнение 4.13.

Следствие 4.4.8. Для каждого частичного автомата Мили существует минимальный, который может быть построен эффективно.

Доказательство. Если задан частичный автомат Мили, то по следствию 4.4.3 нужно лишь проверить, существует ли для некоторого полностью определенного частичного автомата Мили A с числом состояний не большим, чем у A, преобразование t из A в A′. Поскольку (при постоянном A) число подлежащих проверке автоматов A′ и соответствий конечно, а при данном соответствии t из Z в множество состояний проверяемого автомата вопрос о том, является ли это соответствие преобразованием, может быть решен за конечное число шагов, то таким образом за конечное число шагов будет найден автомат, минимальный для A. (Данный метод, конечно, крайне трудоемок!) ■

ОДНОЗНАЧНОСТЬ ПРЕОБРАЗОВАНИЙ

Возникает вопрос: действительно ли нельзя избежать использования соответствий, т. е. нет ли возможности строить хотя бы один минимальный автомат для данного частичного автомата Мили как образ при некотором отображении со свойствами гомоморфизма, используя однозначное преобразование? Мы сейчас покажем, что это возможно только при выполнении некоторых определенных условий.

Пример 4.4.9. Пусть частичные автоматы Мили A и A′ заданы таблицами, приведенными на рис. 4.4.3.

Нетрудно проверить, что A′ является минимальным для A, что каждый минимальный для A автомат изоморфен автомату A′ и что в то же время не существует однозначного преобразования из A в A′.

То, что частичный автомат Мили с одним состоянием не может покрывать автомат A, становится ясным при рассмотрении входа 1 для A, находящегося в состояниях z_2 и z_3. Поскольку соответствие t, определяемое равенствами $t(z_1)=\{z_1', z_2'\}$, $t(z_2)=\{z_1'\}$ и $t(z_3)=\{z_2'\}$, является преобразованием из A в A′, то из теоремы о преобразованиях вытекает, что A′ покрывает A. Итак, A′ является минимальным для A и каждый минимальный для A автомат должен иметь два состояния.

A	z_1	z_2	z_3
0	$z_3/0$	$z_1/0$	$z_1/0$
1	$z_2/-$	$z_1/0$	$z_1/1$

A′	z_1'	z_2'
0	$z_2'/0$	$z_2'/0$
1	$z_1'/0$	$z_1'/1$

Рис. 4.4.3. Частичный автомат Мили с однозначно определенным минимальным автоматом

Предположим, что существует минимальный для A автомат A″ такой, что существует и однозначное преобразование t′ из A в A″. Так как $g''(t'(z_3), 1)=g(z_3, 1)=1$ и $g''(t'(z_2), 1)=g(z_2, 1)=0$, то должно быть $t'(z_2)\neq t'(z_3)$. Кроме того, тогда $f''(t'(z_1), 0)=$ $=t'(f(z_1, 0))=t'(z_3)$.

Если бы было выполнено равенство $t'(z_1)=t'(z_2)$ (A″ имеет ровно два состояния!), то тогда бы мы имели $t'(z_3)=f''(t'(z_1), 0)=$ $=f''(t'(z_2), 0)=t'(f(z_2, 0))=t'(z_1)$, откуда бы следовало противоречие $t'(z_3)=t'(z_2)$. Если бы выполнялось равенство $t'(z_3)=t'(z_1)$, то возникало бы противоречие $t'(z_2)=t'(f^*(z_3, 11))=f''^*(t'(z_3), 11)=f''^*(t'(z_1), 11)=t'(f^*(z_1, 11))=t'(z_1)$.

Пусть A″ — автомат, минимальный для A, и t′ — построенное в доказательстве теоремы 4.4.7 преобразование из A в A″. Поскольку два состояния автомата A″ должны порождать при входе 1 два различных выхода, то должно быть $t'(z_2)\neq Z''\neq t'(z_3)$. Так как преобразование t′ не может быть однозначным, должно выполняться $t'(z_1)=Z''$. Итак, с точностью до обозначений t′ равно описанному выше преобразованию t из A в A′, откуда вытекает изоморфность A′ и A″.

Теорема 4.4.10 (теорема об однозначности преобразований). 1. Пусть A — частичный автомат Мили и A′ — автомат, минимальный для A. Пусть также существует однозначное преобразование из A в A′. Тогда существует доопределение A^+ автомата A такое, что (с точностью до изоморфизма) однозначно определенный автоматом A^+ эквивалентный ему сокращенный автомат Мили является минимальным для A; этот автомат совпадает с доопределением автомата A′.

2. Если частичный автомат Мили A обладает доопределением A^+ таким, что эквивалентный A^+ сокращенный автомат Мили A′ оказывается минимальным для A, то существует однозначное преобразование из A в A′.

Доказательство. 1. Пусть t — однозначное преобразование из A в A′ и A_1' — некоторое произвольное доопределение автомата A′. Тогда t является также и однозначным преобразованием из A в A_1'. Поскольку A_1' минимален, то по теореме 4.4.7 всегда $t^{-1}(f_1'(t(z), x)) \neq \varnothing$. Определим теперь доопределение $A^+ = (Z, X, Y, f^+, g^+)$ автомата A следующим образом:

$$f^+(z, x) = \begin{cases} f(z, x), \text{ если } (z, x) \in D_f, \\ \text{произвольному } z_1 \text{ такому, что } t(z_1) = f_1'(t(z), x) \\ \text{в противном случае,} \end{cases}$$

$g^+(z, x) = g_1'(t(z), x)$ для всех z из Z и всех x из X.

При этом t оказывается гомоморфизмом из A^+ на A_1'. Итак, A_1' эквивалентен A^+. Далее, автомат A_1' является минимальным для A и сокращенным (как автомат Мили).

2. Из теоремы об однозначности минимального автомата (теорема 3.6.4) вытекает, что A′ — гомоморфный образ автомата A^+. Соответствующий гомоморфизм является, очевидно, однозначным преобразованием из A в A′, так как A^+ — доопределение автомата A. ■

Замечание. Читателю рекомендуется рассмотреть упражнение 4.14.

Следствие 4.4.11. Пусть функция переходов частичного автомата Мили A определена всюду и A′ — автомат, минимальный для A. Тогда следующие два условия эквивалентны: 1) существует однозначное преобразование из A в A′; 2) существует доопределение A^+ автомата A такое, что эквивалентный автомату A^+ сокращенный автомат Мили оказывается минимальным для A.

Замечания. 1. Частичный автомат Мили A из примера 4.4.5 обладает всюду определенной функцией переходов, но для него не выполнено условие 2) следствия.

2. Из замечания к определению 4.4.6 и следствия 4.3.10 вытекает, что условие 1) данного следствия выполнено, если автомат, U-минимальный для A, оказывается минимальным для A (см. также упражнение 4.15).

3. Предположение о функции переходов в следствии 4.4.11 необходимо (см. упражнение 4.16).

Доказательство следствия. Используя предыдущие теоремы, следует лишь показать, что из 2) вытекает 1).

Пусть выполнено условие 2). По теореме о преобразованиях (теорема 4.4.7) существует преобразование t из A в A′. Автомат A′ можно доопределить до автомата A_1', полагая $g_1'(z', x) = g^+(z, x)$, — для всех z из Z и всех z′ из t(z). Этого достаточно, так как A и A^+ имеют одно и то же множество состояний и так как по предположению функции переходов автоматов A′ и A всюду определены.

Из сказанного вытекает, что t является преобразованием из A^+ в A_1'. Если бы t не было однозначным, то имелись бы состояния z в Z и z_1' и z_2' в t(z) такие, что $z_1' \neq z_2'$ и $z_i' \geqslant z$ при i=1, 2 (это

вытекает из доказательства теоремы о преобразованиях). Поскольку автоматы A^+ и A_1' определены полностью, то в этом случае состояние z было бы эквивалентно и z_1', и z_2' (см. п.1 определения 4.4.1). Но тогда состояния z_1' и z_2' были бы эквивалентны между собой, что противоречит сокращенности автомата A_1'.■

НЕИЗБЫТОТОЧНОСТЬ ПОКРЫТИЙ

У минимального полностью определенного частичного автомата Мили не может быть, как следует из теоремы об однозначности минимального автомата, двух различных состояний с одинаковыми реакциями. Обобщим это свойство.

Определение 4.4.12 Пусть A и A′ — два частичных автомата Мили. A′ называется *неизбыточным покрытием* для A, если $A' \geqslant A$ и не существует двух различных состояний z′ и z″ у автомата A′, для которых выполнено условие: z′ покрывает каждое состояние автомата A, покрываемое состоянием z″.

Теорема 4.4.13. Пусть A — частичный автомат Мили. Каждый минимальный для A автомат является неизбыточным покрытием для A, но не каждый автомат, являющийся неизбыточным покрытием для A, оказывается минимальным для A.

Доказательство. 1. Пусть A — частичный автомат Мили из примера 4.4.5. В этом случае каждое доопределение автомата A является неизбыточным покрытием для A, так как каждое такое доопределение представляет собой сокращенный автомат. Ни одно доопределение, однако, не является автоматом, минимальным для A.

2. Пусть A′ — автомат, минимальный для A. Предположим, что A′ — избыточное покрытие для A, т. е. что существуют состояния z′ и z″ автомата A′ такие, что $z' \neq z''$ и $z' \geqslant z$ для всех состояний z автомата A таких, что $z'' \geqslant z$.

В таком случае мы можем определить новый частичный автомат Мили A′, отбрасывая состояние z″:

$$A_1' = (Z_1' = Z' - z'', X, Y, f_1', g_1'),$$

$$f_1'(z, x) = \left\{ \begin{array}{l} f'(z, x), \text{ если } f'(z, x) \neq z'' \\ z' \text{ в противном случае} \end{array} \right\} \text{ для всех } (z, x) \text{ из } D_f';$$

$g_1' = g'/Z_1' \times X$.

Если мы покажем, что $A_1' \geqslant A$, то теорема будет доказана, так как A_1' имеет меньше состояний, чем A, что противоречит предположению о минимальности последнего.

Чтобы доказать, что $A_1' \geqslant A$, достаточно, используя теорему о преобразованиях, задать преобразование t′ из A в A_1'.

Пусть t — каноническое преобразование из A в A′. Определим t′ следующим образом:

$$t'(z) = \left\{ \begin{array}{l} t(z) - z'', \text{ если } z'' \in t(z), \\ t(z) \text{ в противном случае.} \end{array} \right.$$

По предположению если $z'' \in t(z)$, то $z' \in t(z)$.

Очевидно, что t' удовлетворяет условиям 1) и 2) определения 4.4.6. Чтобы проверить выполнение условия 3), предположим, что (z, x) — пара из D_f. Из сказанного вытекает, что $t'(z) \neq \varnothing$ и что $(z_1, x) \in D(f_1')$ для всех z_1 из $t'(z)$. Если, далее, $z'' \in t(f(z, x))$, то и $z' \in t(f(z, x))$.

Положим

$$R = \begin{cases} \{z'\}, & \text{если } z'' \in f'(t(z), x), \\ \varnothing & \text{в противном случае.} \end{cases}$$

Тогда при всех (z, x) из D_f имеем $t'(f(z, x)) = t(f(z, x)) - z'' \supseteq \supseteq (f'(t(z), x) - z'') \cup R = f_1'(t'(z), x)$, т. е. условие 3) выполнено. ■

4.5. АЛГЕБРАИЧЕСКАЯ ПОСТАНОВКА ПРОБЛЕМЫ МИНИМИЗАЦИИ

Приведенный в доказательстве следствия 4.4.8 метод минимизации с практической точки зрения бесполезен. Проблема поиска пригодного для практического применения, т. е. просто реализуемого и быстро выполнимого, метода до настоящего времени не имеет удовлетворительного решения. Ниже проблема минимизации будет сведена к алгебраической задаче и для ее решения будет приведен метод, который допускает простое описание. Однако он в качестве существенной составной части включает в себя процедуру поиска переборного характера, так что практически применим только для автоматов со сравнительно небольшим числом состояний.

Основной идеей, лежащей в основе приведенных ниже построений, является обобщение метода сокращения для полностью определенных автоматов Мили. В этом методе (см. теорему 2.3.6) сокращенный автомат Мили формировался на основе системы подмножеств множества состояний исходного автомата (системы классов эквивалентных состояний). В случае частичных автоматов Мили аналогичную роль играют классы совместных состояний.

РЕШЕТКА СИСТЕМ МНОЖЕСТВ

Для дальнейшего нам понадобятся новые понятия.

Определение 4.5.1. Пусть S — конечное множество.

1. Множество $M = \{T_1, T_2, \ldots, T_n\}$ непустых подмножеств T_i (называемых *блоками*) множества S называется *системой множеств* над S, если выполнены условия:

1) $S = T_1 \cup T_2 \cup \ldots \cup T_n$ (т. е. M является *покрытием* множества S);

2) из $T_i \subseteq T_j$ вытекает, что $i = j$ для всех i и j из $\{1, \ldots, n\}$.

$\mathcal{M}(S)$ обозначает (конечное) множество всех систем множеств над S.

2. Пусть U — некоторое множество подмножеств множества S. Тогда под U^* будем понимать систему множеств, которая возникает при удалении из U всех подмножеств, содержащихся в других подмножествах из U, и при присоединении к U блоков $\{s\}$, где

s пробегает разность между S и объединением всех подмножеств из U.

3. Если M и L — системы множеств над S, то:

1) $M \leqslant L$ означает, что каждый блок из M содержится в некотором блоке из L.

2) $M+L=(M \cup L)^{\cdot}$,

$M \cdot L=\{T \cap T' \mid T \in M, T' \in L\}^{\cdot}$.

Замечания. 1. Каждое разбиение множества S, т. е. каждое покрытие множества S дизъюнктными множествами, — это система множеств над S. В частности, множество классов эквивалентности при произвольном отношении эквивалентности на S является системой множеств над S.

2. По определению 4.5.1, п.2 каждое множество T множества S определяет систему множеств над S, которая кратко будет обозначаться $T^{\cdot}: T^{\cdot}=\{T\}^{\cdot}=\{T\} \cup \{\{s\} \mid s \in S-T\}$ при $T \neq \varnothing$ и $\varnothing^{\cdot}=\{\{s\} \mid s \in S\}$.

Очевидно, что для подмножеств T_1 и T_2 множества S соотношение $T_1^{\cdot} \leqslant T_2^{\cdot}$ выполняется тогда и только тогда, когда $T_1 \subseteq T_2$.

3. Отношение «$\leqslant$» является частичным порядком (рефлексивным, антисимметричным и транзитивным отношением) на $\mathcal{M}(S)$. $M+L$ — это наименьшая (относительно $\leqslant$) система множеств, которая больше и M и L; $M \cdot L$ — это наибольшая система множеств, которая меньше и M и L. Таким образом, $\mathcal{M}(S)$ с отношением $\leqslant$ и операциями $+$ и $\cdot$ является решеткой, а для $\leqslant$, $+$ и $\cdot$ справедливы законы, выполняющиеся, например, в решетке всех подмножеств некоторого множества с отношением $\subseteq$ и операциями $\cup$ и $\cap$.

КЛАССЫ СОВМЕСТНЫХ СОСТОЯНИЙ

Для нашей задачи важную роль играют две системы множеств.

Определение 4.5.2. Пусть A — частичный автомат Мили в обычных обозначениях.

1. Подмножество T множества Z называется *классом совместных состояний,* если любые два состояния из T совместны. Класс совместных состояний автомата A называется *максимальным,* если он не содержится ни в каком другом таком классе.

Символом V_A будем обозначать множество всех, по меньшей мере двухэлементных, классов совместных состояний автомата A.

Символом M_A будем обозначать множество всех максимальных классов совместных состояний автомата A.

2. Пусть A′ — неизбыточное покрытие для A и t — каноническое преобразование из A в A′, тогда

$$S_A(A')=\{t^{-1}(z') \mid z' \in Z'\}.$$

Замечание. При предположениях из п.2 определения 4.5.2 выполняется равенство $t^{-1}(z')=\{z \in Z \mid z \leqslant z'\}$ и любые два состояния из $t^{-1}(z')$ совместны.

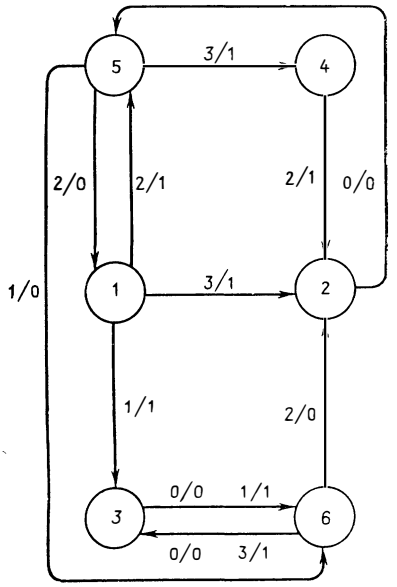
Следствие 4.5.3. Пусть A′ — неизбыточное покрытие для A. Тогда:

1. Если автомат A определен полностью, то $M_A=S_A(A')=$ $=\{[z]\,|\,z\in Z\}$, где $[z]$ — множество всех состояний автомата A, эквивалентных состоянию z.

2. M_A является системой множеств над множеством состояний автомата A, причем $M_A=(V_A)^*$.

3. $S_A(A')$ является системой множеств над множеством состояний автомата A, причем $S_A(A')\leqslant M_A$.

Замечание. Как M_A, так и $S_A(A')$ могут состоять из блоков с непустыми пересечениями, в отличие от случая полностью определенных автоматов Мили.



A'	1'	2'	3'
0	3'/0	3'/0	2'/0
1	2'/1	3'/1	3'/0
2	3'/1	1'/1	1'/0
3	1'/1	–	2'/1

Рис. 4.5.1. Частичный автомат Мили A и минимальный для A автомат A′ с $M_A\neq S_A(A')$

Пример 4.5.4. 1. В ситуации из примера 4.4.9 справедливы равенства $M_A=S_A(A')=\{\{z_1, z_2\}, \{z_1, z_3\}\}$ и $V_A=M_A$.

2. В ситуации из примера 4.4.5 выполняются равенства

$$M_A=\{\{z_1, z_2\}, \{z_2, z_3\}\}=S_A(A')=S_A(A'')=V_A.$$

3. Пусть A — частичный автомат Мили, граф которого изображен на рис. 4.5.1, а A′ — автомат, заданный приведенной на рис. 4.5.1 таблицей.

Используя метод из доказательства теоремы 4.2.12 (или из упражнений 4.9 и 4.10) можно установить, что

$$M_A=\{\{1, 2, 3, 4\}, \{5, 6\}, \{2, 5\}, \{3, 6\}\}.$$

Этот результат можно получить также, проводя следующие несложные рассуждения. То, что состояния 1 и 5, а также 3 и 5 несовместны, легко установить, рассматривая вход 1. Вход 2 демон-

стрирует несовместность состояний 1 и 6, 4 и 5, а также 4 и 6. Если бы состояния 2 и 6 были совместны, то совместными должны бы были быть и состояния 3 и 5 (в соответствии с п.1 следствия 4.2.12). В то же время состояния 2 и 5 совместны, так как состояние $f(2, x)$ определено тогда и только тогда, когда не определено $f(5, x)$ (f — функция переходов, x — произвольный вход). Точно так же показывается совместность состояний 2 и 1, 2 и 4, а также 3 и 4. Из совместности состояний 1 и 2 и состояний 3 и 4 немедленно вытекает совместность состояний 5 и 6 (поскольку при входах 2 и 3 оба эти состояния порождают одинаковые выходы и переходят в совместные состояния 1 и 2 или 3 и 4). Аналогичным образом отсюда следует совместность состояний 2 и 3, а из совместности состояний 2 и 5 — совместность состояний 1 и 4. Легко видеть, что совместны состояния 3 и 6, а следовательно, совместны состояния 1 и 3.

Итак, $V_A=\{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{2, 5\}, \{3, 4\}, \{3, 6\}, \{5, 6\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}\}$.

Наконец, можно показать, что автомат A' является минимальным для A. Действительно, если бы существовал автомат A'', являющийся неизбыточным покрытием для A и имеющий только два состояния z' и z'', то по п.3 следствия 4.5.3 выполнялось бы соотношение $S_A(A'')\leqslant M_A$ и для канонического преобразования t из A в A'' должно бы было выполняться равенство $\{1, 2, \ldots, 6\}=t^{-1}(z')\cup t^{-1}(z'')$. Это возможно только в том случае, когда $t^{-1}(z')=\{1, 2, 3, 4\}$ и $t^{-1}(z'')=\{5, 6\}$ (с точностью до замены z' на z'' и обратно). Пусть теперь x — вход, для которого в A'' определен переход $f''(z'', x)$, и z — состояние из $t^{-1}(z'')$, т. е. такое состояние, что $z''\in t(z)$. По определению преобразования в этом случае $f''(z'', x)\in t(f(z, x))$, так что $f(z, x)\in t^{-1}(f''(z'', x))$.

Отсюда $f(t^{-1}(z''), x)\subseteq t^{-1}(f''(z'', x))$, т. е. $f(t^{-1}(z''), x)\in S_A(A'')$ при всех $(z'', x)\in D_{f''}$. Из предположения об автомате A'' и из вышесказанного при $x=1$ и $x=2$ следовало бы, что $\{3, 6\}$ и соответственно $\{2, 5\}$ должны содержаться в $t^{-1}(z'')$ или в $t^{-1}(z')$, чего быть не может. Итак, A' имеет минимальное число состояний.

Соотношение $A'\geqslant A$ вытекает (по теореме о преобразованиях) из того, что равенствами $t(1)=t(2)=1'$, $t(3)=t(4)=2'$ и $t(5)=t(6)=3'$ определяется преобразование (причем каноническое) из A в A'.

Отсюда немедленно получаем, что $S_A(A')=\{\{1, 2\}, \{3, 4\}, \{5, 6\}\}$.

Отметим, что t является однозначным преобразованием, так что по теореме 4.4.10 доопределение автомата A' оказывается с необходимостью сокращенным автоматом Мили, эквивалентным некоторому доопределению автомата A.

В то же время автомат A' оказывается не единственным минимальным для A, поскольку посредством иного доопределения автомата A (по сравнению с тем, которое приводит к получению A') можно получить минимальный для A автомат A'' с $S_A(A'')=\{\{1, 4\}, \{2, 5\}, \{3, 6\}\}$.

При работе с последним примером мы видели, что множества

$f(t^{-1}(z', x)$ должны принадлежать $S_A(A')$, если требуется, чтобы автомат A' был минимальным для A. Чтобы формализовать этот факт, нам потребуется одно понятие из алгебры.

ОПЕРАТОРЫ ЗАМЫКАНИЯ НА СИСТЕМАХ МНОЖЕСТВ

Определение 4.5.5. Пусть S — конечное множество.

1. *Оператором* (или операцией) *замыкания* на решетке $\mathcal{M}(S)$ называется отображение (произвольное) h из $\mathcal{M}(S)$ в себя, если оно обладает следующими свойствами:

1) $M \leqslant L$ влечет за собой $h(M) \leqslant h(L)$;

2) $M \leqslant h(M)$;

3) $h(h(M)) = h(M)$ — для всех M и L из $\mathcal{M}(S)$.

Если для всех M и L из $\mathcal{M}(S)$ выполняется также равенство

4) $h(M+L) = h(M) + h(L)$,

то оператор h называется *аддитивным*.

2. Пусть h — оператор замыкания на $\mathcal{M}(S)$. Если система множеств M из $\mathcal{M}(S)$ такова, что $M = h(M)$, то система M называется *h-замкнутой*.

Каждый частичный автомат Мили определяет некоторый аддитивный оператор замыкания.

Лемма 4.5.6. Пусть A — частичный автомат Мили в обычных обозначениях. Пусть также h_A — отображение из $\mathcal{M}(Z)$ в себя, определенное условиями:

1. $h_A(T^\cdot) = \{f^*(T, w) \mid w \in F(X)\}^\cdot$ для каждого $T \subseteq Z$;

2. $h_A(\{T_1, \ldots, T_n\}) = h_A(T^\cdot_1) + \ldots h_A(T^\cdot_n)$ — для каждой системы множеств $\{T_1, \ldots, T_n\}$ из $\mathcal{M}(Z)$, не имеющей вида $T^\cdot$, где $T \subseteq Z$.

Тогда h_A является эффективно вычислимым аддитивным оператором замыкания на $\mathcal{M}(Z)$.

Замечание. Отметим, что

$$f^*(T, w) = \{f^*(z, w) \mid z \in T,\ (z, w) \in D(f^*)\}$$

и что U принадлежит $h_A(T^\cdot)$ тогда и только тогда, когда либо U одноэлементно, либо существует слово w такое, что $U = f^*(T, w)$.

Доказательство. Очевидно, что для всех T, $U \subseteq Z$:

1′) $T^\cdot \leqslant U^\cdot$ влечет $h_A(T^\cdot) \leqslant h_A(U^\cdot)$;

2′) $T^\cdot \leqslant h_A(T^\cdot)$;

3′) $h_A(h_A(T^\cdot)) = h_A(T^\cdot)$.

Вследствие п.2 определения оператора h_A выполнено условие 4) аддитивности, а условия 1), 2) и 3) непосредственно вытекают из 1′), 2′), 3′).

Для каждого $T \subseteq Z$ значение $h_A(T^\cdot)$ эффективно вычислимо, поскольку

$$h_A(T^\cdot) = \{f^*(T, w) \mid w \in F(X),\ |w| < 2^{|Z|}\}^\cdot.$$

Действительно, если $w = x_1 x_2 \ldots x_k$ и $k \geqslant 2^{|Z|}$, где $x_i \in X$ при $i = 1, \ldots k$ и $T \subseteq Z$, то существует и $j < 2^{|Z|}$ такое, что $f^*(T, w) = f^*(T, x_1 x_2 \ldots x_j)$, поскольку не все подмножества $f^*(T, x_1 \ldots x_i)$ множества Z при $i = 0, 1, \ldots, k$ могут быть различны (их $k+1$). ■

Легко решается вопрос: является ли данная система множеств замкнутой относительно данного аддитивного оператора замыкания?

Лемма 4.5.7. Пусть S — конечное множество, h — аддитивный оператор замыкания на $\mathscr{M}(S)$ и M — система множеств из $\mathscr{M}(S)$.

Система M является h-замкнутой тогда и только тогда, когда для всех T из M выполнено неравенство $h(T^{\cdot})\leqslant M$.

Доказательство. Пусть M — h-замкнутая система и T — множество из M. Тогда $T^{\cdot}\leqslant M$, и потому $h(T^{\cdot})\leqslant h(M)=M$, что вытекает из пп. 1) и 2) определения 4.5.5. Пусть теперь $M=\{T_1, \ldots, T_n\}=T^{\cdot}_1+\ldots+T^{\cdot}_n$ и $h(T^{\cdot}_i)\leqslant M$ при $i=1, \ldots, n$. Тогда из свойства аддитивности и п. 2 определения 4.5.5 имеем $M\leqslant h(M)=h(T^{\cdot}_1)+\ldots+h(T^{\cdot}_n)\leqslant M$, так что $M=h(M)$.

АЛГЕБРАИЧЕСКАЯ ПОСТАНОВКА ПРОБЛЕМЫ МИНИМИЗАЦИИ

Теперь мы имеем возможность привести алгебраическую постановку проблемы минимизации, которая одновременно оказывается основой для соответствующего метода минимизации.

Теорема 4.5.8 (Полл, Унгер). Пусть A — частичный автомат Мили.

1. Для каждого неизбыточного покрытия A′ автомата A:

1) $S_A(A')$ является h_A-замкнутой;

2) $S_A(A')\leqslant M_A$.

2. Если M — система множеств с n блоками над множеством состояний автомата A такая, что:

1) M является h_A-замкнутой;

2) $M\leqslant M_A$,

то существует по меньшей мере один автомат A′ с n состояниями, являющийся покрытием для автомата A.

Доказательство. 1. Пусть A′ — неизбыточное покрытие для автомата A. Из п.3 следствия 4.5.3 вытекает выполнение условия 2).

Чтобы доказать выполнение условия 1), нам на основе леммы 4.5.7 нужно лишь показать, что $M'=h_A((t^{-1}(z'))^{\cdot})\leqslant S_A(A')$ для любого состояния z′ автомата A′, где t — каноническое преобразование из A в A′.

Любой блок из M′ либо одноэлементен, и тогда он содержится в некотором блоке из $S_A(A')$, либо имеет вид $B=\{f^*(z, w)\,|\,(z, w)\in D_{f^*},\ z\in t^{-1}(z')\}$ при фиксированном слове w из F(X). Рассуждения, аналогичные проведенным при рассмотрении п.3 примера 4.5.4 вместе со случаем 1 доказательства теоремы 4.4.7, приводят к выводу, что B содержится в $t^{-1}(f'^*(z', w))$, т. е. в некотором блоке из M′. Так что условие 1) выполнено.

2. Пусть M — система множеств над Z со свойствами 1) и 2). Мы построим искомое покрытие A′ следующим образом. Пусть $A'=(M, X, Y, f', g')$.

Для каждого блока B и M и каждого x из X положим:

а) $f'(B, x)$ определено тогда и только тогда, когда в B существует Z такое, что $(Z, x) \in D_f$, и в таком случае $f'(B, x) = B'$, где B' — блок из M такой, что $f(B, x) \subseteq B'$; поскольку система M является h_A-замкнутой, то всегда существует ровно один такой блок B'.

б) $g'(B, x)$ определено тогда и только тогда, когда в B существует Z такое, что $(Z, x) \in D_g$, и в этом случае $g'(B, x) = g(z, x)$.

$M \leqslant M_A$ и любые два состояния z и z′ из B совместны, поэтому $g(z, x) = g(z', x)$, если z' — состояние из B такое, что $(z', x) \in D_g$. Так что g' определено корректно.

Чтобы доказать, что $A' \geqslant A$, достаточно на основе теоремы о преобразованиях показать, что определяемое ниже соответствие t из Z в M является преобразованием из A в A′: $t(z) = \{B \in M \mid z \in B\}$.

Условия 1) и 2) определения 4.4.6, как следует из п.б), очевидным образом выполнены. Условие 3) выполнено на основе п.а), поскольку если $f'(B, x) = B'$, то $B' \in t(f(z, x))$ для каждого z из B и потому

$$t(f(z, x)) \supseteq \{B' \mid B' = f'(B, x), z \in B\} = f'(t(z), x) \neq \varnothing. \blacksquare$$

Следствие 4.5.9 (Пратер). Проблема поиска автомата, минимального для данного частичного автомата Мили A, эквивалентна задаче поиска системы множеств M над множеством состояний Z автомата A, обладающей следующими свойствами:

1) M является h_A-замкнутой;

2) $M \leqslant M_A$;

3) если L — система множеств над Z, удовлетворяющая условиям 1) и 2), то $|M| \leqslant |L|$.

Доказательство. 1. Если M — система множеств над Z, удовлетворяющая условиям 1)—3), то по условиям 1) и 2) п.2 теоремы 4.5.8 существует покрытие A′ автомата A с $|M|$ состояниями. Если бы существовал автомат A″, являющийся покрытием для A и имеющий меньшее число состояний, чем автомат A′, то система множеств $L = S_A(A'')$ (по теореме 4.5.8, п.1) удовлетворяла бы условиям 1) и 2), но условие 3) выполнено бы не было. Итак, A′ — автомат, минимальный для A.

2. Пусть A′ — автомат, минимальный для A. В этом случае в силу теоремы 4.4.13 из теоремы 4.5.8 вытекает, что $M = S_A(A')$ удовлетворяет условиям 1)—3). ■

Замечания. 1. Итак, чтобы найти минимальный для A автомат, нужно перебрать все системы множеств над множеством состояний автомата A, блоки которых состоят из совместных состояний. При этом следует отбирать h_A-замкнутые системы и искать среди них систему с минимальным числом блоков. Следуя доказательству п.2 теоремы 4.5.8, можно на базе найденной системы множеств построить искомый автомат.

В качестве дополнения читателю рекомендуется выполнить упражнение 4.17.

2. Примеры 4.4.5 и 4.5.4, п.2 показывают, что, вообще говоря, на оазе одной системы множеств можно строить различные минимальные автоматы для данного автомата.

3. Как видно из примера 4.5.4, п. 3, число множеств, на базе которых строятся исследуемые системы множеств, даже при «небольшой» системе множеств M_A может оказаться весьма большим.

Чтобы убедиться в сказанном, читателю рекомендуется применить обрисованный в п.1 способ к автомату из примера 4.1.1.

4. Пример 4.5.4, п.3 показывает также, что для построения минимального автомата недостаточно использовать систему множеств, состоящую только из максимальных классов совместных состояний (см. по этому поводу также упражнение 4.18).

МОДЕРНИЗАЦИЯ МЕТОДА МИНИМИЗАЦИИ

Для того чтобы иметь возможность уменьшить число исследуемых систем множеств при поиске минимального для A автомата, нам понадобятся новые понятия.

Определение 4.5.10. Пусть S — конечное множество, M — система множеств над S и h — аддитивный оператор замыкания на $\mathscr{M}(S)$.

1. Непустое подмножество T множества S называется *M-множеством*, если $T \cdot \leqslant M$.

2. Если T и U—M-множества, то U называется *h-делимым* на T, если выполнены условия:

1) $U \subseteq T$;

2) $h(T\cdot) \leqslant T\cdot + h(U\cdot)$.

3. M-множество, которое является h-делимым только на себя, называется *h-простым*.

Лемма 4.5.11. Пусть M и h заданы как в определении 4.5.10. Каждое M-множество h-делимо на некоторое h-простое M-множество

Доказательство. По определению все множества, на которые h-делится данное M-множество U, являются надмножествами множества U, т. е. множествами, содержащими U в качестве подмножества. Вследствие конечности множества S число подмножеств множества S конечно. Поэтому для доказательства леммы достаточно показать, что если U, T и R — произвольные M-множества, причем U h-делимо на T и T h-делимо на R, то и U h-делимо на R. Итак, имеем:

$$U \subseteq T,\ h(T\cdot) \leqslant T\cdot + h(U\cdot),$$

$$T \subseteq R,\ h(R\cdot) \leqslant R\cdot + h(T\cdot).$$

Тогда $U \subseteq R$ и $h(R\cdot) \leqslant R\cdot + T\cdot + h(U\cdot) \leqslant R\cdot + h(U\cdot)$, откуда по определению 4.5.10 и вытекает нужный факт. ■

Теорема 4.5.12 (Грасселли, Лючио). Для каждого частичного автомата Мили A существует удовлетворяющая условиям 1)—3) следствия 4.5.9 система множеств над множеством состояний автомата A, блоки которой являются h_A-простыми M_A-множествами.

Замечание. Итак, при поиске минимального автомата для частичного автомата Мили A достаточно ограничивать поиск системами множеств, состоящими из h_A-простых M_A-множеств.

То, что при этом число исследуемых систем множеств не всегда сокращается, показывает пример 4.1.1, в котором все классы совместных состояний являются h_A-простыми.

Доказательство теоремы. Пусть $M=\{B_1, B_2, ..., B_n\}$— удовлетворяющая условиям 1)—3) следствия 4.5.9 система множеств, содержащая k блоков, не являющихся h_A-простыми M_A-множествами, причем $k\geqslant 1$ (иначе нечего доказывать).

Нам достаточно показать, что в этом случае может быть построена система множеств M', удовлетворяющая условиям 1) и 2) следствия 4.5.9, содержащая столько же блоков, что и M, причем такая, что только k—1 ее блок не будет h_A-простым M_A-множеством.

Предположим, что блок B_i — не h_A-простое M_A-множество. По лемме 4.5.11 блок B_i является h_A-делимым на некоторое h_A-простое M_A-множество C_i. Положим тогда $M'=\{B_1, B_2, ..., B_{i-1}, C_i, B_{i+1}, ..., B_n\}$.

Из $B_i\subseteq C_i$ следует $M\leqslant M'$.

Так как C_i является M_A-множеством, то $M'\leqslant M_A$.

Чтобы показать что M' является h_A-замкнутой системой множеств, используем лемму 4.5.7. Так как система M h_A-замкнута, то для всех $j\neq i$, где $1\leqslant j\leqslant n$, имеем $h_A(B_j)\leqslant M\leqslant M'$, а из определения h_A-делимости получаем $h_A(C_i)\leqslant C_i+h_A(B_i)\leqslant M'+M=M'$. Итак, система M' также h_A-замкнута, так что из условия 3) следствия 4.5.9 вытекает равенство $|M'|=|M|$. Таким образом $M'=\{B_1, ..., B_{i-1}, C_i, B_{i+1}, ..., B_n\}$ является искомой системой множеств. ■

В принципе можно еще больше ограничить поиск среди систем множеств, формируя на базе h_A новые аддитивные операторы и доказывая для них результаты, аналогичные теореме 4.5.12.

УПРАЖНЕНИЯ

4.1. По аналогии с примером 4.1.1 постройте частичный автомат Мили с входным алфавитом {0, 1}, вычисляющий максимум (или минимум) двух положительных целых двоичных чисел m и n. Вход автомата формируется следующим образом: числа приводятся к виду, когда они имеют одинаковое число разрядов (добавлением перед числом нужного числа нулей), и после этого, начиная со старшего разряда, «вперемешку» (как в примере 4.1.1) вводятся в автомат Последовательность выходов в четные моменты времени должна представлять максимум (или минимум) данных чисел.

Попытайтесь, далее, уменьшить до минимума число состояний (ср. упражнение 2.3)

4.2. По образцу примера 4.1.2 постройте анализатор «арифметических выражений», определяемых приведенными ниже металингвистическими формулами в форме Бэкуса — Наура:

<арифметическое выражение>::=<арифметическое выражение>+<слагаемое>
<арифметическое выражение>::=<слагаемое>
<слагаемое> ::=<слагаемое>*<множитель>
<слагаемое> ::=<множитель>
<множитель> ::=<арифметическое выражение>
<множитель> ::=a

[Указание. Автомат должен всегда «смотреть на один символ вперед»]

4.3. По методу из примера 4.1.3 постройте декодер для следующего кодирования:

a — 0, b — 11, c — 100, d — 1010, e — 1011.

4.4. Сконструируйте автомат управления железнодорожным шлагбаумом для переезда через железную дорогу с двумя колеями, причем движение по каждой колее идет только в одном направлении. Пусть на достаточно большом расстоянии от шлагбаума на каждом из путей помещены детекторы, посылающие сигнал при прохождении поезда. Итак, автомат получает входы по четырем каналам (по одному на детектор, причем вход от детектора равен 1 тогда, когда он посылает сигнал о прохождении поезда). Он должен порождать выход 1 в том и только в том случае, когда шлагбаум должен быть закрыт. [Указание. Предположите, что расстояние от детекторов до шлагбаума больше, чем любая возможная длина поезда, и что расстояние между двумя поездами, идущими в одном направлении, всегда больше расстояния между детекторами. Считайте далее, что входы от всех детекторов поступают одновременно.]

4.5.* (Шютценбергер, Перро.) Докажите, что кодирование $h: F^+(B) \to F^+(C)$ допускает декодирование с помощью частичного автомата Мили в смысле примера 4.1.3 тогда и только тогда, когда:

1) $h(B)$ конечно;

2) $h(B) \cap h(B) \cdot F^+(C) = \varnothing$.

Условие 2) означает, что ни один префикс кодового слова (т. е. ни одно b' из $h(B)$) не является кодовым словом.

Покажите далее, что условие 2) выполняется для кодирования h в точности тогда, когда для любого u из $h(F^+(B))$ и любого w из $F^+(C)$ выполнено условие: если $uw \in h(F^+(B))$, то $w \in h(F^+(B))$.

4.6.* (Курмит.) Частичный автомат Мили A с $D_f = D_g$ называется автоматом без потери информации конечного порядка типа I, если существует $n \in \mathbf{N}$ такое, что для всех z и z' из Z, всех $x \neq x'$ из X и всех слов u и v из X^n выполняется соотношение $g^*(z, xu) \neq g^*(z', x'v)$. Наименьшее число n с данным свойством называется порядком A.

1. Докажите, что вопрос о том, является ли данный частичный автомат Мили автоматом без потери информации конечного порядка типа I, разрешим; для автомата без потери информации конечного порядка типа I порядок эффективно вычислим.

[Указание. Рассмотрите множество пар состояний z, z' для которых существуют состояние z_0 и слова xw и $x'w'$ одинаковой длины такие, что $x \neq x'$, $g^*(z_0, w) = g^*(z_0, w')$, $z = f^*(z_0, w)$ и $z' = f^*(z, w')$.]

2. Частичный автомат Мили $\tilde{A}$ с теми же множествами входов и выходов, что и у автомата A, и с $D_{\tilde{f}} = D_{\tilde{g}}$ называется инверсным к A типа I с запаз-

дыванием n ($n \in \mathbf{N}$), если для каждого состояния z автомата A существует состояние $\tilde{z}$ автомата $\tilde{A}$ такое, что для любого слова uv с $|v|=n$ такого, что определено слово $g^*(z, uv)$, выполняется равенство $\tilde{g}^*(\tilde{z}, g^*(z, uv))=v'u$, где v' — подходящее слово длины n.

Докажите, что частичный автомат Мили A с $D_f=D_g$ тогда и только тогда является автоматом без потери информации конечного порядка типа I и имеет порядок не меньше n, когда он обладает инверсным автоматом $\tilde{A}$ типа I с запаздыванием $\tilde{n} \geqslant n$. Предложите метод построения инверсного автомата для данного автомата без потери информации конечного порядка типа I. [Указание. В качестве множества состояний автомата $\tilde{A}$ выберите $\{(z, w) \mid z \in Z, w \in F(X), |w| \leqslant \tilde{n}, g^*(z, u)=w$ для некоторого $u \in F(X)\}$.]

3. Покажите, что частичный автомат Мили с n состояниями не может быть автоматом без потери информации конечного порядка типа I и иметь порядок, больший чем $\frac{1}{2}n(n-1)$. Для каждого $n \geqslant 2$ существует сильно связный (см. упражнение 3.9) частичный автомат Мили A с $|X|=n$, $|Y|=\frac{1}{2}n(n-1)$ $\left(\text{или } |Y|=\frac{1}{2}n(n-1)+\left[\frac{(n+1)}{2}\right], \text{ если автомат A определен полностью}\right)$, являющийся автоматом без потери информации конечного порядка типа I и имеющий порядок $\frac{1}{2}n(n-1)$. [Указание. Искомый автомат определяется с помощью выбора некоторого произвольного состояния z_0, из которого, используя входные слова одинаковой длины, можно получать пары состояний z, z′ и действовать далее, как в указании к п. 1.]

4.7. Исследуйте, какие из состояний автоматов в примерах 4.1.1—4.1.3 являются L-эквивалентными, U-эквивалентными, V-эквивалентными или совместными.

4.8. (Гинзбург.) Покажите, что граница в теореме 4.2.14 точна, т. е. постройте для каждого n частичный автомат Мили с двумя несовместными состояниями z_1 и z_2, для которых при всех словах w из $F(X)$ с $|w| \leqslant \frac{1}{2}n(n-1)-1$ выполнено $\bar{g}^*(z_1, w) \sim \bar{g}^*(z_2, w)$.

4.9. (Томеску.) Докажите, что корректен следующий алгоритм для определения всех пар совместных состояний частичного автомата Мили A.

Пусть $A=(Z, X, Y, f, g)$, где $Z=\{z_1, \ldots, z_m\}$ и $X=\{x_1, \ldots, x_n\}$.

Определим булевы матрицы (т. е. матрицы из нулей и единиц) $A_1^{(0)}=\|a_{ij}\|_{m \times m}$ и $C_k=\|c_{ij}\|_{m \times m}$ при $k=1, \ldots, n$ следующим образом:

$a_{ij}=0$ тогда и только тогда, когда существует x в X такое, что $(z_i, x) \in D_g$, $(z_j, x) \in D_g$ и $g(z_i, x) \neq g(z_j, x)$;

$c_{ij}=0$ тогда и только тогда, когда $(z_i, x_k) \in D_f$ и $f(z_i, x_k) \neq z_j$.

Для произвольных квадратных булевых матриц $B=\|b_{ij}\|_{m \times m}$ и $B'=\|b'_{ij}\|_{m \times m}$ введем произведения $B \times B'=\|b_{i1}b'_{1j}+b_{i2}b'_{2j}+ \ldots +b_{im}b'_{mj}\|_{m \times m}$, где + означает логическое ИЛИ ($a+b=0$ тогда и только тогда, когда $a=b=0$);

$$B \cdot B'=\|b_{ij} \cdot b'_{ij}\|_{m \times m},$$

где · означает логическое И ($a \cdot b=1$ тогда и только тогда, когда $a=b=1$).

Пусть, далее, $B \leqslant B'$ тогда и только тогда, когда $b_{ij} \leqslant b'_{ij}$ при $1 \leqslant i, j \leqslant m$. B^T обозначает транспонированную матрицу $\|b_{ji}\|_{m \times m}$.

Построим для $p = 1, 2, \ldots$ и $q = 0, 1, 2, \ldots, n-1$ матрицы $A_p^{(q+1)} = A_p^{(q)} \times (C_{q+1} \times A_p^{(q)} \times C_{q+1}^T)$, $A_{p+1}^{(0)} = A_p^{(n)}$. Тогда $A_1^{(0)} \geqslant A_2^{(0)} \geqslant \ldots \geqslant A_r^{(0)} = A_{r+1}^{(0)}$, где $r \leqslant \frac{1}{2} m(m-1)$, $A_r^{(0)} = \| a_{ij}^{(r)} \|_{m \times m}$ — матрица совместимости для A, т. е. $a_{ij}^{(r)} = 1$ тогда и только тогда, когда состояния z_i и z_j совместны.

4.10. (Келла.) Докажите корректность следующего алгоритма определения всех состояний, не совместных с некоторым состоянием частичного автомата Мили.

Пусть $A = (\{z_1, \ldots, z_m\}, \{x_1, \ldots, x_n\}, Y, f, g)$ определен переходно-выходной таблицей (как в примере 4.2.3). Отметим, что такая таблица имеет n строк (по одной для каждого входа x_i) и m столбцов (по одному для каждого состояния z_j). Применение алгоритма приводит к присоединению к исходной таблице дополнительной строки — так называемой строки несовместности.

Алгоритм задается следующими шагами.

1. Начиная с $i=1$ и $k=2$, проверять для каждой пары z_i, z_k с $k>i$, выполнено ли при $j=1, \ldots, n$ включение $\{(z_i, x_j), (z_k, x_j)\} \subseteq D_g$ и, если это так, выполняется ли равенство $g(z_i, x_j) = g(z_k, x_j)$. Каждый раз, когда данное условие не выполнено, z_k заносится в i-й столбец строки несовместности.

2. Положить $i=1$, $j=1$.

3. Проверить, находится ли z_i в j-й строке. Если да, то перейти к шагу 4, иначе к шагу 5.

4. Просмотреть строку j и проверить, содержатся ли в ней состояния, находящиеся в i-м столбце в строке несовместности (т. е. состояния, про которые уже известно, что они несовместны с z_i). Если такое состояние z_k обнаружено в столбце s строки j и z_i встречается в столбце t строки j, то занести z_t в строку несовместности, причем если $t>s$, то в столбец s, а если $s>t$, то в столбец t.

5. Увеличить j на 1. Если $j>n$, то перейти к шагу 6, иначе к шагу 3.

6. Увеличить i на 1. Если $i>m$, то перейти к шагу 7, иначе положить $j=1$ и перейти к шагу 3.

7. Проверить, было ли на шаге 4 введено новое состояние в строку несовместности. Если да, то перейти к шагу 2, если нет, то к шагу 8.

8. Для $i=1, \ldots, m-1$ занести z_i в строку несовместности во все столбцы, для номеров k которых выполнено условие $k>i$ и z_k содержится в i-м столбце строки несовместности.

4.11.* Повторите рассуждения из разд. 4.3 для понятия L-эквивалентности вместо понятия U-эквивалентности.

4.12. (Гинзбург.) Докажите, что для любых двух состояний частичного автомата Мили разрешим вопрос: покрывает ли одно из них другое? Существует ли алгоритм, решающий этот вопрос и использующий только входные слова длины, меньшей чем $\frac{1}{2}n^2$ (n — число состояний автомата)? [Указание. Используйте теорему 4.2.14.]

4.13. Пусть A — частичный автомат Мили и A′ — автомат, минимальный для

A. Существует ли в точности одно (или много) преобразование из A в A′? Как формулируется соответствующий вопрос и каков ответ на него для полностью определенных автоматов Мили?

4.14. (Мюнтеферинг.) Существует ли частичный автомат Мили A с $D_f \subseteq U_g$, обладающий минимальным автоматом A′, полностью определенным и единственным с точностью до изоморфизма, если не существует однозначного преобразования из A в A′?

4.15. Выполняется ли условие из п.2 замечания к следствию 4.4.11, если выполнены предположение и условие 2) следствия 4.4.11? Иначе говоря, существует ли U-минимальный частичный автомат Мили A с всюду определенной функцией переходов, обладающий несокращенным доопределением A^+ таким, что некоторый эквивалентный автомату A^+ сокращенный автомат Мили является минимальным для A?

4.16. Покажите, что предположение в следствии 4.4.11 является необходимым, т. е. приведите пример частичного автомата Мили A с не всюду определенной функцией переходов, имеющего два доопределения A_1 и A_2 таких, что при $i = 1, 2$ эквивалентные автоматам A_i сокращенные автоматы Мили A'_1 являются минимальными для A, но A'_1 не изоморфен A'_2.

4.17.* Рассмотрите, как метод расщепления состояний из примера 4.4.5 связан с методом из следствия 4.5.9.

4.18. (Эрих.) Пусть A — частичный автомат Мили и для каждого состояния z автомата A пусть U_z — пересечение всех максимальных классов совместных состояний автомата A, содержащих z. Докажите, что каждая система множеств M над множеством состояний автомата A, составленная из максимальных классов совместных состояний ($M \subseteq M_A$), является h_A-замкнутой тогда и только тогда, когда для каждого максимального класса совместных состояний B (из M_A) и каждого входа x (из X) выполнено по меньшей мере одно из следующих условий:

1) $f(B, x) \subseteq B$, если $|f(B, x)| \geqslant 2$;

2) существует состояние z автомата A такое, что $z \notin B$ и $f(B, x) \subseteq U_z$.

ОБЗОР ЛИТЕРАТУРЫ

Не полностью определенные автоматы рассматривались уже в [20] и (более подробно) в [15] (обе работы из списка литературы к гл. 2). Как уже отмечалось в замечании к разд. 4.1, такие автоматы играют важную роль (кроме указанных в примерах случаев) при реализации автоматов. См. по этому поводу литературу из списка к гл. 2.

Пример 4.1.1 взят из работы [3].

Автомат из примера 4.1.2 (и автомат, который требуется построить в упражнении 4.2) — это в значительной степени LR(1)-анализатор. По поводу теории LR(k)-грамматик и LR(k)-анализаторов см., например, [9], по поводу распознавания ключевых слов в некотором слове — [1].

Пример 4.1.3 и упражнения 4.3 и 4.5 относятся к теории кодов (точнее — префиксных кодов), см. [16, 17, 21]. Обобщение автоматов для декодирования префиксных кодов представляют собой автоматы без потери информации — см. [12] (там можно найти аналог упражнения 4.6) и [18] (из списка литературы к гл. 2).

Понятие L-эквивалентности, содержание разд. 4.3 и упражнение 4.11 взяты из работы [2]. Понятие совместности введено в 1958 г. Ауфенкампом Теорема

4.2.14 и упражнение 4.8 взяты из [7] (см. также [7] из списка литературы к гл. 2). По поводу упражнения 4.9 см. [22], упражнения 4.10 — [11].

Содержание разд. 4.4 взято в основном из [13], так же как и упражнение 4.4. Понятие покрытия (в несколько иной форме) было введено в [7] (см. также [7] из списка литературы к гл. 2).

Пример 4.4.5 заимствован из [18] (из списка литературы к гл. 2). Определение 4.4.12 и теорема 4.4.13 восходят к работе [19], где, впрочем, рассматривалась иная модель автоматов.

Рассмотрение в разд. 4.5 базируется на работах [18] и [19], хотя там и рассматривалась иная проблема. О теории решеток см. [7].

Системы множеств в рамках теории автоматов использованы, в частности, в [10]. Пример 4.5.4, п.3 взят из [18] в списке литературы к гл. 2. Теорема 4.5.8 получена в основном в [15], теорема 4.5.12 — в [8]. Другие методы построения минимального автомата описаны в [18, 11 и 3]. Очень простой метод, описанный в виде программы на языке Фортран-4, можно найти в [14]. Иной сравнительно быстрый метод описан в [20]. По вопросу о методах поиска систем множеств см, например, [5]. Упражнение 4.18 взято из [4].

ГЛАВА 5.

АВТОМАТЫ РАБИНА — СКОТТА

5.1. ВВОДНЫЕ ПРИМЕРЫ

При многих исследованиях функционирования машин, процессов и алгоритмов бывает важен только вопрос о том, при каких обстоятельствах из некоторого определенного (начального) состояния может быть достигнуто определенное (конечное или финальное) состояние исследуемого объекта. В таких случаях оказывается избыточным использование модели автомата с выходами. Кроме того, не обязательно должны однозначно определяться результаты всех воздействий на объект, поскольку исследуется только возможность достижения определенного состояния. Ниже будет рассмотрен пример такого рода, связанный с задачей о распределении ресурсов в вычислительной системе, и пример из области программирования.

Два других примера должны продемонстрировать, что часто бывает проще и удобнее описывать метод решения в виде недетерминированного алгоритма — он может быть далее либо (вполне регулярным образом) обращен в обычный детерминированный алгоритм, либо непосредственно реализован на вычислительном устройстве, способном работать в параллельном режиме.

ТУПИКОВЫЕ СИТУАЦИИ В ПАРАЛЛЕЛЬНЫХ ПРОЦЕССАХ

Пример 5.1.1. Некоторая институтская библиотека имеет следующие «либеральные» правила выдачи литературы.

1) Каждый абонент может брать выбранные книги домой.

2) Не существует точных сроков возврата, т. е. абонент возвращает книгу в библиотеку только тогда, когда этого хочет.

3) Каждый читатель может брать одновременно несколько книг; он может, кроме того, оставлять заказ на книги и получать их, как только они будут возвращены в библиотеку.

Мы рассмотрим двух обычных студентов А и В, которым для их дипломных работ рекомендованы статьи из двух сборников. Студенты не знают друг друга и работают дома. Статьи, которые они начинают читать, они читают до тех пор, пока не поймут полностью их содержание.

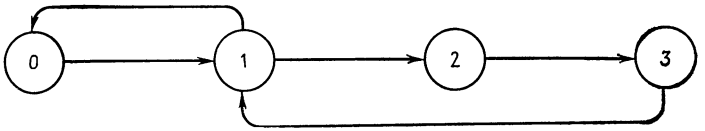


Рис. 5.1.1. Граф состояний студента

Будем считать, что статьи в сборниках «не замкнуты», т. е. что для понимания некоторой статьи из одного сборника может оказаться необходимой статья из другого. Студент, столкнувшийся с такой «незамкнутой» статьей, должен, таким образом, сохранять у себя сборник с этой статьей до тех пор, пока у него не окажется второго сборника и он не прочитает нужную статью.

Для того чтобы исследовать вопрос, являются ли правила работы библиотеки и поведение студентов разумными, т. е. не может ли возникнуть ситуация, когда ни один из студентов не сможет больше работать, полезно рассмотреть следующую модель.

Каждому студенту сопоставим «автомат», который может находиться в следующих четырех состояниях.

0: Ни один из сборников не получен и не заказан.

1: Получен один из сборников, второй не заказан.

2: Получен один из сборников, второй заказан.

3: Получены оба сборника.

Поведение каждого студента может быть тогда описано представленным на рис. 5.1.1 *графом состояний.* В этом графе идущие налево стрелки соответствуют возврату книги в библиотеку, а идущие направо — заказу или получению книги.

Для получения ответа на поставленный выше вопрос нужно рассмотреть различные возможные комбинации состояний «автоматов», соответствующих нашим студентам. С этой целью построим прямое произведение графов состояний, причем на ребрах будем указывать, действиям которого из студентов они отвечают. Отбрасывая невозможные сочетания состояний (скажем, состояние 3 для А и состояние 2 для В), получаем граф, изображенный на рис. 5.1.2.

Из рассмотрения графа состояний системы из двух «автоматов», соответствующих нашим студентам, сразу видно, что может возникнуть так называемая *тупиковая ситуация* — из ситуации 22

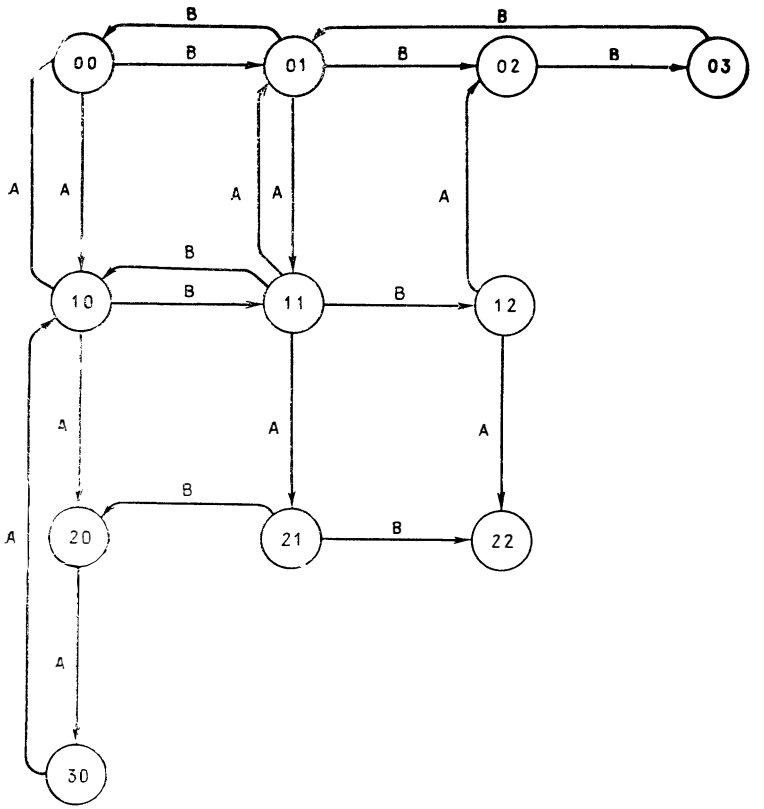


Рис. 5.1.2. Граф состояний системы

(оба студента получили по сборнику и каждый заказал сборник, находящийся у другого) при описанных условиях нет выхода. Граф дает возможность определить последовательность действий, приводящую из ситуации 00 в ситуацию 22. Множество всех таких последовательностей (конечной длины) бесконечно, в связи с чем возникает вопрос: может ли это множество быть описано с помощью конечного выражения, копии которого записываются одна за другой?

Отметим, что наш граф «недетерминирован»: последовательность ABAB может из 00 привести в 00, или в 02, или в 20, или в 22. Это обстоятельство порождает вопрос: существует ли детерминированный алгоритм (автомат с однозначной последовательностью работы), который:

1) устанавливает, что возникла тупиковая ситуация, или

2) своевременно предотвращает наступление тупиковой ситуации (т. е. запрещает некоторые действия в определенных ситуациях). К этому вопросу мы вернемся в примере 5.5.11.

По поводу других «библиотечных проблем» см. упражнение 5.1.

Пример 5.1.2. Рассматривается следующая программа P в обозначениях алгольного типа (при этом считается, что f и g — функции одного переменного, а p и q — одноместные предикаты [1]).

begin (x); Комментарий: в момент начала работы значение x должно уже быть определено.

$(y_1, y_2) := (x, x)$; Комментарий: присвоение значений переменным y_1 и y_2 производится одновременно.

M_1 : **if** $p(y_1)$ **then go to** M_2;

M_3 : **if** $q(y_2)$ **then go to** M_4;

$z := y_1$;

end (z); Комментарий: в этот момент выводится значение z.

$M_2 : y_1 := f(y_1)$;

go to M_1;

$M_4 : (y_1, y_2) := (g(y_1), f(y_2))$;

go to M_3;

Здесь опущены описания переменных, так как нас не будут интересовать ни значения x, ни значения функций и предикатов. В действительности нас будет интересовать только вопрос: какие вообще вычисления может проводить эта программа, т. е. какие в принципе результаты могут быть получены при произвольном x? При этом основное внимание будем уделять рассмотрению последовательностей из f и g, которые соответствуют функциям от подходящего x при подходящей интерпретации f и g, вычисляемым данной программой.

Определим с этой целью *язык значений* WS(P) программы P как множество всех таких последовательностей (последовательность длины 0 означает тождество):

WS(P) = {w из F({f, g}) | существует x такое, что (при некоторой интерпретации p, q, f и g) программа P при задании x прекращает работу через конечное число шагов и w оказывается возникшей при этом последовательностью из f и g, которой отвечает выход z = w(x)}.

Отметим, что P представляет целый класс программ, а именно все программы, которые получаются при фиксации области значений переменной x и при фиксации f и g (коротко: *при интерпретации* P). Таким образом, P оказывается «схемой программ». При некоторых интерпретациях не всем словам w из WS(P) могут соответствовать выходы.

Как и в предыдущем примере, для определения языка значений полезно по схеме программ строить (возможно, не детерминированный) граф, представляющий этот язык. Для этого занумеруем операции присвоения в схеме программ в порядке их появления.

---

[1] Т. е. отображения из области значений переменных в множество {истина, ложь}. — *Прим. перев.*

Граф вычислений BG(P) схемы P будет иметь при этом следующие вершины:

z_0: соответствует команде **begin**;

z_{ij}: i — текущий номер присвоения, j — индекс переменной y, стоящей в i-м присвоении слева, либо 0, если в i-м присвоении слева стоит z;

z_h: соответствует команде **end**.

Ориентированный граф для BG(P) и веса ребер этого графа определяются следующим способом.

Из каждой вершины z_{ij} помеченное символом Λ ребро ведет в z_0.

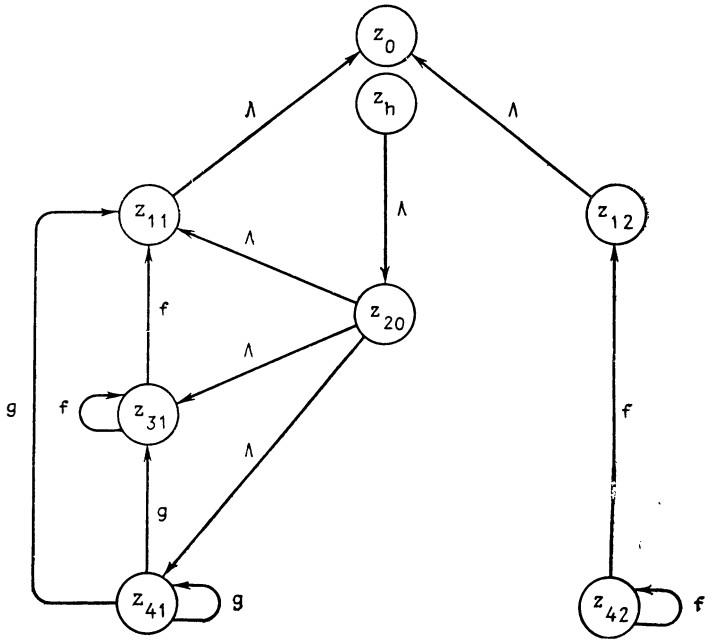


Рис. 5.1.3. Граф вычислений схемы программ P

Из вершины z_{km} ребро, помеченное символом u (где u — либо f, либо g, либо Λ), ведет в вершину z_{ij} в случае, если при соответствующем выборе входа x и соответствующей интерпретации встречающихся в программах предикатов и функций программа после присвоения с номером i в качестве следующего выполнит присвоение с номером k (проверив, возможно, между ними выполнение некоторых логических условий), при этом y_m или z получат значение $u(y_i)$.

Из вершины z_{ij} помеченное символом u ребро ведет в z_0, если в i-м присвоении y_j или z получает значение u(x) (u понимается, как и выше).

Из вершины z_h помеченные символом Λ ребра ведут в каждую вершину z_{i0}.

Данный метод позволяет построить для P граф BG(P), изображенный на рис. 5.1.3.

Язык значений WS(P) *схемы программ* P оказывается теперь множеством всех слов из F({f, g}), которые ведут в графе вычислений схемы из z_h в z_0 [слово w ведет из z_h в z_0, если в BG(P) существует путь из z_h в z_0 такой, что последовательность меток на проходимых ребрах совпадает с w]. Для P таким образом получаем

$$WS(P)=\{g^m f^n \mid m, n\in \mathbf{N}_0\}.$$

Легко заметить, что вершины z_{42} и z_{12} в BG(P) оказываются лишними и что даже вершины z_0, z_h и z_{20} могут быть удалены из графа (вместе с соответствующими ребрами), если получать WS(P) как множество слов, ведущих из z_{41}, из z_{31} или из z_{11} в z_{11}.

Замечание. Если изменить схему программ P, заменив во втором условном переходе q на p, то получится схема P′, для которой указанное выше сокращение не будет возможным. Цикл из M_3 через M_4 в M_3 в данном случае уже можно будет проходить не произвольное число раз, но ровно столько же раз, что и цикл из M_1 через M_2 в M_1. Язык значений схемы P′ будет, таким образом, подмножеством языка значений схемы P:

$$WS(P')=\{g^m f^m \mid m\in \mathbf{N}_0\}.$$

В разд. 5.4 будет показано, что данное множество не является языком значений какой-либо схемы программ, к которой применим описанный метод построения графа вычислений — см. следующее замечание.

Замечание. Описанный выше метод применим к схемам программ, удовлетворяющим следующим условиям:

используется только одна входная переменная x и одна выходная переменная z;

все встречающиеся функции одноместны; пусть X — множество всех встречающихся в схеме функций;

кроме x и z есть еще два множества переменных: $\{y_1, \ldots, y_k\}$ и $\{b_1, \ldots, b_n\}$, где b_i — булевы переменные;

используется только одна команда типа **begin**(x), непосредственно вслед за которой идет присвоение $(y_1, y_2, \ldots, y_k, b_1, b_2, \ldots, b_n) := (u_1(x), u_2(x), \ldots, u_k(x), \beta_1, \beta_2, \ldots, \beta_n)$, где $u_i\in F(X)$ при $i=1, \ldots, k$ и каждое β_i — булева константа («истина» или «ложь»);

каждое присвоение имеет вид $(y_1, \ldots, y_k, b_1, \ldots, b_n) := (u_1(\alpha_1), \ldots, u_k(\alpha_k), t_1(\beta_1), \ldots, t_n(\beta_n))$, где $u_i\in F(X)$, каждое t_i является булевым выражением, каждое α_i — это либо x, либо y_j, и каждое β_i — либо b_j, либо булева константа;

существует только одна команда типа **end**(z), а непосредственно перед ней стоит присвоение вида $z := u(\alpha)$, где $u\in F(X)$ и α равно либо x, либо некоторому y_j;

кроме присвоений используются только условные переходы вида

if $t(\beta)$ **then go to** M_1 **else go to** M_2

или

if $t(\beta)$ **then go to** M_1,

где t — булево выражение, β может быть равно булевой константе либо некоторому b_i, M_1 и M_2 — метки;

все операторы (кроме **begin** (x) и **end** (x)) могут иметь метки;

каждому пути в блок-схеме схемы программ из **begin**(x) в **end**(x) соответствует некоторое возможное вычисление (при подходящей интерпретации); два пути считаются при этом различными, если в них некоторое ребро проходится различное число раз.

Как и в схеме P, в общем случае допускается исключение тривиальных присвоений ($y_i := y_i$ или $b_i := b_i$).

НЕДЕТЕРМИНИРОВАННЫЙ АЛГОРИТМ КЛАССИФИКАЦИИ СЛОВ

Пример 5.1.3. Пусть дан алфавит, т. е. конечное множество X, например $X = \{1, 2, 3\}$.

Требуется построить алгоритм, который для слова w над X устанавливает, входят ли в w по меньшей мере два различных символа, причем хотя бы один — дважды. При этом предполагается, что алгоритм может считывать слово w посимвольно слева направо.

Мы хотим построить недетерминированный алгоритм. Он может иметь несколько выходных каналов. Задача считается решенной, когда решение появилось на одном из таких каналов.

Алгоритм состоит из одного (недетерминированного) управляющего алгоритма ST и (недетерминированных) распознающих алгоритмов U_i (при i из X). Пусть U_i — алгоритм, который определяет, встречается ли в еще не исследованной части слова w либо еще по меньшей мере один символ i и по меньшей мере один символ, отличный от i, либо по меньшей мере дважды встречается некоторый отличный от i символ j.

Алгоритм ST считывает символы слова w один за другим и, встречая символ i, включает в работу алгоритм U_i. Алгоритмы U_i могут работать параллельно. Если один из алгоритмов U_i установил требуемый факт, он должен сообщить об этом управляющему алгоритму ST, и весь алгоритм должен перейти в финальное состояние.

Каждый алгоритм U_i состоит из недетерминированно работающей части (управляющей) ST_i и трех параллельно работающих детерминированных распознающих алгоритмов U_{ij} ($j = 1, 2, 3$). Каждый алгоритм U_{ij} (при $j \neq i$) распознает, встречается ли в оставшейся части слова w по меньшей мере дважды символ j. Алгоритм U_{ii} распознает, встречается ли далее по меньшей мере один символ i и по меньшей мере один иной символ. При сообщении от одного из алгоритмов об установлении требуемого факта алгоритм U_i прекращает работу.

Алгоритмы U_{ij} могут быть, очевидно, описаны графами, приведенными на рис. 5.1.4, где $\{i, j, k\} = X$. Заштрихованные слева

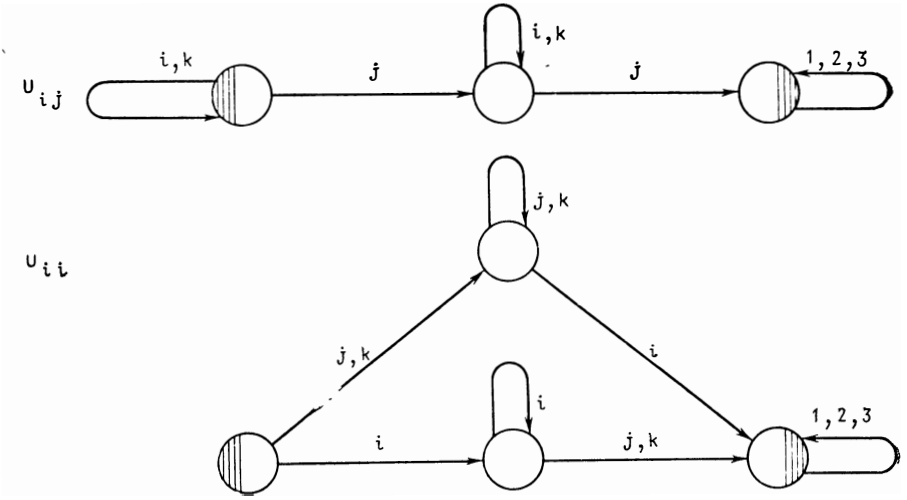


Рис. 5.1.4. Графы U_{ij} при $j \neq i$ и U_{ii}

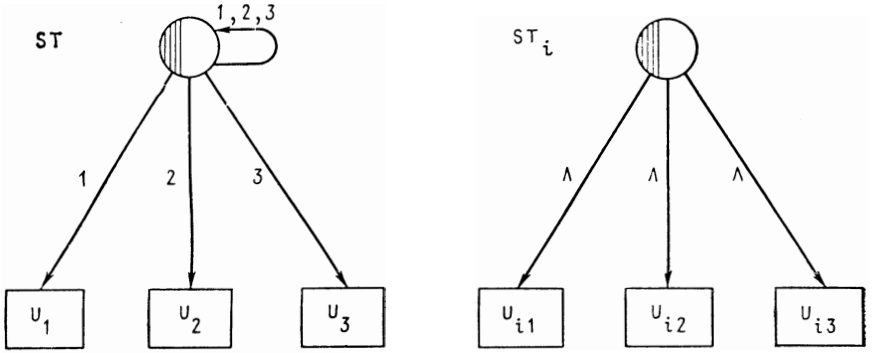


Рис. 5.1.5. Управляющие алгоритмы ST и ST_i

вершины указывают начальные состояния подалгоритмов, а заштрихованные справа — финальные.

Управляющие алгоритмы ST_i имеют одинаковый вид: не проверяя, какой знак поступил на вход, они вызывают алгоритмы U_{ij}. Итак, ST и ST_i имеют графы, показанные на рис. 5.1.5.

Полные графы алгоритмов U_i можно получить, заменяя в графе ST_i прямоугольники, обозначенные U_{i1}, U_{i2} и U_{i3}, графами соответствующих подалгоритмов. Граф всего алгоритма также можно получить, заменяя прямоугольники, помеченные символами U_1, U_2 и U_3, графами соответствующих алгоритмов. При подстановке графов должна быть убрана штриховка, указывающая на начальные состояния, поскольку начальным состоянием алгоритма всегда будет ST. Конечные вершины графов U_{ij} будут конечными вершинами общего алгоритма.

Чтобы установить, что некоторое слово w из F(X) обладает требуемым свойством, нужно, таким образом, найти некоторый путь из начальной в одну из конечных вершин графа алгоритма такой, чтобы последовательность меток на ребрах совпадала со словом w.

НЕДЕТЕРМИНИРОВАННЫЙ АЛГОРИТМ ДЛЯ СИНТАКСИЧЕСКОГО АНАЛИЗА

Пример 5.1.4. Синтаксис языка программирования высокого уровня задается с помощью формы Бэкуса — Наура или аналогичных конструкций (см. разд. 3.1 и 4.1). Для определенных фрагментов программ непосредственно из их определения можно получить (недетерминированные) алгоритмы, способные устанавливать, соответствует ли данный фрагмент программы данному определению. Это будет показано на примере одного определения *заголовка процедуры* из языка программирования Паскаль.

Это определение выглядит так:

<PROCEDURE HEADING>::=PROCEDURE<IDENTIFIER>; |
PROCEDURE<IDENTIFIER>
(<FORMAL PARAMETER
SECTION>{;<FORMAL PARAME-
TER SECTION>});

<FORMAL PARAMETER SECTION>::=<PARAMETER GROUP>|
VAR <PARAMETER GRO
UP> | [FUNCTION <PA-
RAMETER GROUP> |
PROCEDURE <IDENTIFI-
ER> {, <IDENTIFIER>}

<PARAMETER GROUP>::=<IDENTIFIER>{,<IDENTIFIER>}:
<TYPE IDENTIFIER>

<TYPE IDENTIFIER>::=<IDENTIFIER>

<IDENTIFIER>::=<LETTER><LETTER OR DIGIT>*

<LETTER OR DIGIT>::=<LETTER> | <DIGIT>

При этом фигурные скобки {, } означают, что заключенная между ними последовательность символов может повторяться сколько угодно раз (в том числе ни одного раза), а звездочка * означает, что помеченная ею металингвистическая переменная также может повторяться произвольно много раз (и тоже в том числе ни одного раза).

Искомый алгоритм РК состоит из подалгоритмов, которые вызываются одновременно и могут работать параллельно. Когда алгоритму предлагается фрагмент программы, он прочитывает этот фрагмент последовательно слева направо. Если фрагмент начина-

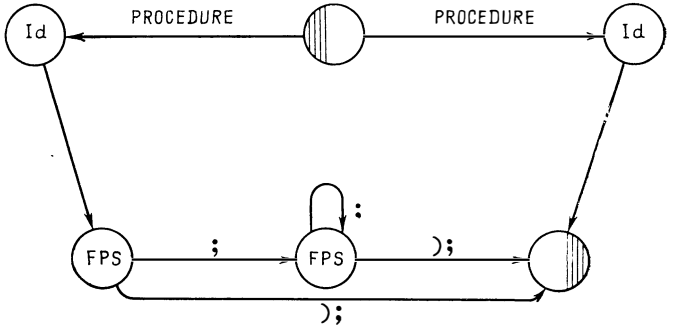


Рис. 5.1.6. Граф РК

ется с PROCEDURE, то вызываются два подалгоритма U_1 и U_2:

U_1 устанавливает, имеет ли последующий текст вид ⟨IDENTIFIER⟩;

U_2 устанавливает, имеет ли последующий текст вид, соответствующий второму варианту из определения.

U_2 прежде всего вызывает подалгоритм Id, который устанавливает, следует ли за ⟨IDENTIFIER⟩ какая-либо последовательность символов. Если такая последовательность начинается со знака (, то вызывается подалгоритм FPS, который устанавливает, следует ли дальше последовательность символов ⟨FORMAL PARAMETER SECTION⟩.

Аналогично может быть детально описана работа подалгоритма U_1. Подалгоритм FPS функционирует также недетерминированным образом. Перед проверкой следующего символа он вызы-

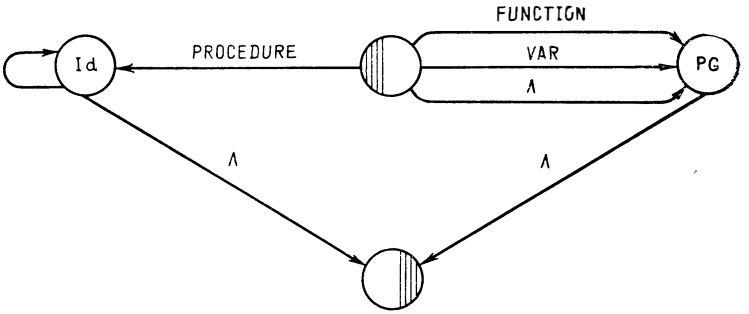


Рис. 5.1.7. Граф FPS

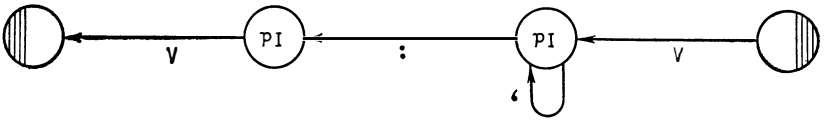


Рис. 5.1.8. Граф PG

вает подалгоритм PG, который реагирует на последовательность символов, отвечающую металингвистической переменной ⟨PARAMETER GROUP⟩, и работает параллельно с другими вызванными FPS подалгоритмами. После того как алгоритм FPS вызвал алгоритм PG, он проверяет, имеет ли начальная часть последовательности знаков вид VAR, FUNCTION или PROCEDURE. Если да, то он вызывает соответствующий подалгоритм, и так далее.

Ради наглядности граф алгоритма PK приведен на рис. 5.1.6 не детально, а только до уровня вызова подалгоритмов. Общий граф можно получить, «вставляя» в приведенный граф алгоритма PK графы алгоритмов Id и FPS.

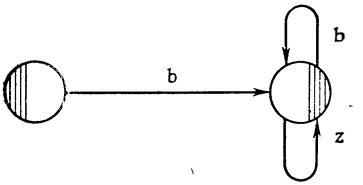


Рис. 5.1.9. Граф Id

Аналогичным образом изображен на рис. 5.1.7 граф алгоритма FPS.

Заштрихованные слева вершины являются начальными, заштрихованные справа — конечными.

Последовательность символов); на ребрах, ведущих в конечную вершину графа алгоритма PK, означает, что оба знака должны встретиться в заданной последовательности.

Граф алгоритма FPS «вставляется» в граф алгоритма PK следующим образом. Каждая помеченная символами FPS вершина графа алгоритма PK заменяется графом с рис. 5.1.7, причем ведущие в заменяемую вершину ребра присоединяются к начальной вершине графа с рис. 5.1.7, а исходящие из заменяемой вершины присоединяются к конечной вершине. Штриховка вершин «вставляемого» графа при этом убирается.

На рис. 5.1.8 и 5.1.9 приведены графы алгоритмов PG и Id. Поясним только, что здесь b — произвольная (допустимая в языке Паскаль) буква, а z — произвольная цифра.

5.2. НЕДЕТЕРМИНИРОВАННЫЕ АВТОМАТЫ РАБИНА — СКОТТА (НРС-АВТОМАТЫ)

Из рассмотренных выше примеров мы прежде всего получим определение в общем виде автоматов Рабина — Скотта, а потом более детально рассмотрим вопрос об их функционировании.

ОПРЕДЕЛЕНИЕ НРС-АВТОМАТОВ

Как показывают примеры 5.1.1—5.1.4, с практической точки зрения процессы в системах, управляющие элементы (например, программы) или алгоритмы часто полезно описывать «недетерминированными» графами. Эти графы мы можем по аналогии с теорией, изложенной в предыдущих главах, рассматривать как представления автоматов, а именно как представления автоматов без выходов и со специальными начальными и финальными состояниями. Такие автоматы функционируют недерминированным об-

разом, т. е. при данном состоянии и данном входе (который может быть и последовательностью отдельных входов) состояние, которое должен принять автомат, может быть определено неоднозначно, так что автомат может «выбирать» между возможными переходами в следующее состояние. Такие автоматы могут изменять свое состояние спонтанно, т. е. не получая никакого входа.

Определение 5.2.1. (Конечный) *недетерминированный автомат Рабина — Скотта* (НРС-автомат) есть пятерка $A=(Z, X, t, S, F)$. Здесь Z и X — конечные множества (*состояний* и *входов* соответственно; X называют также входным алфавитом автомата A); S и F — подмножества множества Z (множества *начальных* и *финальных* состояний соответственно); $t=(Z\times F(X), Z, \tau)$, где τ — конечное подмножество множества $Z\times F(X)\times Z$, т. е. t — соответствие из $Z\times F(X)$ в Z (иначе говоря, t — многозначное отображение из $Z\times F(X)$ в Z с конечной областью определения), называемое *соответствием переходов*.

Элементы множества τ называются *переходами*. Множество

$$\tau_s=(\tau\cap Z\times\{\Lambda\}\times Z)-\{(z, \Lambda, z)\mid z\in Z\}=$$
$$=\{(z, \Lambda, z')\mid (z, \Lambda, z')\in\tau, z\neq z'\}$$

называется множеством *спонтанных переходов*.

Автомат A называется *алфавитным*, если $\tau\subseteq Z\times(X\cup\Lambda)\times Z$. Для алфавитных НРС-автоматов всегда предполагается, что все входы существенны, т. е. что $X\subseteq pr_2\tau$.

Автомат A будем называть *побуквенным*, если он алфавитный и не имеет спонтанных переходов.

Переход (z, w, z') из τ означает, что A при поступлении на вход слова w может перейти из состояния z в состояние z', но при этом допускается, что в τ содержатся и другие переходы вида (z, w, z'') с $z''\neq z'$. Задание переходов вида (z, Λ, z), очевидно, бесполезно — такие переходы могут быть удалены из τ. Множество всех состояний, в которые автомат может перейти из некоторого состояния z при поступлении на вход слова w, есть $t(z, w)$.

Замечание. НРС-автомат A может быть представлен ориентированным взвешенным графом. При этом в качестве вершин выбирают состояния автомата A, ребро с меткой w проводят из z в z', если (z, w, z') — переход автомата A. Метку Λ можно опустить. Такие графы мы будем иногда называть переходными системами.

Ясно, что графы из примеров 5.1.1—5.1.4 можно рассматривать как графы НРС-автоматов, причем (за исключением графа из примера 5.1.4) как графы алфавитных НРС-автоматов. Автомат с графом из примера 5.1.1 оказывается даже побуквенным.

Замечание. Пусть t — соответствие переходов некоторого НРС-автомата A и τ — его график. Каждое входное слово w из $pr_2\tau$ определяет тогда соответствие $t_w=(Z, Z, pr_{1,3}(\tau\cap Z\times\{w\}\times Z))$ из Z в себя ($pr_{1,3}$ обозначает проекцию на первую и третью компоненту). График t_w соответствует множеству всех ребер гра-

фа A с меткой w и описывает все возможные изменения состояний при поступлении на вход слова w. Таким образом, НРС-автомат можно определить, задав множество состояний (вместе с подмножествами начальных и финальных состояний) и конечное множество соответствий t_w из Z в Z, где t_w описывают все возможные реакции автомата A на соответствующие входные слова w.

ПОВЕДЕНИЕ НРС-АВТОМАТОВ

Нашей целью будет описание поведения НРС-автоматов при обработке некоторой последовательности входов.

Определение 5.2.2. Пусть A — НРС-автомат в обозначениях определения 5.2.1. Положим

$\tau^1=\tau$;

$\tau^{n+1}=\{(z, wv, z') \mid$ существует $z''\in Z$ такое, что $(z, w, z'')\in\tau^n$ и $(z'', v, z')\in\tau\}$ — для всех $n\in\mathbf{N}$;

$\tau^0=\{(z, \Lambda, z) \mid z\in Z\}$;

$\tau^*=\bigcup\{\tau^i \mid i\in\mathbf{N}_0\}$.

Определим t^* как соответствие с графиком τ^*, т. е.

$t^*=(Z\times F(X), Z, \tau^*)$.

Это соответствие будем называть *последовательностным соответствием* автомата A.

Замечание 1. Состояние z' принадлежит $t^*(z, w)$, если автомат A при пошаговой обработке слова w может перейти из состояния z в состояние z' (причем некоторые переходы могут, вообще говоря, быть спонтанными). Иначе говоря, это происходит в том случае, когда в графе автомата A существует путь из z в z' такой, что последовательность меток на проходимых ребрах составляет слово w. Действительно, очевидно, что переход (z, w, z') принадлежит τ^n, если в графе автомата A существует путь из z в z' длины n такой, что последовательность меток на ребрах, составляющих этот путь, совпадает с w. Таким образом, если у A нет спонтанных переходов и нет тривиальных переходов вида (z, Λ, z), то $\tau^n\cap Z\times X^m\times Z=\varnothing$ при $n>m\geqslant 0$. Если же автомат A является еще и алфавитным, т. е. в данном случае — побуквенным, то $\tau^n\cap Z\times X^m\times Z$ не пусто тогда и только тогда, когда $m=n\neq 0$.

2. Для алфавитных НРС-автоматов можно доказать, что при произвольных v и w из F(X) и произвольном z из Z выполняется равенство

$t^*(z, vw)=t^*(t^*(z, v), w)=\{z''\in Z \mid$ существует $z'\in t^*(z, v)$ такое, что $z''\in t^*(z', w)\}$

(см. теорему 2.3.2). Этот факт будет также получен в доказательстве п.2 теоремы 5.2.3. Если рассматриваемый НРС-автомат не является алфавитным, то, конечно, данное равенство может не

выполняться, так как множество $t(z, vw)$ может вообще не содержаться в $t^*(t^*(z, v), w)$.

t^* содержит всю существенную информацию о способе функционирования соответствующего автомата A. Хотя множество τ^* бесконечно, нам достаточно, однако, знать только некоторое конечное его подмножество (этот факт будет вскоре получен), и ниже мы увидим, что все множество τ^* может быть описано с использованием «конечных» средств.

Замечание. В дальнейшем, если не оговорено противное, всегда A — HPC-автомат в смысле определения 5.2.1 и X — некоторое конечное множество.

МОНОИД ПЕРЕХОДОВ АЛФАВИТНОГО HPC-АВТОМАТА

Каждая входная последовательность определяет (как это уже было установлено выше для отдельных входов) соответствие из множества состояний в себя. Совокупность таких соответствий описывает целиком поведение автомата A.

Замечание. Соответствия могут применяться последовательно, как обычные отображения (т. е. можно образовывать суперпозиции соответствий); правда, может оказаться, что суперпозиция двух непустых соответствий является пустым соответствием. Множество с ассоциативной (бинарной) операцией, называемой по большей части умножением, обладающее относительно этой операции единичным (нейтральным) элементом, называется, как известно, моноидом. Сюръективное отображение одного моноида на другой называется моноидным эпиморфизмом, если оно является гомоморфизмом, т. е. сохраняет операцию (произведение образов равно образу произведения) (см. гл. 1).

Теорема 5.2.3 (теорема о моноиде переходов). Пусть A — алфавитный HPC-автомат с n состояниями. Для каждого w из $F(X)$ пусть $t^*_w=(Z, Z, \tau^*_w)$ — соответствие из Z в Z с графиком $\tau^*_w=$ $=\mathrm{pr}_{1,3}(\tau^* \cap Z\times\{w\}\times Z)=\{(z, z') \mid (z, w, z')\in\tau^*\}$. Пусть, далее, $Q=2^{n^2}$. Тогда:

1. Для каждого w из $F(X)$ воздействие спонтанных переходов ограничено числом Q, т. е.

$$\tau^*_w=\bigcup\{\mathrm{pr}_{1,3}(\tau^i \cap Z\times\{w\}\times Z) \mid i=|w|,\ |w|+1,\ \ldots,\ Q|w|+Q-1\}.$$

2. С суперпозицией соответствий в качестве моноидной операции множество $T(A)=\{t_w^* \mid w\in F(X)\}=\{t_v^* \mid |v|<Q\}$ является конечным моноидом, так называемым *моноидом переходов* автомата A.

3. Отображение $h\colon F(X)\to T(A)$, где $h(\tilde{w})=t_w^*$ (т. е. $h(w)=$ $=t^{\bullet}_{\tilde{w}}$ и $\tilde{w}$—*зеркальное слово* для w (т. е. при $|w|\leqslant 1$ $\tilde{w}=w$ и при $w=ux$ $\tilde{w}=x\tilde{u}$; см. упражнение 3.13), является моноидным эпиморфизмом.

Замечания. 1. Соответствие t_w^* определяет, в какие состояния может перейти состояние данного автомата при поступлении

на вход слова w; t_w^* оказывается гомоморфным образом $\tilde{w}$, а не w, поскольку суперпозиции соответствий записываются так, что $t_u^* t_v^* = t_{vu}^*$.

2. Из утверждений 1 и 2 теоремы вытекает, что для любого A множество T(A) может быть построено за конечное число шагов (см. упражнение 5.2 и относящуюся к нему литературу). Отметим, что Q при детальном анализе A может быть заменено на меньшую границу.

Доказательство теоремы. Пусть для каждого w из F(X) и каждого i из $\mathbf{N}_0$ соответствие $t_{w,i}$ из Z в Z задается графиком $\tau_{w,i} = pr_{1,3}(\tau^i \cap Z \times w \times Z)$. Очевидно, что $\tau_{w,i} = \varnothing$ при $i < |w|$.

Докажем теперь полной индукцией по $|w|$, что

$$\tau_w^* = \cup\{\tau_{w,i} \mid |w| \leqslant i < Q|w| + Q\}.$$

Пусть $w = \Lambda$. Тогда для каждого i из $\mathbf{N}_0$ имеем $t_{\Lambda,i} = t_\Lambda^i$. Поскольку только Q соответствий из Z в Z могут быть попарно различны, то не могут быть попарно различными соответствия t_Λ^i при $i = 0, 1, \ldots, Q$; т. е. существуют p и q такие, что $0 \leqslant p < q \leqslant Q$ и $t_\Lambda^p = t_\Lambda^q$. Отсюда полной индукцией по j из $\mathbf{N}$ получаем, что $t_\Lambda^{p+j(q-p)} = t_\Lambda^p$.

Пусть k — произвольное число из $\mathbf{N}$ и r — остаток при делении k на q—p, т. е. $k = m(q-p) + r$. Тогда $t_\Lambda^{p+k} = t_\Lambda^{p+r}$ и $p + r < q$. Так что $\tau_\Lambda^* = \cup\{\tau_{\Lambda,i} \mid 0 \leqslant i < Q\}$.

Допустим теперь, что утверждение справедливо для всех слов w длины $j \geqslant 0$. Для $w' = wx \in F(X)$, где $x \in X$ и $|w| = j$, в этом случае имеем (напомним, что автомат A — алфавитный по предположению)

$$\begin{aligned}
\tau_{wx}^* = \{(z, z') \mid & \text{ существуют } z_1, z_2 \in Z \text{ и } i, j \in \mathbf{N}_0 \text{ такие, что} \\
& (z, w, z_1) \in \tau^i, (z_1, x, z_2) \in \tau, (z_2, \Lambda, z') \in \tau^j\} = \\
= \{z, z') \mid & \text{ существуют } z_1, z_2 \in Z \text{ и } i, j \in \mathbf{N}_0 \text{ такие, что } (z, z_1) \in \\
& \in \tau_{w,i}, (z_1, z_2) \in \tau_{x,1}, (z_2, z') \in \tau_{\Lambda,j} \text{ и} \\
& |w| \leqslant i < Q|w| + Q, 0 \leqslant j < Q\} = \\
= \cup\{\tau_{wx,k} \mid & |wx| \leqslant k < Q|wx| + Q\}.
\end{aligned}$$

Итак, утверждение 1 доказано.

Из предыдущих утверждений, кроме того, вытекает равенство $\tau_{wx}^* = \{(z, z') \mid$ существуют $z'' \in Z$ и $r, s \in \mathbf{N}$ такие, что $(z, z'') \in \in \tau_{w,r}$ и $(z'', z') \in \tau_{x,s}$, причем $|w| \leqslant r < Q|w| + Q$ и $1 \leqslant s < 2Q\}$.

Отсюда с учетом 1 следует, если применить операцию объединения множеств к соответствиям (а не только к их графикам; см. гл. 1), что

$$t_{wx}^* = \cup\{t_{x,s} t_{w,r} \mid 1 \leqslant s < 2Q, \ |w| \leqslant r < Q|w| + Q\} = t_x^* t_w^*.$$

Аналогичным образом (заменяя x на Λ) получаем $t_\Lambda^* t_w^* = = t_w^*$.

Докажем теперь утверждение 3 теоремы.

Поскольку h, очевидно, является сюръекцией, нам остается только показать, что для произвольных u и v из F(X) выполнено $\tau_{uv}^* = t_v^* t_u^*$, так как отсюда следует, что $h(\tilde{uv}) = t_{uv}^* = t_v^* t_u^* = h(\tilde{v})h(\tilde{u})$, а это вследствие равенства $\tilde{v}\tilde{u} = \widetilde{vu}$ и означает, что h — гомоморфизм (поскольку вместе с u и v также и $\tilde{u}$ и $\tilde{v}$ пробегают весь моноид F(X)). Мы докажем наше утверждение полной индукцией по длине слова v при постоянном, но произвольном слове u.

При $|v|=0$, т. е. при $v=\Lambda$, утверждение уже доказано выше.

Допустим, что утверждение верно для всех v длины $k \geqslant 0$. Пусть, далее, $v' = vx \in F(X)$, где $|v|=k$ и $x \in X$. Тогда из высказывания, доказанного после доказательства утверждения 1 (и используемого сначала при $w=v$ и потом при $w=uv$), следует

$$t^*_{vx} t^*_u = t^*_x t^*_v t^*_u = t^*_x t^*_{uv} = t^*_{uvx}.$$

Поскольку гомоморфный образ моноида снова является моноидом, то T(A) как образ F(X) при гомоморфизме h оказывается моноидом.

Для того чтобы доказать конечность множества T(A), положим, что $m > Q$ и $w = x_1 \ldots x_m$, где $x_i \in X$, и что $w_0 = \Lambda$ и $w_i = x_1 x_2 \ldots x_i$ при $i = 1, \ldots, m$. Соответствия t^*_{wi} не могут быть все попарно различны, т. е. существуют по меньшей мере два неотрицательных целых числа i и j, $i<j$, такие, что $t^*_{w_i} = t^*_{w_j}$. Поэтому существует по меньшей мере одно слово v с $|v|<|w|$ такое, что $t^*_v = t^*_w$ (а именно $v = w_i x_{j+1} \ldots x_m$). Для кратчайшего слова v с этим свойством выполнено неравенство $|v|<Q$, так как иначе слово v могло бы быть укорочено так же, как и слово w. Тем самым доказано и утверждение 2. ■

Замечание. t^*_Λ есть единичный элемент в T(A), хотя t_Λ и не является, вообще говоря, тождественным отображением (это верно только в том случае, когда у A нет спонтанных переходов).

Отметим далее, что соответствие t_x при $x \in X$ может отличаться от t^*_x, если у A есть спонтанные переходы. Если, скажем, t_x — тождественное отображение Z на себя, то $t^*_x = t^*_\Lambda$.

Пример 5.2.4. Пусть

$A = (\{z_0, z_{11}, z_{12}, z_{20}, z_{31}, z_{41}, z_{42}, z_h\}, \{f, g\}, t, z_h, z_0)$ — НРС-автомат из примера 5.1.2. Тогда

$$T(A) = \{t^*_\Lambda, t^*_f, t^*_g, t^*_{fg}, t^*_{gf}\}.$$

Умножение в T(A) с учетом выполнения для всех u и v из $F(\{f, g\})$ условия $t^*_u t^*_v = t^*_{vu}$ полностью определяется следующими равенствами: $t^*_f t^*_f = t^*_f$, $t^*_g t^*_g = t^*_g$ и $t^*_{fg} t^*_g = t^*_{fg} = t^*_f t^*_{fg}$. Действительно, первые два равенства позволяют каждое t_w с $|w| \geqslant 3$ свести к t^*_u, где u имеет один из видов $(fg)^i$, $g(fg)^i$, $(fg)^i f$ или $g(fg)^i f$ при $i \geqslant 1$. Такие t^*_u сводятся с помощью третьего равенства к t^*_{fg}.

Элементы T(A) описываются таблицей, приведенной на рис. 5.2.1.

	t^*_Λ	t^*_f	t^*_g	t^*_{fg}	t^*_{gf}
z_0	z_0	∅	∅	∅	∅
z_{11}	z_0, z_{11}	∅	∅	∅	∅
z_{12}	z_0, z_{12}	∅	∅	∅	∅
z_{20}	$z_0, z_{11}, z_{20}, z_{31}, z_{41}$	z_0, z_{11}, z_{31}	$z_0, z_{11}, z_{31}, z_{41}$	∅	z_0, z_{11}, z_{31}
z_{31}	z_{31}	z_0, z_{11}, z_{31}	∅	∅	∅
z_{41}	z_{41}	∅	$z_0, z_{11}, z_{31}, z_{41}$	∅	z_0, z_{11}, z_{31}
z_{42}	z_{42}	z_0, z_{12}, z_{42}	∅	∅	∅
z_h	$z_0, z_{11}, z_{20}, z_{31}, z_{41}, z_h$	z_0, z_{11}, z_{31}	$z_0, z_{11}, z_{31}, z_{41}$	∅	z_0, z_{11}, z_{31}

Рис. 5.2.1. Моноид переходов НРС-автомата из примера 5.1.2

НРС-АВТОМАТЫ КАК ПОРОЖДАЮЩИЕ СИСТЕМЫ; ПРАВОЛИНЕЙНЫЕ ГРАММАТИКИ

Как показывают примеры 5.1.2 и 5.1.4, НРС-автомат (с $Z \cap X = \varnothing$) можно рассматривать как систему для порождения последовательностей символов. Переходы (z, w, z') можно при этом считать порождающими правилами вида «заменить z на wz'» (символическая запись: $z \to wz'$). Каждое финальное состояние может быть удалено с помощью правила вида «заменить z на Λ» (иначе: $z \to \Lambda$). Любое порождаемое такой системой слово получается, если, начав с некоторого состояния z из множества начальных состояний S, применять одно за другим имеющиеся правила (в любом порядке) до тех пор, пока не получится слово, не содержащее символа состояния.

Соответствующая НРС-автомату A порождающая система (называемая *праволинейной грамматикой*) является, таким образом, четверкой $G = (Z, X, R, S)$, где Z и X — дизъюнктные конечные множества, $S \subseteq Z$ и R — конечное множество так называемых *правил* (или *продукций*) вида $z \to wz'$ или $z \to \Lambda$ при z и z' из Z и w из $F(X)$.

Пусть $z \in Z$, $u \in F(X)$ и $v \in F(X \cup Z)$. Слово v называется *непосредственно выводимым* из uz в G (символическая запись:

$uz \Rightarrow_G v$), если выполнено следующее условие: при $v \in F(X)$ справедливо равенство $v = u$, а в R имеется правило $z \to \Lambda$; в противном случае $v = uwz'$, а в R имеется правило $z \to wz'$.

Пусть u, v, z имеют тот же смысл, что и в предыдущем абзаце. Слово v называется *выводимым* из uz в G (символическая запись: $uz \Rightarrow_G^* v$), если $uz = v$ или существует конечная последовательность слов w_i, $i = 1, \ldots, n$, такая, что $w_1 = uz$, $w_n = v$ и $w_j \Rightarrow_G w_{j+1}$ при $j = 1, \ldots, n-1$.

Языком, порождаемым грамматикой G, называется множество слов

$$L(G) = \{w \in F(X) \mid \text{существует } z \text{ в } S \text{ такое, что } z \Rightarrow_G^* w\}.$$

Праволинейные грамматики часто определяют, требуя, чтобы выполнялось равенство $|S| = 1$, и допуская правила вида $z \to w$, где $w \in F(X)$. Эквивалентность такого определения приведенному выше будет установлена в разд. 5.5.

Пример 5.2.5. НРС-автомат A, определенный графом на рис. 5.1.3 порождает следующую праволинейную грамматику G: $G = (\{z_0, z_{11}, z_{12}, z_{20}, z_{31}, z_{41}, z_{42}, z_h\}, \{f, g\}, R, z_h)$, где R состоит из следующих правил (ради краткости мы, как при использовании формы Бэкуса—Наура, объединяем два правила $z \to u$ и $z \to v$ в одно $z \to u \mid v$):

$$z_h \to z_{20};\ z_{20} \to z_{11} \mid z_{31} \mid z_{41};\ z_{11} \to z_0;$$
$$z_{31} \to fz_{31} \mid fz_{11};\ z_{41} \to gz_{41} \mid gz_{31} \mid gz_{11};$$
$$z_{42} \to fz_{42} \mid fz_{12};\ z_{12} \to z_0;\ z_0 \to \Lambda.$$

Слово g^3f^2 выводится, например, из z_h следующим образом:

$$z_h \Rightarrow z_{20} \Rightarrow z_{41} \Rightarrow gz_{41} \Rightarrow ggz_{41} \Rightarrow gggz_{31} \Rightarrow$$
$$\Rightarrow g^3fz_{31} \Rightarrow g^3f^2z_{11} \Rightarrow g^3f^2z_0 \Rightarrow g^3f^2.$$

Приведенные порождающие правила могут быть записаны и как формулы в форме Бэкуса—Наура (см. пример 5.1.4). Вместо $z \to wz'$ можно писать $\langle z \rangle ::= w\langle z' \rangle$ и вместо $z \to \Lambda$ — $\langle z \rangle ::= \Lambda$.

5 3. РЕАКЦИЯ, ДОПУСТИМЫЕ МНОЖЕСТВА

Определим теперь понятие реакции НРС-автомата и получим его описание алгебраическими средствами.

НРС-автомат не реализует никакого отображения, но классифицирует входные слова на допустимые и недопустимые. Входное слово w допускается данным НРС-автоматом A, если A может перейти из одного из начальных в одно из финальных своих состояний при введении слова w, иными словами, если в графе автомата A существует путь из одной из начальных вершин в одну из конечных вершин такой, что последовательность меток на проходимых ребрах совпадает с данным входным словом.

РЕАКЦИЯ, ДОПУСТИМЫЕ МНОЖЕСТВА

Для задания реакции некоторого НРС-автомата достаточно, как следует из вышесказанного, определить множество всех допустимых входных слов.

Определение 5.3.1. 1. *Реакцией* автомата A (или *множеством, допустимым* автоматом A) называется множество $L(A) = \{w \in F(X) \mid t^*(S, w) \cap F \neq \varnothing\}$.

2. Пусть X — конечное множество. Подмножество L множества F(X) называется *H-допустимым*[1] множеством, если существует НРС-автомат A с $L = L(A)$. Символом NAkz(X) будет обозначаться множество всех H-допустимых подмножеств множества F(X).

Замечание. Условие $t^*(S, w) \cap F \neq \varnothing$ означает: существуют последовательность $z_0, z_1, \ldots, z_n$ состояний и последовательность $u_1, u_2, \ldots, u_n$ слов из F(X) такие, что $z_0 \in S$, $z_n \div F$, $(z_{i-1}, u_i, z_i) \in \tau$ при $i = 1, \ldots n$ и $w = u_1 u_2 \ldots u_n$. Пустое слово Λ допустимо, если $S \cap F \neq \varnothing$. Для графа автомата A рассматриваемое условие означает, что существует путь из некоторого начального в некоторое финальное состояние такой, что последовательность меток на ребрах вдоль этого пути составляет w.

Пример 5.3.2. 1. Пусть A — НРС-автомат из примера 5.1.1. Тогда L(A) — множество всех последовательностей действий студентов, которые могут привести из начальной ситуации (ни один не заказал и не получил ни одного сборника) в тупиковую ситуацию.

2. Пусть A — НРС-автомат из примера 5.1.2 (см. также пример 5.2.4). Тогда $L(A) = \{g^m f^n \mid m, n \in \mathbf{N}_0\} = WS(P)$.

3. Пусть A—НРС-автомат из примера 5.1.3. Тогда L(A) является множеством слов над {1, 2, 3}, в которых встречаются по меньшей мере две различные цифры и при этом по меньшей мере одна цифра встречается более одного раза.

4. Пусть A — НРС-автомат из примера 5.1.4. Тогда L(A) является множеством всех допустимых заголовков процедур в языке Паскаль.

5. Если G — сопоставленная автомату A соответственно замечанию в конце разд. 5.2 праволинейная грамматика, то $L(G) = L(A)$.

Дальнейшие примеры содержатся в упражнении 5.3.

РАЦИОНАЛЬНЫЕ МНОЖЕСТВА[2]

H-допустимые множества могут быть построены из конечных множеств. С этой целью мы дадим конструктивное определение одного класса множеств. Более строгое определение содержится в п. 3 упражнения 5.7.

Определение 5.3.3. Множество Rat(X) *рациональных* подмножеств F(X) есть наименьшее подмножество $\mathscr{R}$ булеана $\mathscr{P}(F(X))$ [т. е. множества всех подмножеств множества F(X)] со следующими свойствами.

---

[1] Сокращение от «допустимым недетерминированным автоматом Рабина — Скотта». — *Прим. перев.*

[2] Часто используется также термин «регулярные множества». — *Прим. перев.*

1. Пустое множество и каждое одноэлементное подмножество множества X содержатся в $\mathscr{R}$.

2. Вместе с любыми множествами U и V в $\mathscr{R}$ лежат также их объединение $U \cup V$ и их произведение $UV = \{uv \mid u \in U,\ v \in V\}$.

3. Вместе с любым множеством U в $\mathscr{R}$ содержится также порожденный множеством U в F(X) подмоноид

$$U^* = U^0 \cup U^1 \cup U^2 \cup \ldots = \{u_1 u_2 \ldots u_n \mid n \in \mathbf{N}_0,\ u_i \in U\},$$

где $U^0 = \Lambda$, $U^{i+1} = U^i U$.

Замечание. Таким образом, непустое рациональное множество может быть построено из одноэлементных множеств за конечное число операций произведения, объединения и образования подмоноида [1] — эти операции будем называть *рациональными операциями*. В результате оказывается возможным описать данное рациональное множество некоторой конечной последовательностью символов. При этом фигурные скобки в случае одноэлементных множеств опускают. Отметим, наконец, что $\varnothing^* = \Lambda$ (см. также разд. 5.7).

Пример 5.3.4. 1. Язык значений схемы программ P из примера 5.1.2 может быть представлен как рациональное множество: $WS(P) = g^* f^*$.

2. Множество U распознаваемых алгоритмов из примера 5.1.3 последовательностей знаков может быть получено как рациональное множество следующим способом.

Пусть W_i — множество всех (под)слов, распознаваемых подалгоритмом U_i (см. рис. 5.1.4). Тогда для $\{i, j, k\} = \{1, 2, 3\}$ имеем

$$W_i = \{i, k\}^* j \{i, k\}^* j \{1, 2, 3\}^* \cup \{i, j\}^* k \{i, j\}^* k \{1, 2, 3\}^* \cup$$

$$\cup (ii^* \{j, k\} \cup \{j, k\} \{j, k\}^* i) \{1, 2, 3\}^*.$$

Отсюда получаем (см. рис. 5.1.5)

$$U = \{1, 2, 3\}^* (1W_1 \cup 2W_2 \cup 3W_3).$$

3. Если металингвистические переменные в определении из примера 5.1.4 рассматривать как имена множеств и заменить «::=» на «=» и «|» на «∪», то полученные равенства будут представлять встречающиеся в них множества как рациональные. Путем последовательных замен отсюда получается представление множества допустимых заголовков процедур.

Замечание. Из пп. 1 и 2 определения 5.3.3 следует (заметим, что $\varnothing^* = \Lambda$), что Rat(X) содержит все конечные подмножества множества F(X). С учетом п.3 отсюда находим, что каждый конечно-порожденный подмоноид E^* (E—конечное множество) моноида F(X), в частности $X^* = F(X)$, содержится в Rat(X). Так как $F^+(X) = XX^*$, то $F^+(X)$ является рациональным множеством. Обычно вместо LL^* пишут L^+ для $L \subseteq F(X)$. Очевидно, что если множество L рационально, то рационально и L^+.

---

[1] Или итерации. — *Прим. перев.*

Для более глубокого понимания изложенного и в качестве дополнения читателю рекомендуется выполнить упражнения 5.4 и 5.5.

ЗАМКНУТОСТЬ ПО ОТНОШЕНИЮ К РАЦИОНАЛЬНЫМ ОПЕРАЦИЯМ

То, что некоторое множество множеств, замкнутое относительно некоторой операции, замкнуто относительно нее эффективно, означает, что существует метод (алгоритм), реализующий эту операцию (см. гл. 1).

Теорема 5.3.5 (Клини). 1. Множество $\mathrm{NAkz}(X)$ эффективно замкнуто относительно рациональных операций (объединения, произведения и образования подмоноида) и $\mathrm{Rat}(X) \subseteq \mathrm{NAkz}(X)$.

2. Множество $\mathrm{NAkz}(X)$ эффективно замкнуто относительно операции образования зеркального слова, т. е. вместе с U также и его зеркальное множество (множество $\tilde{U} = \{\tilde{u} \mid u \in U\}$) оказывается H-допустимым.

Доказательство. а) Пустое множество является допустимым HPC-автоматом $A = (Z, X, t, S, F)$ с $\tau = \varnothing$ и $S \cap F = \varnothing$. Одноэлементное множество $\{x\}$ допустимо автоматом $A = (\{z, z'\}, X, t, z, z')$ с $\tau = \{(z, x, z')\}$.

С помощью аналогичных построений можно показать, что и каждое конечное подмножество моноида $F(X)$ является допустимым соответствующим HPC-автоматом с двумя состояниями.

б) Пусть U и V — множества из $\mathrm{NAkz}(X)$, а $A_i = (Z_i, X, t_i, S_i, F_i)$, $i = 1, 2$, — HPC-автоматы такие, что $L(A_1) = U$ и $L(A_2) = V$. Будем считать, что $Z_1 \cap Z_2 = \varnothing$ (выполнение этого условия всегда может быть обеспечено переименованием состояний).

Пусть

$$A_3 = (Z_1 \cup Z_2, X, t_1 \cup t_2, S_1 \cup S_2, F_1 \cup F_2);$$

$$A_4 = (Z_1 \cup Z_2, X, t_1 \cup t_2 \cup F_1 \times \{\Lambda\} \times S_2, S_1, F_2);$$

$$A_5 = (Z_1, X, t_1 \cup F_1 \times \{\Lambda\} \times S_1, S_1, F_1);$$

$$\tilde{A}_1 = (Z_1, X, \tilde{t}_1, F_1, S_1) \quad \text{с } \tilde{\tau}_1 = \{(z', \tilde{u}, z) \mid (z, u, z') \in \tau_1\}.$$

Автомат $\tilde{A}_1$ будем называть *зеркальным* для автомата A_1.

Тогда, как нетрудно проверить, $U \cup V = L(A_3)$, $UV = L(A_4)$ и $U^+ = L(A_5)$, так что $U^* = L(A_5) \cup \Lambda$. Кроме того, $\tilde{U} = L(\tilde{A}_1)$.

Автомат A_3 — это результат параллельного соединения автоматов A_1 и A_2. Автомат A_4 — результат последовательного соединения автоматов A_1 и A_2. Автомат A_5 получается в результате соединения спонтанными переходами всех финальных состояний исходного автомата A_1 с его начальными состояниями. Граф автомата $\tilde{A}_1$ получается из графа автомата A_1 изменением направления всех ребер на противоположное и заменой слов, стоящих на ребрах, на зеркальные.

в) Построением зеркального автомата доказано утверждение 2. Поскольку из пустого множества X с помощью рациональных

операций может быть построено произвольное рациональное множество, то из пп. а) и б) вытекает, что каждое рациональное подмножество моноида F(X) является H-допустимым. Утверждение 1 доказано. ∎

Читателю рекомендуется сравнить конструкцию из данного доказательства с построением алгоритмов в примерах 5.1.3 и 5.1.4, а также выполнить упражнение 5.6.

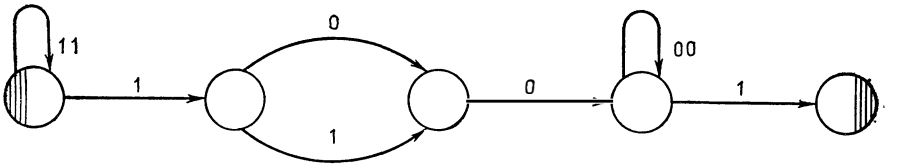


Рис. 5.3.1. HPC-автомат с реакцией L_D

Пример 5.3.6. Покажем, что множество L_D двоичных представлений чисел вида $(2^k-1)2^m+1$ при четной сумме $k+m$ и $m\geqslant 2$ (где k и m — натуральные числа) является H-допустимым. Пусть

$L_{1u}=\{1^k \mid k$ нечетное, $k\in\mathbf{N}\}$;

$L_{1g}=\{1^k \mid k$ четное, $k\in\mathbf{N}\}$;

$L_{0u}=\{0^n \mid n$ нечетное, $n\in\mathbf{N}\}$;

$L_{0g}=\{0^n \mid n$ четное, $n\in\mathbf{N}\}$.

На основании теоремы 5.3.5 заключаем, что $\bar{L}_{1g}=L_{1g}\cup\Lambda=$ $=\{(11)^i \mid i\in\mathbf{N}_0\}=\{11\}^*$ — H-допустимое множество. Из этой же теоремы далее следует, что $L_{1u}=1\bar{L}_{1g}$ и $L_{1g}=11\bar{L}_{1g}$ являются H-допустимыми. Аналогично можно показать, что H-допустимы L_{0u} и L_{0g}.

Поскольку $L_D=L_{1u}L_{0g}1\cup L_{1g}L_{0u}1$, то по теореме 5.3.5 и само множество L_D H-допустимо.

HPC-автомат с реакцией L_D задается графом, изображенным на рис. 5.3.1. (Читателю рекомендуется обдумать вопрос о том, как этот граф может быть получен из HPC-автомата с реакцией L_D, построенного с помощью конструкции, приведенной в доказательстве теоремы 5.3.5. — см. упражнения 5.4, 5.6 и гл. 6.)

РАЦИОНАЛЬНОСТЬ H-ДОПУСТИМЫХ МНОЖЕСТВ

С помощью простого (но не слишком быстрого) метода можно получить для реакции (допустимого множества) произвольного HPC-автомата представление в виде рационального множества, т. е. конечное «линейное» представление для, вообще говоря, бесконечного множества. Вместе с утверждением 1 теоремы 5.3.5 это дает (несмотря на простоту доказательств) один из важнейших результатов теории автоматов.

Иной, но родственный описываемому ниже метод приведен в упражнении 5.7.

Теорема 5.3.7 (Клини). Для каждого конечного множества X выполняется равенство $Rat(X) = NAkz(X)$.

Доказательство. На основании теоремы 5.3.5 следует только показать, что $NAkz(X) \subseteq Rat(X)$. Для этого мы используем метод, с помощью которого граф данного НРС-автомата A может быть преобразован в граф, представленный на рис. 5.3.2, так что R(A) будет рациональным множеством, равным реакции (допустимому множеству) автомата A.

Введем следующее понятие: *обобщенным графом переходов* над X называется взвешенный орграф с начальной вершиной α и конечной вершиной ω, метками на ребрах которого являются рациональные множества. Таким образом, обобщенный граф переходов является пятеркой $V = (C, X, \tau, \alpha, \omega)$, где C — конечное множество (множество вершин), $\alpha \in C$, $\omega \in C$ и τ — конечное подмножество произведения $C \times Rat(X) \times C$.

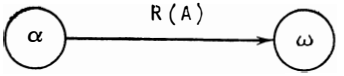


Рис. 5.3.2

Как и в случае НРС-автоматов, реакцией L(V) обобщенного графа переходов V назовем множество всех слов w, ведущих из α в ω, где высказывание «w ведет из α в ω» означает, что существуют конечная последовательность $(\alpha, R_1, c_1), (c_1, R_2, c_2), \ldots, (c_{k-1}, R_k, \omega)$ помеченных ребер графа V и разложение $w = w_1 w_2 \ldots w_k$ такие, что $w_i \in R_i$ при $i = 1, \ldots, k$.

Метод может теперь быть описан в общих чертах следующим образом.

Граф автомата A расширяется путем добавления вершин α и ω и соответствующих ребер до некоторого обобщенного графа переходов с той же реакцией, что и у A. После этого полученный обобщенный граф переходов преобразовывается путем исключения ребер и вершин до тех пор, пока он не приобретает указанный выше вид.

При исключении ребер и вершин применяются следующие три правила: K, S и E.

K (правило исключения ребер). Два ребра с одинаковым началом (скажем, c), одинаковым концом (скажем, c′) и с метками R и R′ соответственно заменяются единственным ребром (из c в c′) с меткой $R \cup R'$. При этом допускается, что $c = c'$ (т. е. что каждое из ребер является петлей) и что $c = \alpha$ или $c' = \omega$. Итак, ребра (c, R, c′) и (c, R′, c′) заменяются ребром $(c, R \cup R', c')$, как показано на рис. 5.3.3.

S (правило исключения петель). Если существует отличная от α и ω вершина (скажем, c) такая, что некоторое ребро (петля) с меткой R имеет вершину с своим началом и концом, то эта петля исключается, а метки всех исходящих из вершины с ребер умножаются слева на R^*. Если же ни одно ребро (после исключения петли) не выходит из вершины c, то вершина c исключается вместе со всеми входящими в нее ребрами. Наконец, вершина c

исключается и в том случае, если в нее не входит ни одно ребро (исключается вместе со всеми исходящими из нее ребрами).

Итак, если

$\alpha \neq c \neq \omega$, $\tau \cap \{c\} \times Rat(X) \times \{c\} = \{(c, R, c)\}$ и

$W_c = \tau \cap \{c\} \times Rat(X) \times (C - c)$,

то τ заменяется на

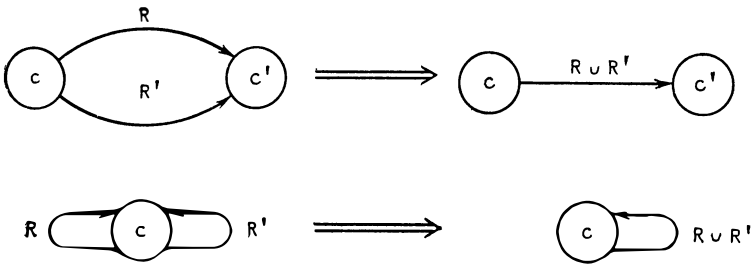


Рис 5.3.3. Правило исключения ребер K

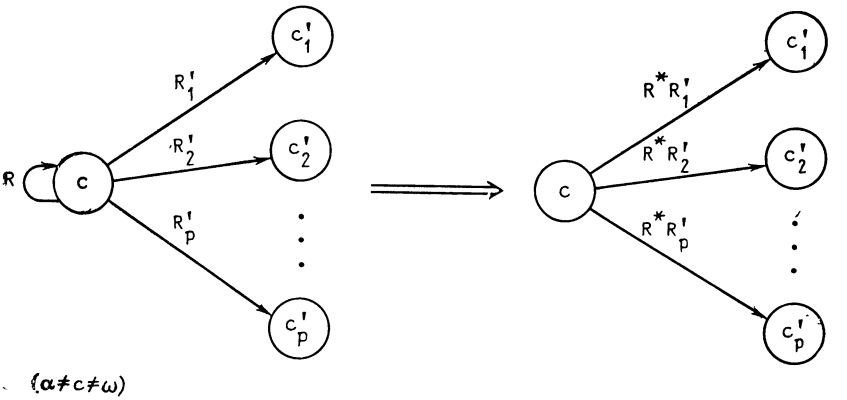


Рис. 5.3.4. Правило исключения петель S

$(\tau - (W_c \cup (c, R, c))) \cup \{(c, R^*, R', c') \mid (c, R', c') \in W_c\}$, а если W_c пусто, то, кроме того, и C заменяется на C—c (рис. 5.3.4).

E (правило исключения вершин). Произвольная отличная от α и ω вершина (скажем, c), у которой нет петли, исключается. При этом каждая пара ребер, состоящая из ребра, ведущего в c из некоторой иной вершины (скажем, из c′) и помеченного R, и ребра, ведущего из c в некоторую другую вершину (скажем, в c″) и помеченного R′, заменяется одним ребром, ведущим из c′ в c″ и помеченным RR′. При этом допускается, что c′=c″ и что уже может иметься ребро, прямо ведущее из c′ в c″. Если же в c не ведет ни одно ребро (или ни одно ребро не исходит из c), то c просто исключается вместе со всеми исходящими (входящими) ребрами.

Итак, если

$\alpha \neq c \neq \omega$, $\tau \cap \{c\} \times \mathrm{Rat}(X) \times \{c\} = \varnothing$, $H_c = \tau \cap C \times \mathrm{Rat}(X) \times \{c\}$ и $W_c = \tau \cap \{c\} \times \mathrm{Rat}(X) \times C$, то C заменяется на C—c, а τ — на

$(\tau - (H_c \cup W_c)) \cup \{(c', RR', c'') \mid (c', R, c) \in H_c, (c, R', c'') \in W_c\}$

(см. рис. 5.3.5).

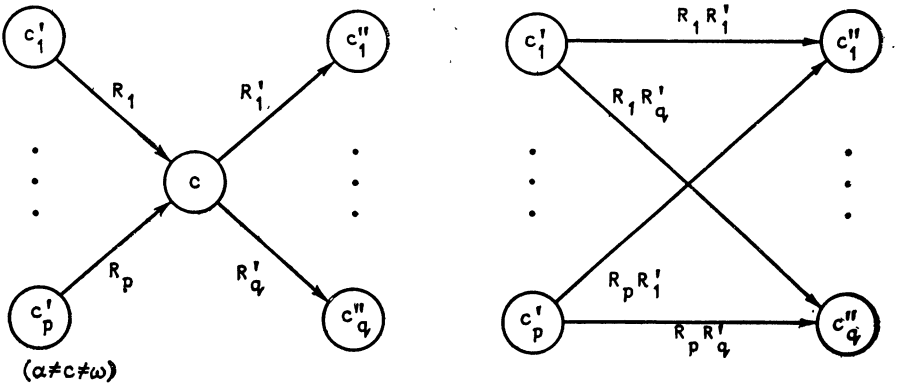


Рис. 5.3.5. Правило исключения вершин E

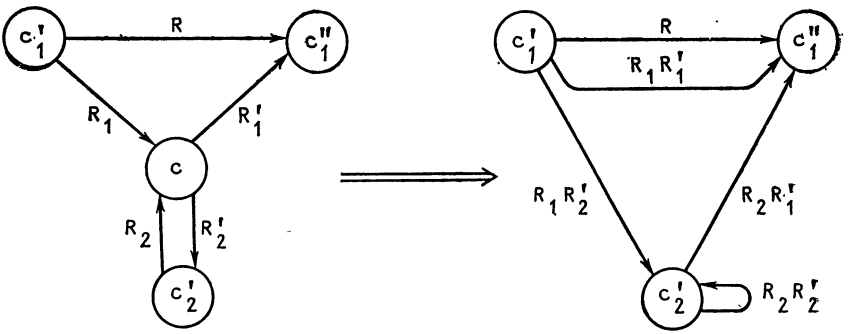


Рис. 5.3.6. Частный случай применения правила E

Утверждение. Каждая новая метка на ребрах, возникающая при применении одного из правил, снова является рациональным множеством. Возникающий при применении любого из правил граф является поэтому снова обобщенным графом переходов, имеющим ту же реакцию, что и исходный, поскольку новые метки на ребрах в точности совпадают с множествами всех слов, ведущих в старом (исходном) графе из соответствующей начальной вершины в соответствующую конечную вершину.

Отметим, что при применении правила E могут возникать кратные ребра и петли (рис. 5.3.6).

Начальный этап. Добавить к графу автомата A две новые (т. е. не содержащиеся в Z) вершины α и ω, провести ребра с меткой Λ из α во все начальные вершины исходного графа и из всех конечных вершин исходного графа в вершину ω; убрать обозначения (штриховку) старых начальных и конечных вершин.

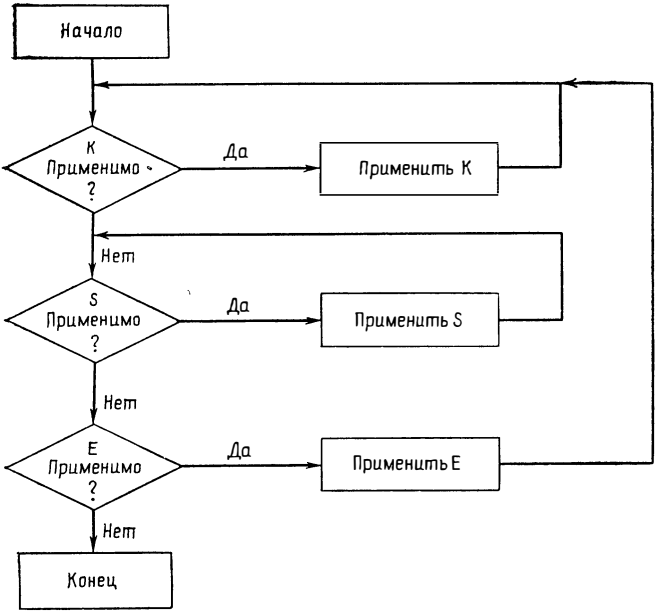


Рис. 5.3.7. Блок-схема этапа исключения

Этап исключения. Применить алгоритм, блок-схема которого приведена на рис. 5.3.7. Иначе говоря, применить сначала во всех возможных случаях правило K, исключив все кратные ребра и кратные петли; применить далее правило S ко всем вершинам, на которых «висят» петли; применить, наконец, правило E, исключив некоторую вершину, после этого перейти к началу алгоритма. Если же правило E неприменимо, то закончить работу.

Заключительный этап. Если в полученном графе не оказалось ребер, ведущих из α в ω, то ввести такое ребро, пометив его символом $\varnothing$.

Результат. После применения метода получается граф с двумя вершинами α и ω, соединенными единственным ребром, меткой на котором является рациональное множество R, т. е. ребром (α, R, ω). При этом $R=L(A)$.

ДОКАЗАТЕЛЬСТВО КОРРЕКТНОСТИ МЕТОДА

Сходимость этапа исключения. Поскольку применение правил K и S уменьшает число ребер в графе, то через конечное число шагов возникает вопрос о применимости правила E. Поскольку,

далее, применение правила E уменьшает число вершин в графе, то это правило может применяться только конечное число раз.

Правильность результата. После выполнения этапа исключения возможны два случая.

1. Остались только вершины α и ω без соединяющего их ребра. Это тот случай, когда в графе автомата A нет ни одного состояния, входящего в какой-либо путь из одной из начальных вершин в одну из конечных. Отметим при этом, что при применении правила S исключаются вершины, на которых «висят» петли, но из которых не выходят никакие иные ребра. Отметим также, что правило E применимо до тех пор, пока в графе имеется хотя бы одна вершина, отличная от α и ω, поскольку в момент постановки вопроса о применимости правила E в графе не может быть петель.

Итак, в данном случае $L(A)=\varnothing$, так что введение на заключительном этапе ребра $(\alpha, \varnothing, \omega)$ приводит к получению правильного результата.

2. Остались только вершины α и ω и соединяющее их ребро (α, R, ω). В этом случае в графе автомата A должен существовать путь из некоторого начального в некоторое финальное состояние, т. е. A должен иметь непустое допустимое множество.

Выполнение в таком случае равенства $R=L(A)$ непосредственно вытекает из приведенного выше утверждения о том, что применение всех трех правил сохраняет множество слов, ведущих в соответствующем обобщенном графе переходов из α в ω.

Ясно, что других случаев быть не может, поскольку у вершин α и ω не могут возникнуть петли, так как ни одно ребро не может вести в α и не может исходить из ω.

Оценка времени работы. Пусть автомат A имеет $(n-2)$ состояния и в графе автомата A встречается $(p-1)$ различных меток (т. е. $|pr_2(\tau)|=p-1$). Сейчас мы получим грубую верхнюю оценку для времени работы метода как функцию от n и p. При этом время работы будет оцениваться числом отдельных операций над ребрами и вершинами (удаление, введение, изменение метки).

Поскольку ориентированный граф с n вершинами может иметь не более n^2 ориентированных ребер, то граф, построенный для автомата A, может иметь не более pn^2 различных взвешенных ребер.

Перед каждой проверкой применимости правила E правило K может быть применено не более $(p-1)n^2$ раз, а правило S — не более n раз. При каждом применении правила K производятся операции над двумя объектами, а при каждом применении правила S — над не более чем n объектами. Итак, всего производится не более $(2p-1)n^2$ отдельных операций.

Каждое применение правила E требует не более n^2 отдельных операций, а всего таких применений может быть не более n.

Итак, в качестве верхней границы для числа отдельных операций получаем границу $2pn^3$. ■

Пример 5.3.8. Применяя описанный метод к НРС-автомату, граф которого приведен на рис. 5.3.1 (см. пример 5.3.6), можно

использовать правила в следующем порядке:

K, S, S, E, E, E, E, E

и получить в качестве выхода представление для L_D:

$L_D = \{11\}^*1\{0,1\}0\{00\}^*1.$

Поскольку, очевидно, $\{11\}^*1 = 1\{11\}^*$, то это представление совпадает с приведенным в примере.

Дополнительная информация о преобразованиях рациональных представлений содержится в разд. 5.6 и 5.7.

Из доказательства корректности метода вытекает следствие.

Следствие 5.3.9. Для произвольного НРС-автомата A разрешим вопрос о непустоте множества $L(A)$.

Теперь можно также увидеть, что последовательностное соответствие t^* может быть описано «конечными средствами».

Следствие 5.3.10. График последовательностного соответствия НРС-автомата может быть представлен с помощью конечного числа рациональных множеств следующим образом:

$$\tau^* = \{z_1\} \times R_1 \times \{z_1'\} \cup \{z_2\} \times R_2 \times \{z_2'\} \cup \ldots \cup \{z_k\} \times R_k \times \{z_k'\}.$$

Здесь $k = |Z|^2$ и $R_i = \{w \mid (z_i, w, z_i') \in \tau^*\}$ при $i = 1, \ldots, k$.

Доказательство. Если $A = (Z, X, t, S, F)$ — заданный НРС-автомат, то $R_i = L(A_i)$, где $A_i = (Z, X, t, z_i, z_i')$.

5.4. ДЕТЕРМИНИРОВАННЫЕ АВТОМАТЫ И РАЗЛИЧИМЫЕ МНОЖЕСТВА

Если нужно реализовать (абстрактный) автомат как последовательную программу или прибор, то для такой реализации нужен детерминированный автомат с единственным начальным состоянием, в графе которого при каждом входном слове существует не более одного пути из начального состояния в некоторое финальное состояние, определяемого этим словом. Возможность использовать несколько финальных состояний демонстрирует упражнение 5.3, п. 1.

Ниже будет дана алгебраическая характеризация множеств, допускаемых детерминированными НРС-автоматами[1], весьма отличная от представления таких множеств с помощью рациональных операций.

ОПРЕДЕЛЕНИЕ ДЕТЕРМИНИРОВАННЫХ НРС-АВТОМАТОВ

Определение 5.4.1. 1. НРС-автомат $A = (Z, X, t, S, F)$ называется *детерминированным автоматом Рабина — Скотта* (ДРС-автоматом), если он имеет только одно начальное состояние s, яв-

[1] Детерминированные НРС-автоматы — это частный случай НРС-автоматов (см. ниже), так что кажущееся на первый взгляд нелепым понятие «детерминированный недетерминированный автомат» отнюдь не бессмысленно. — *Прим. перев.*

ляется побуквенным, и если t — отображение (быть может, частичное), т. е. если $S=\{s\}$, $\tau \subseteq Z \times X \times Z$ и $|t(z, x)| \leqslant 1$ для всех (z, x) из $Z \times X$.

Автомат A называется *полностью определенным детерминированным автоматом Рабина — Скотта* (короче: автоматом Рабина — Скотта или РС-автоматом), если A детерминирован и t — всюду определенное отображение (т. е. $pr_{12}\tau = Z \times X$).

Для РС-автоматов и ДРС-автоматов вместо обозначения t часто используется обозначение f.

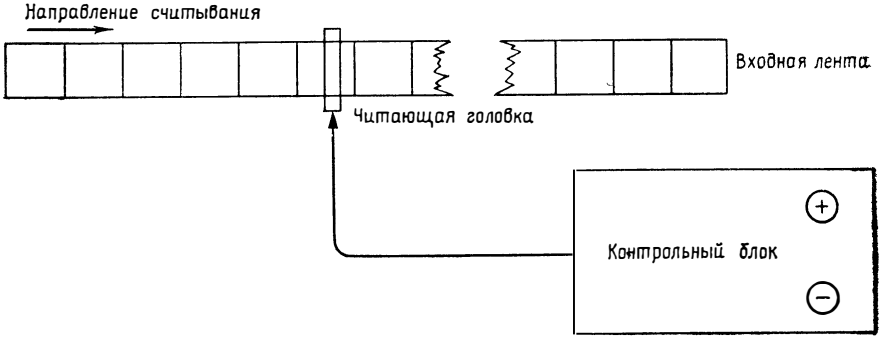


Рис. 5.4.1. **Модель РС-автомата**

2. Подмножество моноида F(X) называется Д-допустимым (допустимым), если оно является реакцией некоторого ДРС-автомата (РС-автомата).

Множество всех Д-допустимых подмножеств моноида F(X) обозначается DAkz(X), а множество всех допустимых подмножеств — Akz(X).

Замечание. Ясно, что у ДРС-автомата и последовательностное соответствие является отображением.

Если у автомата Мили или автомата Мура выделить некоторое состояние в качестве начального и определенные состояния в качестве финальных и отбросить функцию выходов, то будет получен РС-автомат. Более точно связь с автоматами Мили и Мура будет рассмотрена несколько позже.

Замечание. РС-автоматы обычно представляют себе как «читающие машины», состоящие из контрольного блока, который в зависимости от входа может принимать одно из конечного множества различных состояний, и читающей головки, которая считывает символы, записанные на разделенной на отдельные ячейки входной ленте. Читающая головка передает считанные символы контрольному блоку и может передвигаться вдоль входной ленты слева направо (после прочтения каждого символа — на одну ячейку). Когда читающая головка доходит до конца ленты, «читающая машина» останавливает ее движение и показывает (скажем, с помощью двух лампочек), находится ли контрольный блок в этот момент в финальном состоянии (зажигается лампочка,

помеченная символом +) или нет (зажигается лампочка, помеченная символом —) (рис. 5.4.1).

Аналогично можно и НРС-автоматы рассматривать как «читающие машины». Такие машины работают недетерминированным образом и их читающая головка может — в случае неалфавитного НРС-автомата — за один такт прочитать несколько символов.

Очевидно, что «читающая машина», изображенная на рис. 5.4.1, может быть обращена в «пишущую машину», если заменить читающую головку пишущей и контрольный блок управляющим блоком, который не обрабатывает входы, а порождает выходы. Поэтому РС-автомат (и, равным образом, НРС-автомат) может рассматриваться и как машина, порождающая последовательности символов.

РАЗЛИЧИМЫЕ МНОЖЕСТВА

Идеи, аналогичные лежащим в основе теоремы 5.2.3, оправдывают определение еще одного класса множеств, для которого вскоре будет показано, что он совпадает с классом допустимых множеств.

Определение 5.4.2. Подмножество E моноида $F(X)$ называется *различимым*, если существуют конечный моноид M и гомоморфизм h из $F(X)$ на M такие, что $E=h^{-1}(h(E))$.

Множество всех различимых подмножеств моноида $F(X)$ будем обозначать $Erk(X)$.

Примеры различимых множеств даны в упражнениях 5.8 и 5.9.

Лемма 5.4.3. Следующие высказывания эквивалентны.

1. $E\in Erk(X)$.

2. Существуют конечный моноид M, подмножество M' этого моноида и гомоморфизм h из $F(X)$ на M такие, что $E=h^{-1}(M')$.

3. Существует конгруэнция R конечного индекса на $F(X)$ такая, что E стабильно относительно R, т. е. E является объединением некоторых классов эквивалентности относительно R (т. е. R — отношение эквивалентности с конечным числом классов эквивалентности такое, что при произвольных эквивалентных относительно R u и v из $F(X)$ слова wuw' и wvw' при всех w и w' из $F(X)$ также эквивалентны относительно R).

4. Определяемое ниже отношение R_E на $F(X)$, так называемая *синтаксическая конгруэнция* по E, является конгруэнцией конечного индекса:

при произвольных u и v из $F(X)$ соотношение uR_Ev выполняется тогда и только тогда, когда при любых w и w' из $F(X)$ утверждения $wuw'\in E$ и $wvw'\in E$ эквивалентны.

Доказательство. Из п.1 вытекает п.2, если положить (в обозначениях определения 5.4.2) $M'=h(E)$.

Из п.2 следует п.3, так как h индуцирует на $F_1(X)$ конгруэнцию R_h, классами которой являются множества $h^{-1}(m)$ при $m\in M$.

Покажем теперь, что из п.3 вытекает п.4. Пусть E и R удовлетворяют условию 3. То, что отношение R_E является конгруэнцией на $F(X)$, проверяется непосредственно. Если uRv, то wuw' принадлежит E в том и только в том случае, когда wvw' тоже

принадлежит E, так как на основании п.3 вместе с каждым словом содержит все эквивалентные ему относительно R слова.

Таким образом, каждый класс эквивалентности по R содержится целиком в некотором классе эквивалентности по R_E, и потому вместе с R отношение R_E также оказывается конгруэнцией конечного индекса.

Из п.4 вытекает п.1, если выбрать в качестве h определенный конгруэнцией R_E гомоморфизм, а в качестве M — моноид классов конгруэнтности относительно R_E с умножением подмножеств F(X) в качестве моноидного умножения. Поскольку для каждого u из E в этом случае множество $h^{-1}(h(u))$ оказывается содержащим u классом конгруэнтности относительно R_E, он, очевидно, должен целиком лежать в E (положить $w=w'=\Lambda$ в определении R_E). $M_E=M$ будем называть *синтаксическим моноидом* по E.

Интересный пример конгруэнции на F(X) бесконечного индекса дает упражнение 5.10.

Теорема 5.4.4. (Майхилл). Akz(X) = Erk(X).

Доказательство. 1. Пусть L — множество из Akz(X) и A—PC-автомат с $L(A)=\tilde{L}$, где $\tilde{L}$ — множество, зеркальное для L, т. е. множество всех слов $\tilde{w}$, зеркальных для слов w из L (см. теоремы 5.3.5 и 5.2.3). Пусть также M=T(A) — моноид переходов автомата A, h — определенный в теореме 5.2.3 гомоморфизм из F(X) на T(A) и $M'=\{g\in T(A) \mid g(s)\cap F\neq\varnothing\}$.

Тогда, очевидно, $\tilde{w}\in L$ [т. е. $w\in L(A)$] в том и только в том случае, когда $h(\tilde{w})\in M'$. Из п.2 леммы 5.4.3 следует, что в этом случае $L\in Erk(X)$.

2. Пусть $L\in Erk(X)$. На основании п.2 леммы 5.4.3 в этом случае существуют M, M′ и h такие, что $L=h^{-1}(M')$. Построим на этой базе PC-автомат A: A=(M, X, f, e, M′), где e — единичный элемент M, f (m, x) = mh (x), — при всех m из M и всех x из X.

Поскольку h — гомоморфизм, то для любого слова w из F(X) выполнено равенство $f^*(e, w)=h(w)$, т. е. w принадлежит L(A) тогда и только тогда, когда h(w) принадлежит M′. Итак, $L(A)=h^{-1}(M')=L$. ■

Замечание. В первой части доказательства использовалось только то, что автомат A — алфавитный, так что множество Erk(X), а потому и множество Akz(X) равны множеству всех допустимых для алфавитных HPC-автоматов множеств.

Для каждого конечного моноида M существует PC-автомат, имеющий M своим моноидом переходов (см. упражнение 5.11), однако не каждый конечный моноид является синтаксическим моноидом некоторого различимого множества (см. упражнение 5.12). По поводу дальнейших свойств синтаксических моноидов см. упражнение 5.13 и 6.7.

СООТНОШЕНИЯ РЕАКЦИЙ PC-АВТОМАТОВ, АВТОМАТОВ МИЛИ И МУРА

По PC-автомату можно построить автомат Мура, который вычисляет характеристическую функцию допустимого множества

слов данного РС-автомата. В то же время для данного автомата Мура или автомата Мили A можно построить РС-автомат A′ такой, что $L(A')$ будет множеством всех входных слов, при которых A, начиная работу в некотором фиксированном состоянии, порождает выходную последовательность, заканчивающуюся некоторым определенным символом. Далее, для данного частичного автомата Мили множество входных последовательностей, которые переводят автомат, находящийся в некотором определенном состоянии, в заданное последующее состояние, можно рассматривать как H-допустимое множество (равно как и множество входных слов, которым отвечают полностью определенные выходные слова, а также и множество выходных слов, которые можно получить с помощью частичного автомата Мили, находящегося в начале работы всегда в некотором определенном состоянии).

Теорема 5.4.5. 1. Пусть $A=(Z, X, f, s, F)$ — РС-автомат. Тогда $A'=(Z, X, \{0, 1\}, f, h)$, где $h(z)=1$ тогда и только тогда, когда $z\in F$, — автомат Мура такой, что

$$L(A)=\{w\in F(X) \mid h(f^*(s, w))=1\}.$$

2. Пусть $A=(Z, X, Y, f, g)$ — частичный автомат Мили. Тогда:

1) при каждом z из Z и каждом y из Y множество $W(A, z, y)=\{w\in F(X) \mid \widehat{g}_z(w)=y\}\cup\Lambda$ является H-допустимым;

2) при каждом z из Z H-допустимы множества $pr_2(gr\, f^*\cap\{z\}\times F(X)\times Z)=\{w\in F(X) \mid$ определено состояние $f^*(z, w)\}$, $pr_i(gr\, g_z)$, $i=1, 2$.

Доказательство. 1. Из определения автомата A′ непосредственно вытекает, что $h(f^*(s, w))=1$ тогда и только тогда, когда состояние $f^*(s, w)$ принадлежит множеству F; заметим, что РС-автомат полностью определен и детерминирован.

2. 1) Пусть зафиксированы z и y, причем z — релевантное состояние (см. определение 4.3.1) автомата A. Обозначим символом A^0 автомат, являющийся $\overline{0}$-доопределением автомата A (см. лемму 4.3.5). Пусть $A'=(Z', X, Y', f', h)$ — построенный методом из доказательства теоремы 3.4.4 равносильный автомату A^0 автомат Мура, причем будем считать, что используемый в таком построении выход y_0 отличен от y.

Пусть, далее, s — некоторое полученное из z состояние автомата A′ (см. конструкцию из доказательства теоремы 3.4.4) и F — множество всех z′ из Z′ таких, что $h(z')=y$.

Тогда $A''=(Z', X, f', s, F)$ — РС-автомат такой, что $L(A'')\cup\{\Lambda\}=W(A, z, y)$, поскольку по построению при всех w из $F^+(X)$ состояние $f'^*(s, w)$ принадлежит F в том и только в том случае, когда $h(f'^*(s, w))=y$, т. е. $\widehat{g}_z(w)=y$.

По теореме 5.3.5 вместе с множеством $L(A'')$ и множество $L(A'')\cup\{\Lambda\}$ оказывается H-допустимым.

Если z — не релевантное состояние автомата A, то $W(A, z, y)=\{\Lambda\}$, а это множество по теореме 5.3.5 H-допустимо.

2) Пусть $A'=(Z, X, f, z, Z)$. Тогда A' — ДРС-автомат с реакцией

$$L(A')=\{w\in F(X) \mid \text{определено состояние } f^*(z, w)\}.$$

При $i=1, 2$ пусть $A_i=(Z, X_i, f_i, z, Z)$, где $X_1=X$ и $X_2=Y$,

$$\operatorname{gr} f_1=\operatorname{gr} f\cap(\operatorname{pr}_{12}(\operatorname{gr} g)\times Z),$$

$$\operatorname{gr} f_2=\{(z, y, z') \mid \text{существует } x\in F(X) \text{ с } f(z, x)=z' \text{ и } g(z, x)=y\}.$$

Тогда A_i — НРС-автоматы с $L(A_i)=\operatorname{pr}_i(\operatorname{gr} g_z)$ при $i=1, 2$.

Конструкция автоматов A_i становится ясна при рассмотрении графа автомата A. В графе автомата A прежде всего убираются все метки вида x/— или —/y (при x из X и y из Y). После этого исключаются все непомеченные ребра. Пусть в результате получен граф G. Граф автомата A_1 (A_2) получается из графа G исключением из всех меток выходов (соответственно входов) и косых черт. ■

Следствие 5.4.6. Подмножество L моноида F(X) допустимо тогда и только тогда, когда существует автомат Мура $A=\{Z, X, \{0, 1\}, f, h\}$, вычисляющий характеристическую функцию множества L, т. е. автомат, для которого выполнено условие: в Z существует состояние z такое, что

$$L=\{w\in F(X) \mid h(f^*(z, w))=1\}.$$

Доказательство. На основании п.1 теоремы 5.4.5 следует только показать, что при заданном автомате Мура A множество L является допустимым для некоторого РС-автомата. Но это следует из доказательства п.1) утверждения 2 теоремы 5.4.5, если там вместо частичного автомата Мили выбрать автомат Мура. ■

Другие определяемые частичными автоматами Мили допустимые множества рассматриваются в упражнении 5.14.

Из сказанного следует, что множество Akz(X) может рассматриваться как множество всех подмножеств моноида F(X), характеристические функции которых вычислимы некоторым автоматом Мура. Поэтому результаты, полученные для автоматов Мура (и автоматов Мили), могут быть перенесены на Akz(X). В частности, следствия 3.7.3 и 3.7.5 превращаются в утверждения о существовании не допустимых множеств.

Следствие 5.4.7. Следующие множества *не допустимы*:

1) $DYCK_1'=\{w\in F(\{a, b\}) \mid$ в каждом начальном отрезке слова w символов a встречается не меньше, чем символов b; во всем слове w символов a и b поровну$\}$;

2) $\{a^{2^{2^k}} \mid k\in \mathbf{N}_0\}$;

3) $COPY(X)=\{vv \mid v\in F(X)\}$ при $|X|\geqslant 2$.

Замечание. $DYCK_1'$ — это так называемый скобочный язык Дика над одной парой скобок. Действительно, если рассматривать a как открывающую ([ ), а b — как закрывающую ( ]) скобку, то $DYCK_1'$ оказывается в точности множеством правиль-

ных скобочных выражений (см. следствие 3.7.3) над одной парой скобок. Множества $DYCK_1'$ и COPY(X) играют важную роль в теории формальных языков.

КРИТЕРИЙ ДОПУСТИМОСТИ

Утверждение, аналогичное теореме о периодичности для автоматов Мили, определяет важное свойство допустимых множеств, с его помощью часто удается легко показать, что некоторое множество не является допустимым.

Теорема 5.4.8 (теорема об итеративном подслове). Для каждого допустимого множества L существует натуральное число n(L) такое, что для всех слов w из L длины, большей или равной n(L), выполнено следующее условие.

Если выбрать $m \geqslant n(L)$ индексов $i_1 < i_2 < \ldots < i_m$ из множества $\{1, 2, \ldots, |w|\}$, то в F(X) найдутся слова u, v и u′ с $w = uvu'$ (если $w = x_1 x_2 \ldots x_t$, то $u = x_1 x_2 \ldots x_r$ и $v = x_{r+1} \ldots x_s$) такие, что при некоторых $p < q \leqslant L(n)$ выполняются равенства $r = i_p$ и $s = i_q$, и такие, что при всех неотрицательных целых k выполняется включение $uv^k u' \in L$.

Слово v называется *итеративным подсловом* слова w.

Доказательство. Пусть $A = (Z, X, f, s, F)$ — PC-автомат, для которого L является допустимым множеством. Положим $n(L) = |Z|$. Пусть, далее, зафиксированы слово $w = x_1 x_2 \ldots x_t$ и индексы $i_1, i_2, \ldots, i_m$ (см. формулировку теоремы).

В этом случае не все состояния $f^*(s, x_1 \ldots x_{i_j})$ при $j = 0, 1, \ldots, m$[1]) могут быть, очевидно, попарно различны, поскольку их больше чем $|Z|$. Пусть p — наименьшее целое число такое, что существует $j \neq p$ со свойством $f^*(s, x_1 \ldots x_{i_p}) = f^*(s, x_1 \ldots x_{i_j})$. Ясно, что $p < n(L)$.

Пусть, далее, q — наименьшее отличное от p натуральное число, для которого

$$f^*(s, x_1 \ldots x_{i_p}) = f^*(s, x_1 \ldots x_{i_q}).$$

Тогда $q > p$ и $q \leqslant n(L)$.

Пусть $u = x_1 \ldots x_{i_p}$, $v = x_{i_p+1} \ldots x_{i_q}$ и $u' = x_{i_q+1} \ldots x_t$.

Тогда $uvu' = w$ и $f^*(s, u) = f^*(s, uv^k)$ при любом $k \in \mathbf{N}_0$, так что и $f^*(s, uu') = f^*(s, uvu') = f^*(s, uv^k u')$. Остальное очевидно. ■

Замечание. Если допустимое множество задано посредством описания допускающего его PC-автомата, то рассматриваемая в теореме величина n(L) может быть определена эффективным образом.

Чтобы показать, как теорема 5.4.8 применяется для доказательства того, что некоторое множество не является допустимым, рассмотрим широко используемое в теории формальных языков

---

[1] Здесь, очевидно, по определению считается, что $x_1 \ldots x_{i_0} = \Lambda$, так что $f^*(s, x_{i_0} \ldots x_{i_0}) = s$. — *Прим. перев.*

множество PAL так называемых палиндромов (перевертеней), т. е. слов, совпадающих со своими зеркальными (примеры: OTTO, РАДАР, РОТАТОР). Аналогичным способом (без использования результатов, полученных для автоматов Мура) можно передоказать следствие 5.4.7 (см. упражнение 5.15, в котором можно познакомиться и с иными примерами не допустимых множеств).

Следствие 5.4.9. Пусть $|X| \geqslant 2$. Тогда множество $PAL(X) = \{w \in F(X) \mid w = \tilde{w}\}$ не является допустимым подмножеством моноида $F(X)$.

Доказательство. Мы можем предположить, что в X содержатся два различных символа a и b. Предположим также, что множество PAL(X) допустимо. Тогда к нему применима теорема 5.4.8. Пусть $n = n(L)$ — имеющаяся по этой теореме нижняя граница существования итеративного подслова.

Рассмотрим слово $a^n b a^n$ из PAL(X) и выберем индексы $i_j = j$ при $j = 1, \ldots, n$. Из теоремы вытекает, что слово $a^n b a^n$ имеет разложение $a^n b a^n = uvu'$, где $v \neq \Lambda$ и $|uv| \leqslant n$, такое, что слово uu' принадлежит PAL(X). Так как $|uv| \leqslant n$, слово uv должно быть начальным отрезком слова a^n, а слово ba^n — конечным отрезком слова u', т. е. должны существовать числа p, q и r такие, что $q \neq 0$, $u = a^p$, $v = a^q$ и $uva^r = a^n$. Тогда $uu' = a^p a^r b a^n$, где $p + r \neq n$, что противоречит принадлежности слова uu' множеству PAL(X). Итак, предположение ложно. ■

В только что проведенном доказательстве использовался упрощенный вариант теоремы об итеративном подслове. Поскольку этот вариант часто оказывается достаточным, сформулируем его в виде отдельного утверждения.

Следствие 5.4.10 (uvw-теорема). Для каждого допустимого множества L существует натуральное число n(L) такое, что для всех слов w_0 из L длины, большей или равной n(L), существует разложение $w_0 = uvw$ с $v \neq \Lambda$ и $|uv| \leqslant n$ такое, что при всех $k \in \mathbf{N}_0$ слово $uv^k w$ принадлежит L. Если L — допустимое множество для некоторого РС-автомата с n состояниями, то в качестве n(L) можно выбрать n.

Доказательство. Как и в доказательстве следствия 5.4.9, выберем в слове w_0 первые n(L) позиций (т. е. выберем соответствующие индексы). Теперь нужное утверждение непосредственно вытекает из теоремы 5.4.8. ■

ДРУГИЕ ПРИМЕРЫ НЕ ДОПУСТИМЫХ МНОЖЕСТВ

Из доказательства следствия 5.4.9 вытекает, что и множества $\{a^m b a^m \mid m \in \mathbf{N}\}$ и $\{a^m b^m \mid m \in \mathbf{N}\}$ при $a \neq b$ не являются допустимыми. Это доказывает утверждение, высказанное в конце примера 5.1.2.

Чтобы иметь возможность аналогичным образом показывать недопустимость некоторых подобных множеств, нам понадобится следующая лемма.

Лемма 5.4.11. Пусть u и v — слова из F(X).

1. Равенство $uv=vu$ выполняется тогда и только тогда, когда u и v являются «степенями» одного и того же слова, т. е. когда существует слово w в $F(X)$ такое, что $u=w^i$ и $v=w^j$ при некоторых i и j из $\mathbf{N}_0$.

2. Если $uv\neq vu$, то при всех i и j из $\mathbf{N}_0$ выполнено $u^i\neq v^j$.

3. Если $uv\neq vu$, то равенство $u^mv^n=u^kv^k$ при k, m и n из $\mathbf{N}_0$ выполняется тогда и только тогда, когда $k=m=n$.

Доказательство. 1. Достаточно доказать следующее высказывание: из $uv=vu$ вытекает существование w, i и j таких, что $u=w^i$ и $v=w^j$. Обращение этого высказывания тривиально.

Проведем доказательство полной индукцией по $m(u, v)=\max(|u|, |v|)$.

При $m(u, v)=0$ имеем $u=v=\Lambda$. Тогда утверждение выполнено при $w=\Lambda$ и произвольных i и j.

Пусть заданы слова u и v с $m(u, v)=k>0$.

Предположим, что высказывание верно для всех u' и v' с $m(u', v')<k$. Будем считать также, что $|k|=|u|\geqslant|v|$.

При $v=\Lambda$ имеем $w=u$, $i=1$, $j=0$.

Из $|v|=|u|$ и $uv=vu$ следует, что $u=v$, так что в этом случае $w=u$ и $i=j=1$.

Остается случай $|u|>|v|>0$. Из равенства $uv=vu$ вытекает существование в этой ситуации слова u' такого, что $u=u'v$ и $|u'|<|u|$. Тогда $m(u', v)<k$ и $vu'v=vu=uv=u'vv$, так что $vu'=u'v$. По предположению индукции в этом случае существуют w, i и j такие, что $u'=w'$ и $v=w^j$. Но тогда $u=w^{i+j}$ и $v=w^j$, что и требовалось доказать.

2. Предположение: существуют i и j в $\mathbf{N}$ такие, что $u^i=v^j$. Из условия леммы немедленно вытекает, что $i\neq1$ и $j\neq1$. Далее достаточно рассмотреть случай $|u|\leqslant|v|$.

При $|u|=|v|$ из предположения следует $u=v$, что противоречит условию леммы. Поэтому можно считать, что $|u|<|v|$. Тогда из предположения вытекают равенства $u^kv^j=u^ku^i=u^iu^k=v^ju^k=vv^{j-1}u^k$ при всех k из $\mathbf{N}$, так что существуют m и v' такие, что $0<|v'|<|u|$, $0<m<i$ и $v=u^mv'$.

Используя последнее равенство вместе с предположением, получаем $u^{i+1}=uv^j=uv^{j-1}u^mv'$, т. е. имеем для u разложение $u=u_1v'$.

Поэтому $u^{i-1}u_1v'=u^i=v^j=v^{j-1}u^mv'$, так что $u^{i-1}u_1=v^{j-1}u^{m-1}u$.

Отсюда получается разложение $u=u_2u_1$ с $|u_2|=|v'|$ и $u^{i-2}u=v^{j-1}u^{m-1}u_2$, так что $u=u_3u_2$.

Поскольку $|u_3|=|u_1|$, то на основании $u_3u_2=u=u_1v'$ имеем $u_3=u_1$ и $u_2=v'$. Отсюда получаем $u_1v'=u=u_2u_1=v'u_1$.

Используя теперь утверждение 1 леммы, находим, что в данном случае должны существовать w, p и q такие, что $u_1=w^p$ и $v'=w^q$.

Из сказанного следует, что $u=w^{p+q}$ и $v=w^{(p+q)m+q}$, а это в силу утверждения 1 леммы противоречит предположению о том, что слова uv и vu различны.

3. Пусть $u^mv^n=u^kv^k$, где $m\leqslant n$ (случай $n\leqslant m$ рассматривается

аналогично). Если $k \leqslant m$ ($k \geqslant n$), то $u^{m-k}v^{n-k} = \Lambda$ ($u^{k-m}v^{k-n} = \Lambda$), так что $k = m = n$. Если $m \leqslant k \leqslant n$, то $v^{n-k} = u^{k-m}$, что по утверждению 2 леммы возможно только при $n-k = k-m = 0$, т. е. при $k = m = n$. ■

Теорема 5.4.12. При произвольных u и v из F(X) таких, что $uv \neq vu$, множество $L(u, v) = \{u^m v^m \mid m \in \mathbf{N}\}$ *не допустимо.*

Доказательство. Предположение: $L = L(u, v) \in Akz(X)$.

Пусть $n = n(L)$ — число из теоремы об итеративном подслове и $w = u^n v^n$ — слово из L(u, v).

Выберем, чтобы применить теорему 5.4.8, индексы $i_j = j \cdot |u|$ при $j = 1, \ldots, n$. Тогда должно существовать разложение $u^n v^n = u_1 v_1 u_1'$ такое, что $u_1 = u^p$, $v_1 = u^q$ (где $q \neq 0$ и $p + q \leqslant n$) и $u_1 u_1'$ — слово из L(u, v).

В то же время, поскольку $u_1 u_1' = u^{n-q} v^n$ и $n - q \neq n$, слово $u_1 u_1'$ не может иметь вида $u^m v^m$ на основании п.3 леммы 5.4.11, т. е. не может принадлежать L(u, v). Итак, предположение ложно. ■

5.5. ЭКВИВАЛЕНТНОСТЬ РАЗЛИЧНЫХ ПОНЯТИЙ

Хотя различные введенные в данной главе понятия, используемые для описания классов множеств, кажутся весьма далекими друг от друга, мы установим, что на самом деле они эквивалентны. Это обеспечивается, с одной стороны, особенностью структуры свободно порожденного конечным множеством моноида F(X) и, с другой стороны, конечностью множеств состояний автоматов различных типов.

РАВЕНСТВО МНОЖЕСТВ NAkz(X) и Akz(X)

Как уже говорилось во вводных примерах, важно знать, можно ли по данному НРС-автомату построить РС-автомат, реагирующий (на входные последовательности) точно таким же образом. В таком случае соответствующий РС-автомат может иметь, вообще говоря, существенно больше состояний, чем «эквивалентный» НРС-автомат (см. также гл. 6). Эквивалентность НРС-автоматов будет, как и в случае автоматов Мили или Мура, определяться с помощью понятия реакции.

Определение 5.5.1. Два НРС-автомата называются *эквивалентными*, если их реакции равны.

Следствие 5.5.2. Пусть A_i при $i = 1, 2$ — РС-автоматы с начальными состояниями s_i и пусть A_i' — сопоставленные им в п.1 теоремы 5.4.5 автоматы Мура. Тогда автоматы A_1 и A_2 эквивалентны в том и только в том случае, когда s_1 и s_2 как состояния автоматов A_1' и A_2' соответственно имеют одинаковые реакции.

Доказательство. Равенство $L(A_1) = L(A_2)$ по теореме 5.4.5. п.1 эквивалентно выполнению равенства $h_1(f_1^*(s_1, w)) = h_2(f_2^*(s_2, w))$ при всех w из F(X).

Это возможно тогда и только тогда, когда при любой последовательности $x_1, \ldots, x_n$ входов из X выполнено равенство

$$h_1(s_1)h_1(f_1(s_1, x_1))h_1(f_1^*(s_1, x_1x_2)) \ldots h_1(f_1^*(s_1, x_1 \ldots x_n)) =$$
$$= h_2(s_2)h_2(f_2(s_2, x_1))h_2(f_2^*(s_2, x_1x_2)) \ldots h_2(f_2^*(s_2, x_1 \ldots x_n)),$$

которое эквивалентно, очевидно, равенству $1s_1 = h_{2s_2}$ (см. также доказательство теоремы 4.2.9). ■

Замечание. Итак, вопрос об эквивалентности РС-автоматов разрешим, поскольку он разрешим для автоматов Мура. Прямой метод исследования проблемы эквивалентности будет приведен в гл. 6.

Часть метода построения РС-автомата, эквивалентного данному НРС-автомату, содержится уже в теореме Майхилла (см. замечание после доказательства теоремы 5.4.4). Остальное вытекает из теоремы 5.3.7. Другое доказательство (и даже более «обычное») будет дано в гл. 6, где будет также показано, на сколько больше состояний может иметь РС-автомат, чем эквивалентный НРС-автомат.

Теорема 5.5.3 (Рабин, Скотт). Для каждого НРС-автомата может быть эффективно построен эквивалентный РС-автомат.

Доказательство. Для каждого НРС-автомата методом из доказательства теоремы 5.3.7 можно построить рациональное представление его реакции. По этому представлению можно методом из доказательства п.1 теоремы 5.3.5 построить НРС-автомат, причем алфавитный, поскольку рациональное множество всегда может быть построено на базе одноэлементных множеств. Для этого алфавитного НРС-автомата методом из доказательства теоремы 5.4.4 может быть построено представление его допустимого множества (реакции) как различимого множества и по нему (методом из доказательства той же теоремы) — РС-автомат с той же самой реакцией. Все построения могут быть выполнены эффективным образом (см. также замечание к теореме 5.2.3). В гл. 6 будет изучен прямой метод, при котором используются только преобразования автоматов. ■

Из теорем Майхилла, Рабина и Скотта, а также Клини немедленно вытекает центральная теорема теории автоматов Рабина—Скотта.

Следствие 5.5.4 (теорема Клини, Майхилла). $\mathrm{Erk}(X) = \mathrm{Akz}(X) = \mathrm{DAkz}(X) = \mathrm{NAkz}(X) = \mathrm{Rat}(X)$.

Замечание. Поскольку допустимые множества, таким образом, имеют регулярное с различных точек зрения строение (см. также следующий подраздел), они также часто называются *регулярными множествами.*

ЗАМКНУТОСТЬ ОТНОСИТЕЛЬНО ОПЕРАЦИЙ ПЕРЕСЕЧЕНИЯ, ДОПОЛНЕНИЯ И ОБРАЗОВАНИЯ ЧАСТНЫХ

Из следствия 5.5.4 сразу получаем дальнейшие важные высказывания о множестве $\mathrm{Akz}(X)$, позволяющие строить допустимые множества без помощи автоматов или доказывать, что некоторые определенные множества не являются допустимыми.

Теорема 5.5.5. Множество $\mathrm{Akz}(X)$ с теоретико-множественными операциями объединения, пересечения и дополнения образует булеву алгебру. Более того, множество $\mathrm{Akz}(X)$ эффективно замк-

нуто относительно образования конечных объединений, пересечений и операции дополнения в моноиде $F(X)$.

Доказательство. Из первой теоремы Клини (теорема 5.3.5) и того факта, что дополнение пересечения двух множеств равно объединению их дополнений (закон Моргана), вытекает, что нужно доказать только замкнутость множества $Akz(X)$ относительно операции дополнения.

Итак, пусть L — множество из $Akz(X)$, т. е. существует РС-автомат $A=(Z, X, f, s, F)$ с $L=L(A)$. Поскольку f, а потому и f^* — всюду определенные отображения, то $A'=(Z, X, f, s, Z-F)$ есть РС-автомат с $L(A')=F(X)-L(A)=F(X)-L$. ■

Иное доказательство того, что $Akz(X)$ является булевой алгеброй, требуется построить в упражнении 5.16.

Замечание. Множество $Akz(X)$ замкнуто и относительно операции вычитания множеств, так как для произвольных подмножеств U и V моноида $F(X)$ выполнено $U-V=F(X)-(V\cup(F(X)-U))$.

Определение 5.5.6. Пусть U и V — подмножества моноида $F(X)$.

Правым частным U по V назовем множество $U/V=\{w\in F(X) \mid$ существует слово $v\in V$ такое, что $wv\in U\}=\{w\in F(X) \mid wV\cap U\neq\varnothing\}$.

Левым частным U по V назовем множество $V\setminus U=\{w\in F(X) \mid$ существует слово $v\in V$ такое, что $vw\in U\}=\{w\in F(X) \mid Vw\cap U\neq\varnothing\}$.

Правое (левое) частное U по V получается, таким образом, путем «отрезания» от слов из U конечных (начальных) отрезков, являющихся словами из V.

Замечание. Следует иметь в виду, что образование частных не является обратной операцией для умножения. Например, для $U=\{aba\}$ и $V=\{ab, ba\}$ имеем:

$$U/V=V\setminus U=\{a\}, \quad \text{но} \quad (U/V)\cdot V=(V\setminus U)\cdot V=\{aab, aba\}\neq U$$

и $V\cdot(U/V)=V\cdot(V\setminus U)=\{aba, baa\}\neq U$.

Другие свойства операции образования частных рассматриваются в упражнении 5.17.

Теперь мы получим один чрезвычайно общий результат о замыканиях.

Теорема 5.5.7. Пусть U — допустимое, V — произвольное подмножество моноида $F(X)$. Тогда множества U/V и $V\setminus U$ оба допустимы, однако допускающие их автоматы не всегда могут быть построены эффективным образом. Если же и множество V допустимо, то по заданным автоматам, допускающим U и V, может быть эффективно построен РС-автомат, имеющий реакцию U/V (или $V\setminus U$).

Доказательство. 1. Покажем сначала, что множество U/V допустимо. Пусть A — РС-автомат с реакцией U. Тогда РС-автоматом с реакцией U/V является автомат $A'=(Z, X, f, s, F')$ с множеством финальных состояний

$F' = \{z \in Z |$ существует слово $v \in V$ такое, что $f^*(z, v) \in F\}$. Действительно, для $w \in L(A')$ выполнено условие: существует v в V такое, что $wv \in U$. В то же время, поскольку для w из U/V существует v в V такое, что $wv \in L(A)$, то $f^*(f^*(s, w), v) \in F$, так что $w \in L(A')$.

Ясно, что автомат A′ определен неэффективно, если множество V не задано эффективным образом. Поскольку множество всех подмножеств множества F(X) несчетно, а множество всех эффективно (т. е. с помощью «конечных средств») задаваемых подмножеств этого множества может быть всего лишь счетным, то такие не определимые эффективно множества существуют.

Предположим, теперь, что множество V допустимо. Поскольку при каждом z из Z множество $\{w \in F(X) | f^*(z, w) \in F\}$ является реакцией автомата $A_z'' = (Z, X, f, z, F)$, то по теореме 5.5.5 допустимо и множество $\{v \in V | f^*(z, v) \in F\} = V \cap L(A_z'')$ и на основании следствия 5.3.9 разрешим вопрос, является ли это множество пустым, а $z \in F'$ тогда и только тогда, когда $V \cap L(A_z'') \neq \varnothing$. Итак, в данном случае A′ может быть задан эффективно.

2. Поскольку $vw \in U$ тогда и только тогда, когда $\tilde{w}\tilde{v} \in \tilde{U}$, то при $Q = V \setminus U$, очевидно, $\tilde{Q} = \tilde{U} \setminus \tilde{V}$. Поскольку по теореме 5.3.5 множество Akz(X) эффективно замкнуто относительно перехода к зеркальным словам, из п.1 данного доказательства вытекает, что вместе с U также $\tilde{Q} = \tilde{U} \setminus \tilde{V}$ и $Q = \tilde{\tilde{Q}}$ являются допустимыми и что допускающий Q PC-автомат может быть построен эффективным образом, если множество V допустимо. ■

НЕДОПУСТИМОСТЬ МНОЖЕСТВА КВАДРАТОВ ЦЕЛЫХ ЧИСЕЛ

Теперь нетрудно привести хороший пример доказательства того, что данное множество не является допустимым. При этом будет показано, что с помощью конечного автомата нельзя решить вопрос, является ли данное число квадратом некоторого натурального числа.

Приводимое ниже доказательство демонстрирует общий метод, цель которого состоит в том, чтобы на базе свойства замкнутости некоторого класса множеств показать, что данное множество не принадлежит этому классу. Для применения метода достаточно знать хотя бы одно заведомо не принадлежащее классу множество и получить его из данного множества и множеств, принадлежащих классу, с помощью допустимых операций.

Следствие 5.5.8 (Ритчи). Множество двоичных представлений квадратов натуральных чисел не является допустимым.

Доказательство. Из теоремы 5.5.5 вытекает, что достаточно рассматривать множество Q двоичных представлений без дополнительных нулей (т. е. без нулей, стоящих слева от самой левой единицы), поскольку множество всех двоичных представлений $\bar{Q}$ (с дополнительными нулями) квадратов натуральных чисел удовлетворяет соотношению $1\{0, 1\}^* \cap \bar{Q} = Q$.

Пусть M — множество двоичных представлений (без дополнительных нулей) квадратов вида $(2^{n+1} - 1)^2$ при $n \in \mathbf{N}$.

Так как $(2^{n+1}-1)^2=(2^n-1)2^{n+2}+1$, то множество M является подмножеством допустимого множества L_D из примера 5.3.6.

Нетрудно проверить, что $M/\{0, 1\}=\{1^n0^n \mid n\in\mathbf{N}\}$.

Из теоремы 5.4.12 при $u=1$ и $v=0$ следует, что множество $M/\{0, 1\}$ не допустимо, так что по теореме 5.5.7 не допустимо и множество M.

Покажем теперь, что $L_D\cap Q=M$. Отсюда получим утверждение следствия, так как по теореме 5.5.5 вместе с Q должно бы было быть допустимым и M.

Итак, для чисел a, n и m из **N** таких, что $m+n$ — четное число и $m\geqslant 2$, следует доказать: если $a^2=(2^n-1)2^m+1$, то $m=n+2$ и $a=2^{n+1}-1$.

Пусть $a^2=(2^n-1)2^m+1$, где $n\geqslant 1$, $m\geqslant 2$ и $m+n$ — четное число.

Тогда $a\geqslant 2$ и $(a+1)\cdot(a-1)=(2^n-1)\cdot 2^m$. Отсюда вытекает, что числа $a+1$ и $a-1$ — четные, причем, очевидно, не могут оба делиться на 4, так что одно из них обязательно должно делиться на 2^{m-1}.

Пусть, скажем, $a+1=2^{m-1}b$ при нечетном b. Тогда $(2^n-1)2^m=(a+1)(a-1)=(2^{m-1}b)(2^{m-1}b-2)$, так что $2^n-1=b(2^{m-2}b-1)$ и потому $n\geqslant m-2$.

Такая оценка для n получается и в случае, если $a-1=2^{m-1}b$.

Если a — целое положительное решение уравнения $x^2=2^{m+n}-2^m+1$ при постоянных m и n с четной суммой таких, что $n\geqslant m-2$, то должно существовать натуральное число c такое, что

$$2^{\left(\frac{m+n}{2}\right)}-c=a.$$

При $c\geqslant 2$ было бы справедливо неравенство

$$a^2=\left(2^{\left(\frac{m+n}{2}\right)}-c\right)^2\leqslant 2^{m+n}-4\cdot 2^{\frac{(m+n)}{2}}+4=d.$$

Отсюда, так как $m+n\geqslant 2m-2$, следовало бы $2^{m+n}-2^m+1-d=-2^m+1+4\cdot 2^{\frac{(m+n)}{2}}-4\geqslant -2^m-3+4\cdot 2^{m-1}=2^m-3>0$, т. е $2^{m+n}-2^m+1>d\geqslant a^2$, так что обязательно должно быть $c=1$.

Из равенства

$$\left(2^{\frac{(m+n)}{2}}-1\right)^2=2^{m+n}-2\cdot 2^{\frac{(m+n)}{2}}+1$$

получаем далее, что a может быть решением, только если $2\cdot 2^{\frac{(m+n)}{2}}=2^m$, т. е. $m=n+2$. Тем самым высказанное выше утверждение доказано.■

РАЗРЕШИМОСТЬ НЕКОТОРЫХ ВОПРОСОВ О НРС-АВТОМАТАХ

В информатике возникают вопросы не только о том, являются ли данные утверждения о существовании или методы построения эффективными, но и о том, можно ли эффективным образом установить наличие у объектов некоторых свойств. С такого рода проблемами разрешимости мы уже знакомились — см. следствие 5.3.9 и замечание к следствию 5.5.2. Из того, что рассмотренные там вопросы оказались разрешимыми (эффективно), и из теоремы об итеративном подслове вытекает ряд дальнейших высказываний о разрешимости.

Теорема 5.5.9. Для произвольных НРС-автоматов A и B разрешимы следующие вопросы:

1. Являются ли A и B эквивалентными?
2. Пусто ли множество $L(A)$?
3. Бесконечно ли множество $L(A)$?
4. Выполнено ли включение $L(A) \subseteq L(B)$?
5. Верно ли, что $L(A) = L$, где L — рациональное множество, описанное (конечной) конструкцией в соответствии с определением 5.3.3?
6. Верно ли, что $L(A = L)$, где L задано как различимое множество, т. е. определен конечный моноид M и гомоморфизм h из $F(X)$ на M? (Заметим, что h однозначно определяется уже значениями $h(x)$ для x из X.)

Доказательство. Утверждение о разрешимости вопроса 1 вытекает из теоремы 5.5.3, следствия 5.5.2 и теоремы 3.3.2. Его можно и непосредственно вывести из утверждения о разрешимости вопроса 4.

Утверждение о разрешимости вопроса 2 вытекает из следствия 5.3.9 или из утверждения о разрешимости вопроса 1, если в качестве B выбрать НРС-автомат, для которого допустимым является пустое множество. Простейший метод решения вопроса 2 состоит в проверке, существует ли в графе автомата A «прямой» (без петель) путь из одной из начальных вершин в какую-либо из конечных вершин.

Теорема об итеративном подслове порождает метод решения вопроса 3. Мы можем предположить, что A — РС-автомат с n состояниями (на основании теоремы 5.5.3).

Множество $L = L(A)$ бесконечно тогда и только тогда, когда в L существует слово w_0 длины, большей или равной n. Действительно, такое слово w_0 может быть (см. следствие 5.4.10) разложено так, что $w_0 = uvw$, где $v \neq \Lambda$ и все слова $uv^k w$ при $k = 0, 1, 2, \ldots$ принадлежат L. Если же все слова из L короче n, то L конечно.

Пусть L бесконечно и пусть w_0 — слово из L, имеющее минимальную длину среди всех слов множества L длины, большей или равной n. По следствию 5.4.10 в этом случае существуют слова u, v и w такие, что $w_0 = uvw$, $v \neq \Lambda$, $|uv| < n$ и $uw \in L$. Отсюда вытекает, что $|uw| < w_0$, а из минимальности w_0 следует, что $|uw| < n$, и потому $|w_0| < 2n$.

Итак, чтобы решить вопрос о том, является ли множество L бесконечным, достаточно проверить, допускает ли автомат A какое-либо из конечного множества слов w_0 с $n \leqslant |w_0| < 2n$.

Рассмотрим теперь вопрос 4. По автомату B можно построить (см. доказательство теоремы 5.5.5) РС-автомат C с $L(C) = F(X) - L(B)$. Далее можно построить РС-автомат D с $L(D) = L(A) \cap L(C)$ (см. доказательство той же теоремы). Очевидно, что $L(A) \subseteq L(B)$ тогда и только тогда, когда L(D) пусто, а этот вопрос разрешим — см. утверждение о разрешимости вопроса 2.

Рассматривая вопрос 5, допустим, что L задано как рациональное множество. В этом случае методом из доказательства теоремы Клини (теорема 5.3.5) можно построить НРС-автомат B с $L(B) = L$, после чего использовать утверждение о разрешимости вопроса 1.

Рассмотрим, наконец, вопрос 6. Если L задано как различимое подмножество, то построим методом из доказательства теоремы Майхилла (теорема 5.4.4) РС-автомат B с $L(B) = L$ и применим утверждение о разрешимости вопроса 1. ■

Следствие 5.5.10. Для любых двух подмножеств моноида $F(X)$, заданных как рациональные, различимые или допустимые множества, разрешимы вопросы, являются ли эти множества совпадающими, как дизъюнктными, или одно из них содержит другое.

Пример 5.5.11. 1. Рассмотрим систему совместно протекающих последовательностных процессов, каждый из которых может принимать конечное число состояний. Эти процессы могут быть представлены, как в примере 5.1.1, единственным конечным графом. Тупиковые ситуации соответствуют вершинам графа, из которых не исходят ребра.

Теперь нетрудно предложить алгоритм, устанавливающий, может ли система из определенных начальных состояний прийти в тупиковую ситуацию. Действительно, рассмотрим граф системы как граф некоторого НРС-автомата, финальными состояниями которого являются тупиковые ситуации, и применим доказательство п. 2 теоремы 5.5.9.

Таким же образом можно легко ответить на поставленные в конце примера 5.1.1 вопросы о существовании алгоритмов, которые, во-первых, устанавливают, имеется ли тупиковая ситуация, и во-вторых, вообще не допускают ее возникновения.

Чтобы получить ответ на первый вопрос было бы, однако, неправильным использовать теорему Рабина — Скотта. Действительно, полученный в результате применения этой теоремы РС-автомат A′ должен допускать все последовательности действий, которые могут (но, вообще говоря, не должны) привести к одной из тупиковых ситуаций. Рассмотрим, скажем, в условиях примера 5.1.1 последовательность ABAB: она может привести не только в состояние 22, но и в состояния 00, 02 и 20. Если бы автомат, эквивалентный РС-автомату A′, использовался как индикатор тупиковых ситуаций, то он должен был бы во всех случаях, на-

пример, когда система снова пришла в начальное состояние 00, сигнализировать о возникновении тупиковой ситуации.

Чтобы в данном случае построить детерминированный алгоритм, необходимо более точно описать саму систему процессов. В условиях примера 5.1.1 следует делать различие между действиями студентов: пусть a_i (соответственно — b_i), i=1, 2, 3, означает получение, возврат и заказ книги студентом A(B). Тогда, например, последовательность $a_1b_1a_3b_3$ ведет в тупиковую ситуацию, а последовательность $a_1b_1a_2b_2$ — нет. Полученный таким образом ДРС-автомат A_0 представляет собой детерминированный алгоритм для сигнализации о возникновении тупиковой ситуации.

Используя автомат A_0 можно сразу построить и ДРС-автомат, представляющий алгоритм, с помощью которого можно избежать тупиковой ситуации. В качестве финальных состояний такого автомата следует выбрать все состояния, не являющиеся ни тупиковыми, ни такими, из которых система с необходимостью переходит в тупиковое состояние (т. е. такими, что все исходящие из них пути ведут в тупиковые состояния). Используя этот автомат, можно избежать тупиковой ситуации, если выбирать только допустимые этим автоматом последовательности действий.

2. Две схемы программ (см. пример 5.1.2) можно назвать слабо эквивалентными, если языки значений этих схем совпадают. По теореме 5.5.9, п.1 вопрос о слабой эквивалентности схем программ, удовлетворяющих условиям из замечания в примере 5.1.2, разрешим, поскольку языки значений таких схем программ являются рациональными множествами (см. также пример 5.3.4).

5 6 РАВЕНСТВА И СИСТЕМЫ РАВЕНСТВ

На основе примеров 5.3.6 и 5.3.8 можно заключить, что одно и то же множество может иметь два различных представления в виде рационального множества. В связи с этим возникает проблема тождества двух рациональных представлений множеств (т. е. проблема определения того, являются ли два данных рациональных представлений представлениями одного и того же множества). Из следствия 5.5.10 вытекает, что эта проблема всегда имеет эффективное решение, хотя оно и получается окольным путем — построением соответствующих НРС-автоматов.

В данном и в следующих разделах будет разработан математический аппарат, позволяющий устанавливать тождественность рациональных представлений множеств, используя только преобразования таких представлений. Вообще говоря, необходимое при этом число операций все же не уменьшается, поскольку в худшем случае оно также оказывается экспоненциальным по отношению к длине выражений (см. также разд. 6.2).

Из того факта, что рациональная операция «объединения» совпадает с операцией теоретико-множественного объединения,

рациональная операция «произведения» — с операцией произведения подмножеств моноида $F(X)$, а операция образования подмоноида может рассматриваться как бесконечное объединение всех конечных степеней данного множества, непосредственно вытекает ряд равенств между рациональными представлениями множеств. Эти равенства очень удобно использовать для преобразования таких представлений.

Читателю рекомендуется также обратить внимание на приведенные в упражнении 5.18 п. 1 отрицания равенств.

Теорема 5.6.1. Пусть R, S и T — произвольные рациональные подмножества моноида $F(X)$. Тогда справедливы следующие равенства:

(0) $\varnothing^* = \{\Lambda\}$,
(1) $R \cup (S \cup T) = (R \cup S) \cup T$,
(2) $R(ST) = (RS)T$,
(3) $R \cup S = S \cup R$,
(4) $R(S \cup T) = RS \cup RT$,
(5) $(R \cup S)T = RT \cup ST$,
(6) $R \cup R = R$,
(7) $\varnothing^* R = R$,
(7′) $R\varnothing^* = R$,
(8) $\varnothing R = \varnothing$,
(8′) $R\varnothing = \varnothing$,
(9) $R \cup \varnothing = R$,
(10) $R^* = \varnothing^* \cup R^* R$,
(10′) $R^* = \varnothing^* \cup RR^*$,
(11) $R^* = (\varnothing^* \cup R)^*$,
(12) $(R^*)^* = R^*$,
(13) $R^* R^* = R^*$,
(14) $(R \cup S)^* = (R^* S^*)^*$,
(15) $(R \cup S)^* = (R^* S)^* R^*$,
(16) $(R \cup S)^* = S^* (RS^*)^*$,
(17) $(R \cup S)^* = R^* \cup R^* S (R \cup S)^*$,
(18) $(R \cup S)^* = (R^* S)^* \cup (S^* R)^*$,
(19) $(RS)^* R = R(SR)^*$,
(20) $(R^* S)^* = \varnothing^* \cup (R \cup S)^* S$,
(21) $(RS^* T)^* = \varnothing^* \cup R(S \cup TR)^* T$,
(22) $R^m (R^n)^* = (R^n)^* R^m$,
(23) $R^* = (\varnothing^* \cup R \cup \ldots \cup R^{n-1})(R^n)^*$.

Доказательство. Справедливость равенств (0)—(13), (19), (22) и (23) непосредственно вытекает из сказанного выше (см. упражнение 5.5).

Замечание. В дальнейшем данные равенства будут использоваться без указания их номеров в данной теореме.

Мы докажем сначала равенства (17) и (21) непосредственно, а потом с помощью преобразований выведем из них остальные равенства [(14)—(16), (18) и (20)].

Равенство (17). Включение $(R \cup S)^* \supseteq R^* \cup R^*S(R \cup S)^*$ вытекает из $R^* \subseteq (R \cup S)^*$ и из того, что $R^m S(R \cup S)^n \subseteq (R \cup S)^{m+1}(R \cup S)^n$ при всех m и n из $\mathbf{N}_0$.

Чтобы доказать, что

$$(R \cup S)^* \subseteq R^* \cup R^*S(R \cup S)^*,$$

полной индукцией по n докажем, что при всех натуральных n

$$(R \cup S)^n \subseteq R^* \cup R^*S(R \cup S)^*.$$

При $n=1$ утверждение очевидно. Допустим, что оно верно и при $n=k$. Тогда получаем

$$\begin{aligned}(R \cup S)^{k+1} &= (R \cup S)(R \cup S)^k \subseteq (R \cup S)(R^* \cup R^*S(R \cup S)^*) = \\ &= RR^* \cup RR^*S(R \cup S)^* \cup S(R^* \cup R^*S(R \cup S)^*) \subseteq \\ &\subseteq R^* \cup RR^*S(R \cup S)^* \cup S(R \cup S)^* = \\ &= R^* \cup R^*S(R \cup S)^*.\end{aligned}$$

Равенство (21). Из равенства (17), заменяя R на S и S на TR, получаем

$$R(S \cup TR)^*T = RS^*T \cup RS^*TR(S \cup TR)^*T,$$

а отсюда методом полной индукции для каждого n из $\mathbf{N}$ получаем

$$R(S \cup TR)^*T = RS^*T \cup (RS^*T)^2 \cup \ldots \cup (RS^*T)^n \cup (RS^*T)^n R(S \cup TR)^*T.$$

Отсюда вытекает, что $(RS^*T)^n \subseteq \varnothing^* \cup R(S \cup TR)^*T$ при любом n из $\mathbf{N}_0$, так что

$$(RS^*T)^* \subseteq \varnothing^* \cup R(S \cup TR)^*T.$$

Чтобы доказать включение $(RS^*T)^* \supseteq \varnothing^* \cup R(S \cup TR)^*T$, покажем сначала, используя полную индукцию, что при всех n из $\mathbf{N}_0$ выполняется включение

$$RS^*(S \cup TR)^n S^*T \subseteq (RS^*T)^*. \tag{1}$$

При $n=0$ включение (1) очевидно. Допустим, что оно выполнено при $n=k$. Тогда

$$\begin{aligned}&RS^*(S \cup TR)(S \cup TR)^k S^*T = RS^*S(S \cup TR)^k S^*T \cup \\ &\cup RS^*TR(S \cup TR)^k S^*T \subseteq RS^*(S \cup TR)^k S^*T \cup RS^*T \times \\ &\times (RS^*(S \cup TR)^k S^*T) \subseteq (RS^*T)^* \cup RS^*T(RS^*T)^* = (RS^*T)^*.\end{aligned}$$

Из включения (1) для любого n из $\mathbf{N}_0$ вытекает включение $R(S \cup TR)^nT \subseteq (RS^*T)^*$, откуда немедленно следует доказываемое утверждение.

Равенство (20). Положив в (21) $R=\varnothing^*$, $S=R$ и $T=S$, получаем (20).

Равенство (16). Применяя сначала равенство (21) при $T=\varnothing^*$, потом равенство (17), меняя ролями R и S, получаем равенство (16):

$$S^*(RS^*)^*=S^*(\varnothing^*\cup R(S\cup R)^*)=$$
$$=S^*\cup S^*R(S\cup R)^*=(S\cup R)^*=(R\cup S)^*.$$

Равенство (15). Применяем равенство (19), используя R^* вместо R, и равенство (16), меняя ролями R и S:

$$(R^*S)^*R^*=R^*(SR^*)^*=(S\cup R)^*.$$

Равенство (14). Применяем равенство (20), используя S^* вместо S, (15), используя S^* вместо R и R вместо S; (12), (13) и (15), меняя ролями R и S:

$$(R^*S^*)^*=\varnothing^*\cup(R\cup S^*)^*S^*=\varnothing^*\cup((S^*)^*R)^*\times$$
$$\times(S^*)^*S^*=\varnothing^*\cup(S^*R)^*S^*=\varnothing^*\cup(S\cup R)^*.$$

Равенство (18). Из включения $(R^*S)^*\subseteq(R^*S)^*R$ и равенства (15) вытекает цепочка равенств

$$(R^*S)^*R^*=(R^*S)^*\cup(R^*S)^*R^*=$$
$$=(R^*S)^*\cup(S^*R)^*S^*=(R^*S)^*\cup(S^*R)^*\cup(S^*R)^*S^*S.$$

Поскольку из (20) и (15) следует, что

$$(R^*S)^*=\varnothing^*\cup(R\cup S)^*S=\varnothing^*\cup(S^*R)^*S^*S,$$

то из полученной выше цепочки равенств немедленно вытекает равенство (18). ■

СИСТЕМА РАВЕНСТВ НРС-АВТОМАТА

Каждому НРС-автомату может быть сопоставлена некоторая система равенств над рациональными множествами, из которой может быть определена реакция этого автомата.

Пример 5.6.2. Рассмотрим определенный графом, изображенным на рис. 5.6.1, НРС-автомат A_0.

Пусть L_i — множество входных слов, переводящих автомат A_0 из состояния z_i в одно из финальных состояний. В частности, $L_1=L(A_0)$.

Тогда

$$L_1=0L_1\cup 11L_2\cup\Lambda L_2\cup 11L_3=0L_1\cup\{\Lambda,\ 11\}L_2\cup 11L_3,$$
$$L_2=\Lambda L_1\cup 0L_2\cup\Lambda L_3\cup\Lambda,$$
$$L_3=0L_2\cup\Lambda.$$

Если мы введем «неизвестные» y_1, y_2 и y_3 и будем вместо знака «$\cup$» использовать знак «+», то получим систему равенств

$$y_1=0y_1+\{\Lambda,\ 11\}y_2+11y_3,$$
$$y_2=\Lambda y_1+0y_2+\Lambda y_3+\Lambda,$$
$$y_3=\varnothing y_1+0y_2+\varnothing y_3+\Lambda.$$

Вектор $(y_1, y_2, y_3) = (L_1, L_2, L_3)$ оказывается тогда решением системы. Это решение можно получить, если сначала преобразовать данную систему, как обычную систему уравнений в линейной алгебре, используя метод исключения неизвестных (метод Гаусса), а потом попытаться подобрать решение получившейся системы.

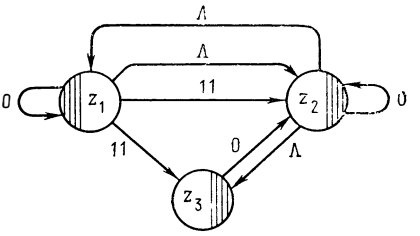


Рис. 5.6.1. НРС-автомат A_0

Заменяя y_3 в уравнениях для y_1 и y_2, получаем

$$y_1 = 0y_1 + \{\Lambda, 11\}y_2 + 110y_2 + 11 = 0y_1 + \{\Lambda, 11, 110\}y_2 + 11,$$

$$y_2 = y_1 + 0y_2 + 0y_2 + \Lambda + \Lambda = y_1 + 0y_2 + \Lambda = 0y_2 + (y_1 + \Lambda).$$

При постоянном y_1 решение уравнения для y_2 можно искать с помощью последовательных приближений:

$$y_2^{(0)} = \Lambda,\ y_2^{(1)} = 0 + y_1 + \Lambda,\ y_2^{(2)} = 00 + 0(y_1 + \Lambda) + (y_1 + \Lambda),$$

$$y_2^{(3)} = 000 + 00(y_1 + \Lambda) + 0(y_1 + \Lambda) + (y_1 + \Lambda), \ldots$$

Отсюда (методом полной индукции) определяем, что при всех натуральных i выполняется включение $y_2 \supseteq y_2^{(i)}$. Действительно, $y_2 \supseteq \Lambda$ и из $y_2 \supseteq y_2^{(i)}$ следует, что $y_2 = 0y_2 + y_1 + \Lambda \supseteq 0y_2^{(i)} + y_1 + \Lambda = y_2^{(i+1)}$. Итак, $y_2 \supseteq \bigcup\{y_2^{(i)} \mid i \in N_0\}$, т. е. $y_2 \supseteq 0^* + 0^*(y_1 + \Lambda) = 0^*(y_1 + \Lambda)$.

Подставляя последнее включение в равенство для y_1, находим

$$y_1 \supseteq 0y_1 + \{\Lambda, 11, 110\}0^*(y_1 + \Lambda) + 11 =$$

$$= (0 \cup 0^* \cup 110^* \cup 1100^*)y_1 + (0^* \cup 110^* \cup 1100^* \cup 11) =$$

$$= (0^* \cup 110^*)y_1 + (0^* \cup 110^*).$$

Используя последовательные приближения (как и в случае y_2), из последнего включения получаем $y_1 \supseteq (0^* \cup 110^*)^*(0^* \cup 110^*)$.

Подстановка правой части этого включения вместо y_1 в «неравенство» для y_2 и в равенство для y_3 дает $y_2 \supseteq 0^*(0^* \cup 110^*)^*$ и $y_3 \supseteq 00^*(0^* \cup 110^*)^* \cup \Lambda$.

Покажем теперь, что наименьшие (онтосительно включения) значения, которые могут принимать y_1, y_2 и y_3, в точности совпадают с реакциями L_1, L_2 и L_3. Для этого нам понадобятся три правила исключения, приведенные в доказательстве 5.3.7.

Ясно, что правила исключения не обязательно должны применяться в порядке, определяемом блок-схемой, изображенной на рис. 5.3.6.

Как и в доказательстве теоремы 5.3.7, присоединим прежде всего к графу автомата A_0 новое начальное состояние α и новое финальное состояние ω.

Применение правила E к состоянию z_3 (см. рис. 5.6.1) и последующее применение правила K соответствует подстановке

правой части уравнения для y_3 вместо y_3 в уравнения для y_1 и y_2. После этого получаем граф, в котором из z_1 в ω ведет ребро с меткой 11, из z_1 в z_2 — ребро с меткой $\{\Lambda\}\cup\{11\}\cup\{110\}$, остальные же метки и ребра не изменяются.

Исключение с помощью правила S петли у вершины z_2 приводит к появлению на ребрах, ведущих из z_2 в z_1 и в ω, меток 0^* — это полученное при последовательных приближениях наименьшее значение для y_2.

Теперь исключение с помощью правила E вершины z_2 (и последующее применение правила K) приводит к появлению петли у вершины z_1, а у ребра, ведущего из z_1 в ω, — метки $(0^*\cup 110^*)$.

Последнее исключение петли у вершины z_1 показывает, что полученное выше наименьшее значение для z_1 совпадает с L_1, откуда следует, что наименьшими значениями для y_2 и y_3 являются L_2 и L_3 соответственно.

Реакции L_1, L_2 и L_3 не являются, однако, единственным решением системы уравнений. Возьмем, например,

$$L_1' = (0^*\cup 110^*)^*(0^*\cup 110^*\cup\{111\}) = L_1\cup(0^*\cup 110^*)^*111,$$

т. е. $L_1'\neq L_1$. Используя теперь соотношения для y_2 и y_3, выберем

$$L_2' = 0^*L_1'\cup 0^* = L_2\cup 0^*(0^*\cup 110^*)^*111 \neq L_2,$$

$$L_3' = 0L_2'\cup\Lambda = L_3\cup 0(0^*\cup 110^*)^*111 \neq L_3.$$

Чтобы показать, что L_1', L_2' и L_3' составляют решение нашей системы уравнений, нужно только доказать, что $0^*L_1'\subseteq L_1'$ и $11L_2'\subseteq L_1'$. Действительно, включения $L_1'\subseteq L_2'$ и $0L_2'\subseteq L_3'\subseteq L_2'$ вытекают непосредственно из определения L_2' и L_3' и вместе с $11L_2'\subseteq L_1'$ приводят к $11L_3'\subseteq L_1'$. Далее, из $0^*L_1'\subseteq L_1'$ немедленно следует, что $0L_1'\subseteq L_1'$, а так как $0^*\subseteq L_1'$, то и $L_2'\subseteq L_1'$ (так что даже $L_2'=L_1'$).

Используя равенство (17) из теоремы 5.6.1, получаем

$$0^*\cup 0^*110^*(0^*\cup 110^*)^* = (0^*\cup 110^*)^*.$$

Отсюда сразу находим, что $0^*L_1'\subseteq L_1'$ и $11L_2' = 11L_1'\subseteq L_1'$.

Из сказанного вытекает также равенство $L_2=L_1$, что можно, впрочем, усмотреть и непосредственно из самой системы уравнений, так как для любого решения U_1, U_2, U_3 этой системы из первого уравнения вытекает включение $U_1\supseteq U_2$, а из второго — $U_2\supseteq U_1$.

Теперь мы займемся более подробным исследованием намеченной в примере 5.6.2 связи между реакцией НРС-автомата и решением соответствующей системы уравнений.

Определение 5.6.3. Пусть состояния НРС-автомата A занумерованы таким образом, что $Z=\{z_1, z_2, \ldots, z_n\}$ и $S=\{z_1, z_2, \ldots \ldots, z_m\}$.

1. *Реакцией состояния* z_i будем называть множество $L_i = \{w \in F(X) \mid t^*(z_i, w) \cap F \neq \varnothing\}$, т. е. L_i — это реакция НРС-автомата A_i, получающегося из A в результате замены S на $\{z_i\}$.

Пусть, далее, L_{ij} при $i, j \in \{1, \ldots, n\}$ — множество всех меток в графе автомата A на ребрах, ведущих из z_i в z_j, т. е. $L_{ij} = \{w \in F(X) \mid (z_i, w, z_j) \in \tau\}$.

Пусть, наконец, при каждом $i = 1, \ldots, n$

$$\delta_i = \begin{cases} \Lambda, & \text{если } z_i \in F, \\ \varnothing & \text{в противном случае,} \end{cases}$$

т. е. δ_i определяет, содержится ли в соответствующем автомату A обобщенном графе переходов (см. доказательство теоремы 5.3.7) ребро с меткой Λ, ведущее из z_i в ω.

2. Пусть $Y = \{y_1, \ldots, y_n\}$ — непересекающееся с множеством входов X множество переменных (неизвестных), которые могут принимать значения из булеана $\mathscr{P}(F(X))$. Соответствующей автомату A системой уравнений Gl(A) называется система

$$y_1 = L_{11}y_1 + L_{12}y_2 + \ldots + L_{1n}y_n + \delta_1,$$

$$y_2 = L_{21}y_1 + L_{22}y_2 + \ldots + L_{2n}y_n + \delta_2.$$

. . . . . .

$$y_n = L_{n1}y_1 + L_{n2}y_2 + \ldots + L_{nn}y_n + \delta_n.$$

Если вектор-столбец переменных y_i обозначить символом y, вектор-столбец значений δ_i — символом δ и $n \times n$-матрицу с компонентами $m_{ij} = L_{ij}$ — символом M, то можно, вводя умножение и сложение векторов и матриц формально так же, как в линейной алгебре, записать приведенную выше систему уравнений в виде

$$y = My + \delta.$$

Здесь умножение — обычное произведение множеств слов из $\mathscr{P}(F(X))$ и сложение — теоретико-множественное объединение.

Далее определим M^0 как единичную матрицу E, в которой на главной диагонали стоят символы Λ (т. е. $e_{ii} = \Lambda$), а все остальные компоненты равны $\varnothing$ (т. е. $e_{ij} = \varnothing$ при $i \neq j$). Кроме того, положим $M^i = MM^{i-1}$ при $i = 1, 2, \ldots$

Поскольку в $\mathscr{P}(F(X))$ существуют бесконечные суммы (т. е. бесконечные теоретико-множественные объединения), то можно построить $M^* = \sum_{i=0}^{\infty} M^i$.

Определим, наконец, для n-компонентных векторов над $\mathscr{P}(F(X))$ отношение включения: если U и V — векторы над $\mathscr{P}(F(X))$ (n-компонентные), то $U \subseteq V$ тогда и только тогда, когда $U_i \subseteq V_i$ при всех $i = 1, \ldots, n$.

Хотя мы будем использовать только векторы-столбцы, но, задавая такие векторы покомпонентно, будем записывать их как векторы-строки.

Вектор $V=(V_1, \ldots, V_n)$ с $V_i \subseteq F(X)$ является *решением* описанной выше системы уравнений, если

$$V=MV+\delta.$$

Замечание. Пункт 3 упражнения 5.18 показывает, что НРС-автомату можно сопоставить систему равенств отличным от описанного выше способом.

Теорема 5.6.4. (Арден). Пусть A — НРС-автомат из определения 5.6.3, $L=(L_1, \ldots, L_n)$ — вектор реакций состояний этого автомата и Gl(A) — соответствующая автомату A система уравнений. Тогда:

1. L удовлетворяет Gl(A), т. е. справедливо равенство $L=ML+\delta$.

2. Вектор L может быть получен из δ путем последовательных приближений, т. е. если положить $L^{(0)}=\delta$ и $L^{(k)}=ML^{(k-1)}$ при $k \geqslant 1$, то $L=L^{(0)}+L^{(1)}+\ldots$, т. е. $L=M^*\delta$.

3. Для любого решения V системы Gl(A) выполнено условие $L \subseteq V$, т. е. $L=M^*\delta$ является наименьшим (по включению) решением системы Gl(A).

Доказательство. 1. Как и в примере 5.6.2, нетрудно убедиться в том, что $L_i=L_{i1}L_1+L_{i2}L_2+\ldots+L_{in}L_n+\delta_i$ при любом $i=1, \ldots, n$.

Отсюда немедленно вытекает, что $L=ML+\delta$. Таким образом, условие 1 выполнено.

2. Пусть V — произвольное решение системы Gl(A). Тогда $L^{(0)}=\delta \subseteq V$ и $MV \subseteq V$, откуда методом полной индукции получаем, что при всех k из $\mathbf{N}_0$ выполнено включение $L^{(k)} \subseteq V$. Итак, $M^*\delta \subseteq V$.

3. На основании пп. 1 и 2 выполняется включение $M^*\delta \subseteq L$. Если мы покажем, что $M^*\delta \supseteq L$, то теорема будет полностью доказана.

Чтобы доказать, что $M^*\delta \supseteq L$, полной индукцией по k покажем, что для i-й компоненты $L_i^{(k)}$ вектора $L^{(k)}$ (при $i=1, \ldots, n$) выполнено условие $L_i^{(k)}=\{w \in F(X) \mid$ существует состояние $z \in F$ такое, что $(z_i, w, z) \in \tau^k\}=\{w \in F(X) \mid$ существуют $s_0, s_1, \ldots, s_k \in Z$ и $u_1, u_2, \ldots, u_k \in F(X)$ такие, что $z_i=s_0$, $s_k \in F$, $(s_{j-1}, u_j, s_j) \in \tau$ при $j=1, \ldots, k$ и $u_1u_2 \ldots u_k=w\}$.

При $k=0$ и $k=1$ выполнение данного условия очевидно. Допустим, что оно выполнено при фиксированном $k \geqslant 1$.

По определению

$$L_i^{(k+1)}=L_{i1}L_1^{(k)}+L_{i2}L_2^{(k)}+\ldots+L_{in}L_n^{(k)}+\delta_i,$$

причем $L_{ij}=pr_2(\tau \cap \{z_i\} \times F(X) \times \{z_j\})$.

По предположению индукции любое слово w из $L_{ij}L_j^{(k)}$ имеет вид $w=uw'$, где $u \in pr_2(\tau)$ и $w' \in pr_2(\tau^k)$, так что $w \in pr_2(\tau^{k+1})$.

Поскольку для каждого слова w существуют начальное состояние z_i и натуральное число k такие, что w из z_i через k не-

спонтанных переходов приводит автомат в некоторое финальное состояние, то для каждого w из L существует множество $L_i^{(k)}$ такое, что $w \in L_i^{(k)}$, а это и означает выполнение включения $L \subseteq M^*\delta$. ∎

ОБЩИЕ ЛИНЕЙНЫЕ СИСТЕМЫ РАВЕНСТВ

Чтобы решить вопрос об условиях, обеспечивающих единственность решения системы равенств, и получить формулу для решения, рассмотрим случай общей линейной системы над $\mathscr{P}(F(X))$, т. е. системы равенств вида $y = My + R$, где элементы матрицы M и компоненты вектора R являются произвольными подмножествами моноида $F(X)$.

Для того чтобы сформулировать условие, обеспечивающее единственность решения, нам понадобится следующее определение.

Определение 5.6.5. $n \times n$-матрица $M = \|m_{ij}\|$, где $m_{ij} \subseteq F(X)$ при $1 \leqslant i, j \leqslant n$, обладает *свойством пустого слова,* если существует последовательность $i_1, i_2, \ldots, i_k$ $(k \geqslant 1)$ индексов из $\{1, \ldots, n\}$ такая, что $\Lambda \in m_{i_p i_{p+1}}$ при $1 \leqslant p \leqslant k-1$ и $\Lambda \in m_{i_k i_1}$. Каждая такая последовательность индексов называется *LW-последовательностью* матрицы M.

Замечание. Каждая матрица, на главной диагонали которой встречается множество, содержащее Λ, обладает свойством пустого слова. В случае $k=2$ определение требует существования p и q таких, что $\Lambda \in m_{pq} \cap m_{qp}$, этот случай рассматривался в примере 5.6.2.

Теорема 5.6.6. (Арден, Боднарчук). 1. Система равенств $y = My + P$ над $\mathscr{P}(F(X))$ имеет единственное решение, если M не обладает свойством пустого слова.

Решение в этом случае имеет вид $y = M^*R$.

Если при этом все компоненты R и все элементы M — рациональные множества, то и все компоненты решения M^*R — рациональные множества, причем решение может быть построено эффективно.

2. Если M обладает свойством пустого слова, то каждый вектор $V = M^*(R+T)$, где $T_i = \varnothing$ при всех i, не входящих ни в одну LW-последовательность матрицы M, является решением системы $y = My + R$, в частности вектор M^*R является решением.

Вектор M^*R содержится в каждом решении рассматриваемой системы равенств, и векторы вида $M^*(R+U)$ с $U \subseteq M^*R + MM^*U$ также являются решениями.

Замечания. 1. Если M обладает свойством пустого слова, то каждое решение системы равенств $y = My + R$ имеет вид $M^*(R+T)$, где T — вектор такой, что $T_i = \varnothing$ при всех i, не входящих ни в одну LW-последовательность матрицы M (см. п.2 упражнения 5.19).

2. Для системы равенств $y = yM + R$ справедливы совершенно аналогичные утверждения (см. п. 1 упражнения 5.19).

Доказательство теоремы. Пусть M — $n\times n$-матрица и R — n-компонентный вектор над $\mathscr{P}(F(X))$.

Рассмотрим систему равенств $y=My+R$.

1. Так как $M(M^*R)+R=(MM^*+E)R=M^*R$, то вектор M^*R является решением данной системы равенств.

Если V — произвольное решение рассматриваемой системы равенств, то $V=MV+R$, $V=M(MV+R)+R$ и так далее, т. е. при всех k из $\mathbf{N}$

$$V=M^{k+1}V+M^kR+M^{k-1}R+\ \dots\ +MR+R. \tag{2}$$

Отсюда вытекает, что $M^*R\subseteq V$.

2. Любой элемент $m_{ij}^{(p+1)}$ матрицы $M^{(p+1)}$ при $p\geqslant 0$ имеет вид $m_{i1}m_{1j}^{(p)}+m_{i2}m_{2j}^{(p)}+\ \dots\ +m_{in}m_{nj}^{(p)}$. Если Λ содержится в одном из «слагаемых», то должен существовать индекс k такой, что $\Lambda\in m_{ik}\cap m_{kj}^{(p)}$, поскольку пустое слово Λ принадлежит произведению двух множеств слов тогда и только тогда, когда оно принадлежит каждому из этих множеств (см. упражнение 5.5).

Итак, если некоторый элемент матрицы M^q при каком-то $q\geqslant n$ содержит пустое слово, то должна существовать последовательность $j_0, j_1, \dots, j_q$ индексов из $\{1, \dots, n\}$ такая, что $\Lambda\in m_{j_ij_{i+1}}$ при $i=0, 1, \dots, q-1$. Из неравенства $q\geqslant n$ следует, что не все индексы в данной последовательности могут быть различны, т. е. существуют r и s $(0\leqslant r<s\leqslant q)$ такие, что $j_r=j_s$. В этом случае последовательность $j_r, j_{r+1}, \dots, j_{s-1}$ оказывается LM-последовательностью матрицы M, т. е. M обладает свойством пустого слова.

3. Если M не обладает свойством пустого слова, то, как следует из п. 2, ни один элемент матриц M^p при $p\geqslant n$ не содержит пустого слова. Пусть тогда V — произвольное решение рассматриваемой системы равенств, $i\in\{1, \dots, n\}$, w — слово из V_i и $r=|w|$. Пусть, далее, $k+1=(r+1)n$. Тогда каждый непустой элемент матрицы M^{k+1} содержит только слова длины, не меньшей $r+1$. Поэтому слово w не может содержаться ни в одной компоненте вектора $M^{k+1}V$. Из формулы (2) (см. п.1 доказательства) вытекает, что слово w должно содержаться в некоторой компоненте одного из векторов M^iR при $1\leqslant i\leqslant k$ и потому также в некоторой компоненте вектора M^*R. Отсюда следует, что $V\subseteq M^*R$, что вместе с п. 1 доказательства дает $V=M^*R$.

Итак, первая часть утверждения 1 теоремы доказана.

4. Допустим теперь, что матрица M обладает свойством пустого слова и пусть V — некоторое произвольное решение рассматриваемой системы равенств. Из результатов п.1 доказательства следует, что $V=M^*R+U$.

Подставляя это выражение в систему, имеем

$$M^*R+U=M(M^*R+U)+R=MM^*R+MU+R.$$

Отсюда вытекает, что $MU\subseteq M^*R+U$ и, далее,

$$M^2U\subseteq M(M^*R+U)\subseteq M^*R+U.$$

Таким образом, для всех натуральных чисел k получаем $M^kU \subseteq M^*R+U=V$ и поэтому $M^*U \subseteq V$.

Итак, $V=V+M^*U=M^*(R+U)$.

Снова подставляя полученное выражение для V в исходную систему, получаем

$M^*(R+U)=MM^*(R+U)+R$, т. е.

$M^*R+M^*U=M^*R+MM^*U$.

Отсюда

$$U \subseteq M^*R+MM^*U. \tag{3}$$

В то же время из формулы (3) снова вытекает включение $M^*U \subseteq M^*R+MM^*U$, а отсюда следует, что $M^*(R+U)$ является решением. Итак, условие (3) — необходимое и достаточное условие для того, чтобы вектор $M^*(R+U)$ был решением рассматриваемой системы равенств.

5. Пусть снова M — матрица, обладающая свойством пустого слова, и $V=M^*(R+T)$, где $T_i=\varnothing$ для всех i, не входящих ни в одну LW-последовательность матрицы M. Для таких i очевидным образом выполнено включение

$$T_i \subseteq (M^*R+MM^*T)_i.$$

Пусть теперь j — индекс из некоторой LW-последовательности. Тогда должно существовать натуральное число k такое, что $\Lambda \in (M^k)_{jj}$ [1]. Отсюда следует, что $T_j \subseteq (M^kT)_j$, так что при $U=T$ выполнено условие (3) и поэтому V является решением.

Утверждение 2 теоремы доказано.

6. Допустим теперь, что все элементы матрицы M и все компоненты вектора R — рациональные множества и что матрица M не обладает свойством пустого слова. Полной индукцией по числу строк n матрицы M докажем, что в этом случае все компоненты вектора M^*R — рациональные множества, причем доказательство будет одновременно определять способ построения этих множеств.

При $n=1$ утверждение очевидно.

Допустим, что утверждение верно при $n=k-1$. Рассмотрим систему равенств с $n=k$ неизвестными. В последнем равенстве этой системы, записанном в виде

$y_k=(m_{k1}y_1+ \ldots +m_{k(k-1)}y_{k-1}+R_k)+m_{kk}y_k$, заключенное в скобки выражение будем считать известным, т. е. определенным множеством слов. Таким образом, мы получаем случай системы из одного равенства с одним неизвестным, и поскольку выполнено условие $\Lambda \notin m_{kk}$, это уравнение имеет единственное решение

$$y_k=m^*_{kk}(m_{k1}y_1+ \ldots +m_{k(k-1)}y_{k-1}+R_k).$$

Подставляя это решение в первые $k-1$ уравнения системы, получаем систему из $k-1$ уравнения вида

$y_i=(m_{il}+m_{ik}m^*_{kk}m_{k1})y_1+ \ldots +(m_{i(k-1)}+$

[1] Т. е. если $M^k=\|m_{ij}^{(k)}\|$, то $\Lambda \in m_{jj}^{(k)}$. — *Прим. перев.*

$+m_{ik}m^*_{kk}m_{k(k-1)})y_{k-1}+R_i+m_{ik}m^*_{kk}R_k$.

Элементы $(k-1)\times(k-1)$-матрицы M' этой системы имеют, таким образом, вид $m'_{ij}=m_{ij}+m_{ik}m^*_{kk}m_{kj}$.

Если бы теперь было выполнено включение $\Lambda\in m'_{ij}$, то выполнялось бы и включение $\Lambda\in M_{ij}$ или $\Lambda\in m_{ik}\cap m_{kj}$. Иначе говоря, если бы матрица M' обладала свойством пустого слова, то и матрица M обладала бы им. Поэтому матрица M' не может обладать свойством пустого слова.

Множества m'_{ij}, очевидно, рациональны, если рациональны множества m_{ij}.

По предположению индукции система равенств

$$y'=M'y'+R' \text{ с } R_i'=R_i+m_{ik}m^*_{kk}R_k$$

имеет единственное решение, компоненты которого являются рациональными множествами, так как если рациональны R_i, то и R_i' рациональны.

Итак, получено решение с рациональными компонентами для системы из $n=k$ равенств.

Утверждение 1 теоремы полностью доказано. ■

Следствие 5.6.7. Система равенств, соответствующая побуквенному НРС-автомату, имеет только одно решение.

Следствие 5.6.8. Если L и R — рациональные множества и $\Lambda\notin L$, то уравнение $y=Ly+R$ имеет единственное решение $y=L^*R$.

О решении уравнения вида $y=Uy+yV+R$ см. п.3 упражнения 5.19.

5.7. РАЦИОНАЛЬНЫЕ ВЫРАЖЕНИЯ

Представление допустимых множеств в виде рациональных является одним из важнейших средств теории автоматов. Поскольку, как мы видели, возможны различные представления одного и того же множества с помощью рациональных операций и так как эквивалентность различных представлений может быть показана с помощью большого числа различных правил, полезно иметь в своем распоряжении формальное исчисление, облегчающее корректную и систематическую обработку рациональных представлений. Чтобы получить такое исчисление, можно действовать так, как это принято в математической логике: сначала определить синтаксис формального языка для описания рациональных множеств и равенств, потом задать формальное определение семантики языковых конструкций. После этого можно ставить вопрос: когда различные (языковые) конструкции являются эквивалентными, т. е. имеют одинаковое значение, и каким образом может быть установлена такая эквивалентность? Наконец, возникает проблема аксиоматизации для исчисления с равенством.

Пусть, как обычно, X — произвольное фиксированное непустое конечное множество с m элементами $x_1, \ldots, x_m$. Алфавит формального языка рациональных выражений [для описания рациональных подмножеств моноида F(X)] содержит знаки:

индивидных констант, т. е. обозначения фиксированных индивидов (объектов), из которых строятся остальные индивиды (здесь — элементы множества Rat(X)):

$\varnothing$ — для пустого множества и $x_1, \ldots, x_m$ — для множеств $\{x_i\}$ при $i=1, \ldots, m$;

функциональных констант, т. е. в данном случае обозначения рациональных операций:

$+$ — для объединения,

$\cdot$ — для произведения (множеств слов),

* — для операции образования подмоноида;

предикатной константы, с помощью которой будет обозначаться совпадение множеств, описанных, вообще говоря, различными выражениями:

$=$

вспомогательных символов — правой и левой скобки:

), (.

При этом предполагается, что знаки x_i отличаются друг от друга и от всех остальных используемых знаков.

В качестве метаязыковых символов будут использоваться:

строчные греческие буквы, в частности α, β, γ, как обозначения для выражений (при этом мы всегда вместо «выражение, обозначенное символом α» будем говорить «выражение α»).

знак $\equiv$, используемый для записи того факта, что различные (вообще говоря) символы для выражений относятся к одному и тому же выражению, т. е. $\alpha \equiv \beta$ означает, что α и β являются одной и той же последовательностью символов.

Определение 5.7.1. Пусть $X=\{x_1, \ldots, x_m\}$ и $K=X \cup \varnothing, +, \cdot, ^*,), ($.

1. Множество RA(X) *рациональных выражений над* X — это наименьшее подмножество моноида F(K), для которого выполнены условия:

1) множество содержит константы $\varnothing, x_1, \ldots, x_m$;

2) множество вместе с α и β содержит $(\alpha+\beta)$, $(\alpha\cdot\beta)$ и $(\alpha)^*$.

2. Множество RG(X) *рациональных равенств над* X — это множество всех последовательностей символов вида $\alpha=\beta$, где α и β — рациональные выражения из множества RA(X).

Замечание. С позиций математической логики рациональные выражения суть термы, а рациональные равенства — формулы.

Утверждение. 1. RA(X) является (рекурсивным) подмножеством моноида F(K). Действительно, для любого слова w над K, т. е. для любой последовательности символов из K, за конечное число шагов можно установить, является ли это слово рациональ-

ным выражением. Это можно показать, как и в случае других определений данного типа, например, следующим образом.

Сначала проверяется, правильна ли скобочная структура выражения (предъявленного слова), т. е. проверяется, возникает ли после удаления из слова всех отличных от скобок символов слово из языка $DYCK_1'$ (см. по этому поводу доказательство п.2 теоремы 3.7.2 и п. 1 следствия 5.4.7). После этого, начиная с самых внутренних пар скобок, проверяется, стоит ли внутри данной пары скобок правильно построенное выражение (см. также нижеследующую лемму).

2. Множество $RG(X)$ является, конечно, вычислимым подмножеством моноида $F(K \cup \{=\})$ (см. п.1).

3. Если $X' \subseteq X$, то $RA(X') \subseteq RA(X)$ и $RG(X') \subseteq RG(X)$.

Чтобы иметь возможность определить семантику некоторого рационального выражения, т. е. найти представляемое этим выражением рациональное множество, мы должны действовать по аналогии с индуктивным определением понятия «рациональное выражение». Для этого нам нужно убедиться в том, что любое рациональное выражение не может быть построено различными способами и что таким образом не может возникнуть неоднозначность.

Лемма 5.7.2. Для каждого рационального выражения γ из $RA(X)$ имеет место в точности одна из следующих альтернатив:

1) $\gamma \equiv \varnothing$;
2) $\gamma \equiv x_i$ при однозначно определенном i из $\{1, \ldots, m\}$;
3) $\gamma \equiv (\alpha + \beta)$ при однозначно определенных α и β из $RA(X)$;
4) $\gamma \equiv (\alpha \cdot \beta)$ при однозначно определенных α и β из $RA(X)$;
5) $\gamma \equiv (\alpha)^*$ при однозначно определенном α из $RA(X)$.

Доказательство. По определению соотношение $\alpha \equiv \beta$ для выражений α и β из $RA(X)$ выполнено тогда и только тогда, когда они являются по сути дела одной и той же последовательностью символов.

Итак, если α — выражение длины 1, то оно должно быть равно либо $\varnothing$, либо x_i. Если же α имеет длину, не меньшую 3, то либо последним символом в α является $*$, и тогда $\alpha = (\beta)^*$ при некотором однозначно определенном β, либо α имеет вид 3) или 4).

Допустим, что $\alpha \equiv (\beta + \gamma)$ и, кроме того, существуют β' и γ' в $RA(X)$ такие, что $\alpha \equiv (\beta' + \gamma')$. Поскольку последовательности символов $(\beta + \gamma)$ и $(\beta' + \gamma')$ должны совпадать, то отсюда следует, что $\beta \equiv \beta'$ и $\gamma \equiv \gamma'$.

Дальнейшие рассуждения проводятся совершенно аналогично. ■

Замечание. Из леммы 5.7.2 вытекает также, что $RA(X)$ может рассматриваться как свободная алгебра с двуместными операциями $+$ и $\cdot$ и одноместной операцией $*$.

Встретившиеся в лемме 5.7.2 подвыражения при преобразованиях равенств будут ниже заменяться на другие выражения (ср. разд. 5.6). С этой целью введем одно соотношение между выражениями.

Определение 5.7.3. Пусть α и β — выражения из множества

RA(X). α называется *правильным подвыражением* β, если выполнено одно из следующих условий:

1) $\beta \equiv \alpha$ или $\beta \equiv (\alpha)^*$;

2) существует γ в RA(X) такое, что либо $\beta \equiv (\alpha+\gamma)$, либо $\beta \equiv (\gamma+\alpha)$, либо $\beta \equiv (\alpha\cdot\gamma)$, либо $\beta \equiv (\gamma\cdot\alpha)$;

3) существует γ в RA(X) такое, что α является правильным подвыражением γ, а γ является правильным подвыражением β.

Лемма 5.7.4. Вопрос о том, является ли одно рациональное выражение правильным подвыражением другого рационального выражения, разрешим.

Доказательство. Лемма 5.7.2 обосновывает рекурсивный метод разложения данного рационального выражения на подвыражения. Заметим, что для выражения γ из RA(X) можно эффективным образом установить, какую из форм 1)—5) оно имеет, и что каждое γ из RA(X) имеет конечную длину (состоит из конечного числа символов), так что может иметь только конечное число правильных подвыражений. ■

СЕМАНТИКА

Значение рационального выражения будет определено рекурсивным сопоставлением рациональным выражениям рациональных множеств. Поэтому сначала следует установить, что такое сопоставление может быть однозначным.

Поскольку рациональные выражения должны описывать все рациональные множества (для чего и введена эта конструкция), то понадобится и доказательство сюръективности соответствующего отображения.

Теорема 5.7.5. Приведенный набор равенств определяет отображение r из RA(X) на Rat(X):

$r(\varnothing) = \varnothing$;

$r(x_i) = \{x_i\}$ при $i = 1, \ldots, m$;

$r(\alpha+\beta) = r(\alpha) \cup r(\beta)$ при $\alpha, \beta \in RA(X)$;

$r(\alpha\cdot\beta) = r(\alpha)\, r(\beta)$ при $\alpha, \beta \in RA(X)$;

$r((\alpha)^*) = (r(\alpha))^*$ при $\alpha \in RA(X)$

Доказательство. 1. Нужно доказать, что рекурсивно определеное отображение r определено корректно и является отображением на Rat(X). Мы покажем это, используя лемму 5.7.2, индукцией «по правильным подвыражениям».

Пусть γ — выражение из RA(X). Тогда γ имеет один из приведенных в лемме 5.7.2 видов с однозначно определенными компонентами.

Если $\gamma \equiv \varnothing$ или $\gamma \equiv x_i$, то, очевидно, $r(\gamma)$ — однозначно определенное рациональное множество.

Если $\gamma \equiv (\alpha)^*$ с однозначно определенным α и $r(\alpha)$ — однозначно определенное рациональное множество, то и $r(\gamma)$ оказывается однозначно определенным рациональным множеством.

Если. наконец, $\gamma=(\alpha+\beta)$ или $\gamma=(\alpha\cdot\beta)$ с однозначно определенными α и β и $r(\alpha)$ и $r(\beta)$ — однозначно определенные рациональные множества, то и $r(\gamma)$ — однозначно определенное рациональное множество.

2. Множества $\varnothing=r(\varnothing)$ и $\{x_i\}=r(x_i)$ принадлежат $r(RA(X))$, а каждое рациональное множество по определению 5.3.3 может быть построено из этих множеств с помощью операции $\cup$, $\cdot$ и *. Отсюда следует, что r является сюръективным отображением. ▪

Замечания. 1. Отображение r оказывается гомоморфизмом из свободной алгебры $(RA(X); +, \cdot, ^*)$ на алгебру $(Rat(X); \cup, \cdot, ^*)$, часто называемую *алгеброй Клини.*

2. Могут рассматриваться, конечно, и гомоморфизмы алгебры $(RA(X); +, \cdot, ^*)$ в другие алгебры, например в множество подмножеств произвольного моноида (или группы) с операциями объединения, произведения и образования подмоноида (см. по этому поводу разд. 8.8).

Определение 5.7.6. 1. Определенное в теореме 5.7.5 отображение $r: RA(X)\to Rat(X)$ называется *стандартной семантикой рациональных выражений.* Для α из $RA(X)$ множество $r(\alpha)$ называется *представленным (определенным) α рациональным множеством.*

2. Рациональное равенство $\alpha=\beta$ называется **верным** (выполненным), если $r(\alpha)=r(\beta)$. В таком случае говорят, что *выражения α и β эквивалентны.*

Из теоремы 5.5.11 немедленно вытекает теорема.

Теорема 5.7.7. 1. Для произвольного НРС-автомата A и любого рационального выражения α разрешим вопрос о выполнении равенства $L(A)=r(\alpha)$.

2. Для произвольных рациональных выражений α и β разрешим вопрос о выполнении равенства $\alpha=\beta$.

Поскольку рациональные выражения и равенства имеют очень простую структуру и простую семантику, можно, не опасаясь неправильного понимания, использовать следующие обычные упрощения обозначений.

Соглашение об обозначениях. В рациональных выражениях опускаются:

внешние скобки, т. е. вместо $(\alpha+\beta)$ или $(\alpha\cdot\beta)$ пишется просто $\alpha+\beta$ и соответственно $\alpha\cdot\beta$;

скобки, оказывающиеся излишними при следующих соглашениях: знак $\cdot$ связывает сильнее, чем знак $+$; знак * связывает сильнее, чем $\cdot$, так что, например, вместо $(\alpha)^*$ можно писать α^* и вместо $(\alpha\cdot\beta)+(\gamma\cdot\beta)$ — $\alpha\cdot\beta+\gamma\cdot\beta$;

знак $\cdot$, т. е. вместо $\alpha\cdot\beta$ пишется $\alpha\beta$.

В сложных термах, например в $\alpha(\beta+\gamma)$ или в $(\alpha\beta)^*$, скобки, конечно, могут быть необходимы.

Из сказанного вытекает, что эквивалентность рациональных выражений может быть определена с помощью их семантики, т. е. с помощью построения автоматов, обладающих соответствующими реакциями. В разд. 5.6 мы, однако, уже установили, что из равенств над $Rat(X)$ можно получать новые равенства и что, таким

образом, вопрос о выполнении равенств может быть сведен к вопросу о выполнении простейших равенств. При этом было важным то обстоятельство, что уравнения вида $y=Ly+R$ могут быть решены и имеют единственные решения, если Λ не принадлежит L. Сейчас мы убедимся в том, что выполнение соответствующего условия для рациональных выражений может быть проверено чисто синтаксическим образом (без использования семантики).

Лемма 5.7.8. Пусть α — выражение из RA(X). Определим рекурсивно, что α обладает *свойством пустого слова* тогда и только тогда, когда выполнено одно из следующих условий:

1) существует β в RA(X) такое, что $\alpha\equiv\beta^*$;

2) существуют β и γ в RA(X) такие, что $\alpha=\beta+\gamma$ и β или γ обладает свойством пустого слова;

3) существуют β и γ в RA(X) такие, что $\alpha=\beta\gamma$ и β и γ обладают (оба!) свойством пустого слова.

Тогда для каждого рационального выражения однозначно определено, обладает ли оно свойством пустого слова, причем вопрос о наличии у данного рационального выражения этого свойства может быть решен за конечное число шагов.

Далее, α обладает свойством пустого слова тогда и только тогда, когда $\Lambda\in r(\alpha)$.

Доказательство. 1. Из доказательства леммы 5.7.2 вытекает, что для каждого рационального выражения эффективно может быть установлено, какой из видов 1)—5) оно имеет. Кроме того, возможен только один из случаев и соответствующие разложения определены однозначно. Таким образом, определение однозначно.

Наличие свойства пустого слова может быть проверено эффективно, поскольку каждое рациональное выражение за конечное число шагов может быть разложено на выражения вида x_i или $\varnothing$.

2. То, что α обладает свойством пустого слова тогда и только тогда, когда $\Lambda\in r(\alpha)$ доказывается индукцией «по правильным подвыражениям» с использованием леммы 5.7.2:

если $\alpha\equiv\varnothing$ или $\alpha=x_i$, то $\Lambda\notin r(\alpha)$ и α не обладает свойством пустого слова;

если $\alpha\equiv(\beta)^*$, то $\Lambda\in r(\beta^*)=(r(\beta))^*$;

если $\alpha\equiv\beta+\gamma$, то $\Lambda\in r(\alpha)$ тогда и только тогда, когда $\Lambda\in r(\beta)$ или $\Lambda\in r(\gamma)$;

если $\alpha\equiv\beta\gamma$, то $\Lambda\in r(\alpha)$ тогда и только тогда, когда $\Lambda\in r(\beta)$ и $\Lambda\in r(\gamma)$.

СИСТЕМА АКСИОМ ДЛЯ РАЦИОНАЛЬНЫХ РАВЕНСТВ

Для множества всех (истинных) рациональных равенств над X будут приведены множество аксиом и два правила вывода, позволяющие получить из аксиом все истинные рациональные равенства, т. е. все утверждения об эквивалентности рациональных выражений.

Говоря об аксиомах, мы говорим на самом деле о схемах аксиом, порождающих бесконечные семейства равенств. Эти равенства

могут быть получены при замене символов α, β и γ произвольными конкретными рациональными выражениями.

Определение 5.7.9. (Саломаа, Урпонен). *Система аксиом* $\mathrm{Ax}(X)$ *для рациональных равенств над* X состоит из:

1) следующих девяти аксиом, в которых α, β и γ обозначают произвольные рациональные выражения над X:

(a_1) $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$;

(a_2) $(\alpha\beta)\gamma=\alpha(\beta\gamma)$;

(a_3) $\alpha+\beta=\beta+\alpha$;

(a_4) $\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$;

(a_5) $(\alpha+\beta)\gamma=\alpha\gamma+\beta\gamma$;

(a_6) $\alpha\varnothing^*=\alpha$;

(a_7) $\alpha\varnothing=\varnothing$;

(a_8) $\alpha^*=\alpha\alpha^*+\varnothing^*$;

(a_9) $\alpha^*=(\alpha+\varnothing^*)^*$;

2) следующих двух правил вывода:

Правило замены (E). Пусть β_1 — правильное подвыражение рационального выражения α_1 и пусть α_2 — результат замены какого-либо вхождения β_1 в α_1 выражением β_2 из $\mathrm{RA}(X)$. Тогда из истинности равенств $\alpha_1=\gamma$ **и** $\beta_1=\beta_2$ вытекает истинность равенств $\alpha_2=\gamma$ и $\alpha_2=\alpha_1$.

Правило решения уравнений (G). Пусть α, β и γ — рациональные выражения из $\mathrm{RA}(X)$, причем β не обладает свойством пустого слова. Тогда из истинности равенства $\alpha=\beta\alpha+\gamma$ вытекает истинность равенства $\alpha=\beta^*\gamma$.

Замечание. Леммы 5.7.4 и 5.7.8 обеспечивают эффективность применения правил E и G, поскольку условия их применимости могут быть эффективно проверены в каждом случае, причем чисто синтаксическими методами.

Теорема 5.7.10. Система аксиом $\mathrm{Ax}(X)$ совместна, т. е. аксиомы (a_1) — (a_9) являются истинными рациональными равенствами и с помощью правил E и G из истинных рациональных равенств могут быть получены только истинные рациональные равенства.

Доказательство. 1. Истинность аксиом вытекает непосредственно из теоремы 5.6.1.

2. Правило E.

а) Пусть β_1 — правильное подвыражение выражения α_1 в смысле условия 1) или 2) определения 5.7.3, скажем, $\alpha_1\equiv\beta_1{}^*$, $\alpha_1\equiv\beta_1\delta$ или $\alpha_1\equiv\beta_1+\delta'$.

Тогда $\alpha_2\equiv\beta_2{}^*$, $\alpha_2\equiv\beta_2\delta$ или $\alpha_2\equiv\beta_2+\delta'$.

Из $r(\alpha_1)=r(\gamma)$ и $r(\beta_1)=r(\beta_2)$ в этом случае вытекает, что $r(\alpha_2)=(r(\beta_2))^*=(r(\beta_1))^*=r(\alpha_1)$, или $r(\alpha_2)=r(\beta_2)r(\delta)=r(\beta_1)r(\delta)=r(\alpha_1)$, или $r(\alpha_2)=r(\beta_2)\cup r(\delta')=r(\beta_1)\cup r(\delta')=r(\alpha_1)$.

Остальные случаи могут быть разобраны аналогично.

б) Пусть теперь β_1 — правильное подвыражение выражения α_1 в смысле условия 3) определения 5.7.3, т. е. пусть существует правильное подвыражение η_1 выражения α_1 такое, что β_1 является правильным подвыражением выражения η_1 в смысле условия 1) или 2) определения 5.7.3. Тогда, как и в случае а), для выражения η_2, получаемого в результате замены β_1 на β_2, выполняется равенство $r(\eta_1)=r(\eta_2)$, т. е. равенство $\eta_1=\eta_2$.

Итак, утверждение может быть доказано методом полной индукции, поскольку если β_1 — правильное подвыражение выражения α_1, то существует последовательность $\beta_1=\delta_0, \delta_1, \ldots, \delta_k=\alpha_1$ рациональных выражений такая, что δ_i — правильное подвыражение δ_{i+1} в смысле условия 1) или 2) определения 5.7.3 при $i=0, 1, \ldots, k-1$.

3. Правило G. Если β не обладает свойством пустого слова, то уравнение $y=r(\beta)y+r(\gamma)$ по следствию 5.6.8 и лемме 5.7.8 имеет единственное решение $y=(r(\beta))^*r(\gamma)$.

Итак, если $r(\alpha)=r(\beta)r(\alpha)+r(\gamma)$, то выполнено и равенство $r(\alpha)=(r(\beta))^*r(\gamma)$, так что вместе с $\alpha=\beta\alpha+\gamma$ истинно и равенство $\alpha=\beta^*\gamma$. ∎

Системой аксиом определяется формальное исчисление, в рамках которого чисто синтаксическими преобразованиями (т. е. применением правил E и G) на базе аксиом может быть доказана истиннность всех (истинных) рациональных равенств.

Определение 5.7.11. *Доказательством* рационального равенства $\alpha=\beta$ в системе аксиом Ax(X) называется конечная оканчивающаяся равенством $\alpha=\beta$ последовательность рациональных равенств такая, что каждое из входящих в нее равенств либо является результатом замены в одной из аксиом символов α, β и γ на определенные рациональные выражения (или символы, обозначающие такие выражения), либо возникает в результате применения одного из правил вывода E или G к предыдущим равенствам последовательности.

Если для равенства $\alpha=\beta$ существует доказательство в системе аксиом Ax(X), то оно называется *выводимым* в Ax(X), что обозначается так: $\vdash \alpha=\beta$.

Говорят, далее, что равенство $\alpha=\beta$ *выводимо в системе аксиом* Ax(X) *из множества равенств* M, если оно выводимо из системы аксиом, возникающей при присоединении к Ax(X) в качестве дополнительных аксиом равенств из M.

Из теоремы 5.7.10 немедленно вытекает следствие.

Следствие 5.7.12. Каждое выводимое в Ax(X) равенство истинно.

Теорема 5.7.13. (Саломаа, Урпонен). Система аксиом Ax(X) полна, т. е. каждое истинное рациональное равенство выводимо в Ax(X). Далее, множество всех истинных рациональных равенств перечислимо, т. е. может быть предложен эффективный метод, с помощью которого можно получить все истинные рациональные равенства и только их.

Аксиомы (a_1) — (a_9) и правила вывода E и G взаимно неза-

висимы, т. е. если из системы аксиом удалить одну из аксиом или одно из правил вывода, то в рамках оставшейся системы аксиом уже не каждое выводимое в Ax(X) равенство будет выводимым.

Доказательство этой теоремы, занимающее очень много места, мы не приводим (см. по этому поводу упражнение 5.20 и литературу к этой главе).

ДОКАЗАТЕЛЬСТВА В СИСТЕМЕ АКСИОМ

В качестве примеров доказательств в Ax(X) докажем теперь некоторые простые, но очень нужные для дальнейшего равенства — прежде всего, без использования правила G.

Лемма 5.7.14. Пусть α, β, δ и η — рациональные выражения. Тогда:

1) $\vdash \alpha=\alpha$;

2) из $\vdash \alpha=\beta$ следует $\vdash \beta=\alpha$;

3) из $\vdash \alpha=\beta$ и $\vdash \beta=\delta$ следует $\vdash \alpha=\delta$;

4) из $\vdash \alpha=\delta$ и $\vdash \beta=\eta$ следует $\vdash \alpha+\beta=\delta+\eta$, $\vdash \alpha\beta=\delta\eta$ и $\vdash \alpha^*=\delta^*$.

Доказательство. 1. Из аксиомы (a_6) имеем $\vdash a\varnothing^*=\alpha$. В правиле вывода E положим $\alpha_1\equiv\beta_1\equiv\alpha\varnothing^*$ и $\beta_2\equiv\gamma\equiv\alpha$. Тогда $\alpha_2\equiv\alpha$, а на основании аксиомы (a_6) имеем $\vdash \alpha_1=\gamma$ и $\vdash \beta_1=\beta_2$. Используя E, теперь получаем $\vdash \alpha_2=\gamma$, т. е. $\vdash \alpha=\alpha$.

2. В правиле E положим $\alpha_1\equiv\beta_1\equiv\alpha$ и $\beta_2\equiv\beta$. Тогда $\alpha_2\equiv\beta$. Если $\vdash \alpha=\beta$, то $\vdash \beta_1=\beta_2$, и из E следует, что $\vdash \alpha_2=\alpha_1$, т. е. $\vdash \beta=\alpha$.

3. Из $\vdash \alpha=\beta$ в силу п. 2 следует $\vdash \beta=\alpha$. Пусть $\vdash \beta=\delta$. В правиле E положим $\alpha_1\equiv\beta_1\equiv\beta$, $\beta_2\equiv\alpha$ и $\gamma\equiv\delta$. Тогда $\alpha_2\equiv\alpha$, $\vdash \beta_1=\beta_2$ и $\vdash \alpha_1=\gamma$, и из E следует, что $\vdash \alpha_2=\gamma$, т. е. $\vdash \alpha=\delta$.

4. Из $\vdash \alpha=\delta$ и $\vdash \beta=\eta$ на основании п. 2 следует, что $\vdash \delta=\alpha$ и $\vdash \eta=\beta$.

В правиле E положим сначала $\alpha_1\equiv\delta+\eta$, $\beta_1\equiv\delta$ и $\beta_2=\alpha$. Тогда $\alpha_2\equiv\alpha+\eta$ и $\vdash \beta_1=\beta_2$, и можно заключить, что $\vdash \alpha_2=\alpha_1$, т. е. $\vdash \alpha+\eta=\delta+\eta$.

Выберем теперь в E $\alpha_1\equiv\alpha+\eta$, $\beta_1\equiv\eta$, $\beta_2\equiv\beta$ и $\gamma\equiv\delta+\eta$. Тогда $\alpha_2\equiv\alpha+\beta$, $\vdash \beta_1=\beta_2$ и $\vdash \alpha_1=\gamma$. Применяя правило E, имеем $\vdash \alpha_2=\gamma$, т. е. $\vdash \alpha+\beta=\delta+\eta$.

Доказательство $\vdash \alpha\beta=\delta\eta$ проводится аналогично.

Выбирая, наконец, в E $\alpha_1\equiv\delta^*$, $\beta_1\equiv\delta$ и $\beta_2\equiv\alpha$, так что $\alpha_2\equiv\alpha^*$ и $\vdash \beta_1=\beta_2$, из E получаем $\vdash \alpha_2=\alpha_1$, т. е. $\vdash \alpha^*=\delta^*$. ■

Замечание. Лемма 5.7.14 утверждает, что для знака «=» в случае рациональных равенств в Ax(X) выводимы все обычные свойства знака равенства. Иначе говоря, в лемме 5.7.14 доказано, что отношение эквивалентности рациональных выражений представляют собой конгруэнцию в алгебре $(RA(X); +, \cdot, ^*)$, в точ-

ности совпадающую с конгруэнцией, индуцированной гомоморфизмом r.

Теперь мы докажем выводимость рациональных равенств, соответствующих равенствам (6)—(9) теоремы 5.6.1. При этом будем использовать результаты леммы 5.7.14 без ссылок и запись «$\vdash \alpha=\beta=\gamma$» вместо «$\vdash \alpha=\beta$ и $\vdash \beta=\gamma$». Кроме того, из-за ассоциативности операций $+$ и $\cdot$ [аксиомы (a_1) и (a_2)] будем опускать лишние скобки.

Теорема 5.7.15 (Урпонен). Пусть α — рациональное выражение из RA(X). Тогда:

1) $\vdash \alpha+\varnothing=\alpha$;

2) $\vdash \alpha+\alpha=\alpha$;

3) $\vdash \varnothing\alpha=\varnothing$;

4) $\vdash \varnothing^*\alpha=\alpha$.

Доказательство. Полагая в (a_8) и (a_6) $\alpha\equiv\varnothing$, получаем

$\vdash \varnothing^*=\varnothing\varnothing^*+\varnothing^*=\varnothing+\varnothing^*$.

Используя теперь (a_9) при $\alpha\equiv\varnothing$, имеем

$\vdash \varnothing^*=(\varnothing+\varnothing^*)^*=(\varnothing^*)^*$.

С помощью (a_8) при $\alpha\equiv\varnothing^*$ отсюда находим

$\vdash (\varnothing^*)^*=\varnothing^*(\varnothing^*)^*+\varnothing^*$.

Последние равенства вместе с (a_6) при $\alpha\equiv\varnothing^*$ дают

$\vdash \varnothing^*=\varnothing^*+\varnothing^*$.

Первое и последнее равенства и аксиома (a_6) порождают

$\vdash \alpha=\alpha\varnothing^*=\alpha(\varnothing+\varnothing^*)$ и $\vdash \alpha=\alpha\varnothing^*=\alpha(\varnothing^*+\varnothing^*)$.

Из сказанного с помощью аксиом (a_4), (a_6), (a_7) и (a_3) теперь получаем

$\vdash \alpha=\alpha\varnothing+\alpha\varnothing^*=\varnothing+\alpha=\alpha+\varnothing$ и

$\vdash \alpha=\alpha\varnothing^*+\alpha\varnothing^*=\alpha+\alpha$.

Итак, пп. 1) и 2) доказаны.
Из (a_7) и (a_2) следует, что

$\vdash \varnothing=\varnothing\varnothing$, так что $\vdash \varnothing\alpha=(\varnothing\varnothing)\alpha=\varnothing(\varnothing\alpha)$.

Заменяя в 1) α на $\varnothing\alpha$, получаем

$\vdash \varnothing\alpha=\varnothing(\varnothing\alpha)+\varnothing$.

Поскольку $\varnothing$ не обладает свойством пустого слова, то применение правила G дает

$\vdash \varnothing\alpha=\varnothing^*\varnothing$.

Из аксиомы (a_7) и последнего равенства следует п.3). Из пп. 3), 1) и аксиомы (a_3) следует

$\vdash \alpha = \varnothing\alpha + \alpha$, так что, используя G, получаем п.4). ■

Замечание. В системах аксиом, приводимых обычно в учебниках, равенства 1) и 2) теоремы 5.7.15 рассматривают как аксиомы и вместо (a_6) и (a_7) используют в качестве аксиом равенства 3) и 4) этой же теоремы. Кроме того, в (a_8) и в правиле вывода G меняют местами сомножители в произведениях (см. по этому поводу п. 4 упражнения 5.20). При использовании системы аксиом для определения реакции НРС-автомата необходима, однако, форма аксиом, приведенная в определении 5.7.9.

Для того чтобы иметь возможность применять, хотя бы в некотором измененном виде, правило решения уравнений (G) также и в случаях, когда наличествует свойство пустого слова, нам понадобится следующая лемма.

Лемма 5.7.16. Для каждого α из RA(X), обладающего свойством пустого слова, существует в RA(X) выражение α_1, не обладающее свойством пустого слова и такое, что $\vdash \alpha = \alpha_1 + \varnothing^*$.

Доказательство. Проведем доказательство полной индукцией по длине выражения α. Если $\alpha \equiv \varnothing^*$, то выберем $\alpha_1 \equiv \varnothing$. Тогда по теореме 5.7.15, п.1) $\vdash \alpha = \alpha_1 + \varnothing^*$.

Если же неверно, что $\alpha \equiv \varnothing^*$, то по лемме 5.7.8 α должно иметь один из следующих видов: $\alpha \equiv \beta^*$, $\alpha \equiv \gamma + \gamma'$ или $\alpha \equiv \delta\eta$.

Рассмотрим сначала третий случай. Поскольку δ и η короче, чем α, то можно предположить, что существуют δ_1 и η_1 в RA(X) такие, что $\vdash \delta = \delta_1 + \varnothing^*$, $\vdash \eta = \eta_1 + \varnothing^*$, но δ_1 и η_1 не обладают свойством пустого слова. Тогда $\vdash \alpha = \delta\eta = (\delta_1 + \varnothing^*)(\eta_1 + \varnothing^*) = \delta_1\eta_1 + \delta_1 + \eta_1 + \varnothing^*$. При $\alpha_1 \equiv \delta_1\eta_1 + \delta_1 + \eta_1$ получаем требуемое утверждение.

Случай $\alpha \equiv \gamma + \gamma'$ разбирается аналогично.

Пусть теперь $\alpha = \beta^*$. Если β не обладает свойством пустого слова, то при $\alpha_1 = \beta\beta^*$ из аксиомы (a_8) вытекает утверждение $\vdash \alpha_1 + \varnothing^*$, поскольку, в этом случае и $\beta\beta^*$ не обладает свойством пустого слова.

Если же β обладает свойством пустого слова, то по предположению индукции можно считать, что существует не обладающее свойством пустого слова выражение β_1 такое, что $\vdash \beta = \beta_1 + \varnothing^*$.

Из аксиом (a_9) и (a_8) в этом случае получаем $\vdash \alpha = \beta^* = (\beta_1 + \varnothing^*)^* = \beta_1^* = \beta_1\beta_1^* + \varnothing^*$, так что при $\alpha_1 = \beta_1\beta_1^*$ доказываемое утверждение выполнено. ■

Докажем, наконец, чтобы продемонстрировать возможность применения леммы 5.7.16, рациональные равенства, соответствующие равенствам (12), (13) и (16) теоремы 5.6.1. При этом результаты теоремы 5.7.15 и аксиомы (a_1) — (a_7) будут использоваться без дальнейших ссылок.

Лемма 5.7.17. Пусть α и β — выражения из RA(X). Тогда:

1) $\vdash (\alpha+\beta)^*=\beta^*(\alpha\beta^*)^*$;

2) $\vdash \alpha^*\alpha^*=\alpha^*$;

3) $\vdash (\alpha^*)^*=\alpha^*$. ■

Доказательство. 1) Предположим сначала, что ни α, ни β не обладают свойством пустого слова. Пусть тогда $\gamma=\beta^*(\alpha\beta^*)^*$. Из аксиомы (a_8) вытекает, что

$$\vdash \gamma=(\alpha\beta^*)^*+\beta\beta^*(\alpha\beta^*)^*=\alpha\beta^*(\alpha\beta^*)^*+\beta\beta^*(\alpha\beta^*)^*+\varnothing^*=$$

$$=(\alpha+\beta)\gamma+\varnothing^*.$$

Используя правило G, получаем $\vdash \gamma=(\alpha+\beta)^*$.

Если же α и β обладают (оба) свойством пустого слова, то по лемме 5.7.16 существуют не обладающие свойством пустого слова выражения α_1 и β_1 такие, что

$$\vdash \alpha=\alpha_1+\varnothing^* \text{ и } \vdash \beta=\beta_1+\varnothing^*.$$

Для определенного выше выражения γ, используя аксиомы (a_9) и (a_8), имеем

$$\vdash \gamma=\beta_1^*((\alpha_1+\varnothing^*)\beta_1^*)^*=\beta_1^*(\alpha_1\beta_1^*+\beta_1\beta_1^*)^*=$$

$$=\beta_1^*((\alpha_1+\beta_1)\beta_1^*)^*.$$

При β_1 вместо β и $(\alpha_1+\beta_1)$ вместо α из сказанного и из аксиомы (a_9) получаем

$$\vdash \gamma=(\alpha_1+\beta_1+\beta_1)^*=(\alpha+\beta)^*.$$

Случаи, когда либо только α, либо только β не обладают свойством пустого слова, разбираются аналогично.

2) Из аксиомы (a_8) следует

$$\vdash \alpha^*=\varnothing+\alpha\alpha^*+\alpha\alpha^*=\alpha^*+\alpha\alpha^*.$$

Если α не обладает свойством пустого слова, то применение правила G дает

$$\vdash \alpha^*=\alpha^*\alpha^*.$$

Если же α обладает свойством пустого слова, то по лемме 5.7.16 существует не обладающее свойством пустого слова выражение α_1 такое, что $\vdash \alpha=\alpha_1+\varnothing^*$. Используя (a_9), в этом случае имеем

$$\vdash \alpha^*=(\alpha_1+\varnothing^*)^*=\alpha_1^*=\alpha_1^*+\alpha_1\alpha_1^*.$$

Применение правила G теперь дает

$$\vdash \alpha^*=\alpha_1^*=\alpha_1^*\alpha_1^*=\alpha^*\alpha^*.$$

3) Из п. 1) и аксиом (a_8) и (a_9) следует

$$\vdash \alpha^*=\alpha\alpha^*+\varnothing^*+\varnothing^*=\varnothing^*+\alpha^*=\varnothing^*+(\varnothing^*+\alpha)^*=$$
$$=\varnothing^*+\alpha^*(\varnothing^*\alpha^*)^*=\alpha^*(\alpha^*)^*+\varnothing^*=(\alpha^*)^*.\blacksquare$$

Аналогичным образом могут быть доказаны все рациональные равенства, соответствующие равенствам теоремы 5.6.1 (см. упражнение 5.20, п.1].

УПРАЖНЕНИЯ

5.1. Порядок выдачи книг в некоторой библиотеке, содержащей N томов, допускает выдачу одному абоненту не более n книг (где $n<N$). Некий пользователь библиотеки (скажем, снова студент, готовящий дипломную работу), которому в течение короткого времени нужно иметь много книг, будет пытаться уменьшить затраты труда на сдачу и получение книг и время на размышления о том, какую именно книгу сдать, если он уже взял из библиотеки n книг и ему нужна новая книга. Если этот пользователь немного знаком с теорией операционных систем, то он будет использовать исследуемый в этой теории алгоритм, по которому сдается книга, которая не была нужна в течение наиболее длительного срока.

Представьте данный алгоритм в виде автомата, выбрав в качестве входного алфавита множество номеров томов {1, 2, ..., N}, в качестве множества состояний — множество упорядоченных последовательностей номеров имеющихся у пользователя томов (упорядоченных по времени последнего использования). Решите вопрос о том, каким образом при постоянном N автомат для $n=k+1$ может быть получен из автомата для $n=k$.

5.2.* Предложите по возможности быстрый метод определения моноида переходов алфавитного НРС-автомата. Какова максимальная длина входных слов, используемых в этом методе?

5.3. Задайте НРС-автоматы, допускающие следующие множества.

1. $\{\Lambda, 1\}$. Покажите, что НРС-автомат без спонтанных переходов, допускающий это множество, должен иметь либо больше начальных, либо больше финальных состояний.

2. Множество всех слов над {0, 1}, в которых единицы встречаются только блоками четной длины, а число таких блоков единиц нечетно (например, 11011110011 — слово из этого множества, а 011011 и 10101 — нет).

3. Множество всех слов нечетной длины над {0, 1}, в которых встречаются и символ 0, и символ 1, но не встречается подслово 01.

4. Множество всех кратных числу 3 натуральных чисел в десятичной записи (без дополнительных нулей, читаемых слева направо).

5.4. 1. Представьте в виде рациональных множеств множества из упражнения 5.3 и следующие множества из $\mathscr{P}(F(\{0, 1\}))$:

1) множество всех слов, содержащих как четное число единиц, так и четное число нулей;

2) множество всех слов, не содержащих в качестве подслова слово 010, т. е не имеющих вида u010v;

3) множество всех слов из множества, указанного в п. 1) [или в п. 2)], не принадлежащих данному конечному множеству E, например множеству $E=\{0011, 0, 1, 11, 10\}$;

4) множество всех слов из множества, указанного в п.1), не принадлежащих множеству из п.2).

2. Обозначим символом Rat множество всех рациональных подмножеств всех конечно порожденных свободных моноидов, так что $U \in \mathrm{Rat}$ тогда и только тогда, когда существует конечное множество X такое, что $U \in \mathrm{Rat}(X)$. Докажите, что множество Rat эффективно замкнуто относительно рациональных операций.

5.5. Докажите (для $U, V \subseteq F(X)$) следующее:

1) $\varnothing^* = \{\Lambda\}$;
2) $\Lambda \in UV$ тогда и только тогда, когда $\Lambda \in U \cap V$;
3) $\Lambda \in U^+ (= UU^*)$ тогда и только тогда, когда $\Lambda \in U$;
4) $UU^* = U^*U$;
5) $U^* = (\varnothing^* \cup U)^*$;
6) $(U^*)^* = U^*$;
7) $U^*U^* = U^*$;
8) $(UV)^*U = U(VU)^*$;
9) $U^m (U^n)^* = (U^n)^* U^m$ при $m, n \in \mathbf{N}$;
10) $U^* = (\varnothing^* \cup U \cup \ldots \cup U^{n-1})(U^n)^*$ при $n \in \mathbf{N}$.

5.6. 1. Методом из доказательства теоремы 5.3.5 постройте НРС-автомат, реакция которого — множество L_D из примера 5.3.6. Преобразуйте этот автомат с помощью сохраняющих реакцию преобразований в НРС-автомат, граф которого изображен на рис. 5.3.1. Постройте, далее, НРС-автоматы, допускающие множества 1)—4) из примера 5.4, п.1.

2. Преобразуйте конструкцию в п.б) доказательства теоремы 5.3.5 таким образом, чтобы не были нужны спонтанные переходы, т е. вместо введенных при построении автомата A_4 спонтанных переходов (z, Λ, z') для каждого слова w, для которого $t_2(z', w) \neq \varnothing$, добавьте все переходы (z, w, z''), где $z'' \in t_2(z', w)$ и $z \in F_1$. Аналогично преобразуйте и автомат A_5.

3. (Бар — Хиллел, Перлес, Шамир.) Отображение σ из $F(X)$ в $\mathscr{P}(F(X))$ называется рациональной подстановкой, если оно обладает следующими свойствами:

1) $\sigma(\Lambda) = \{\Lambda\}$;
2) $\sigma(uv) = \sigma(u)\sigma(v)$ для всех $u, v \in F(X)$;
3) $\sigma(x) \in \mathrm{Rat}(X)$ для всех $x \in X$.

Очевидно, каждый гомоморфизм h из $F(X)$ в $F(X)$ можно рассматривать как рациональную подстановку h': полагаем $h'(u) = \{v\}$, если $h(u) = v$.

Докажите, что для каждой рациональной подстановки σ: $F(X) \to \mathscr{P}(F(X))$;

а) каждое множество $\sigma(w)$ при w из $F(X)$ является рациональным множеством;

б) если определить для $U \subseteq F(X)$ образ при отображении σ как $\sigma(U) = \bigcup \{\sigma(w) \mid w \in U\}$, то $\sigma(U)$ — рациональное множество при каждом рациональном множестве U, причем НРС-автомат с реакцией $\sigma(U)$ может быть построен непосредственно из автомата, имеющего реакцию U. [Указание. Выберите алфавитный НРС-автомат с реакцией U и замените в его графе каждое ребро с меткой $x \in X$ на граф допускающего $\sigma(x)$ НРС-автомата.] Таким образом, множество Rat(X) эффективно замкнуто относительно рациональных подстановок (а также относительно гомоморфизмов).

5.7. 1 *. (Макнотон, Ямада.) Предложите метод, с помощью которого для любого НРС-автомата A можно получить представление L(A) в виде рациональ-

ного множества, не используя при этом доказательство теоремы 5.3.7. [Указание. Пусть $Z=\{z_1, z_2, \ldots, z_n\}$ и W_{ij}^k — множество слов из $F(X)$, переводящих автомат A из состояния z_i в состояние z_j, причем так, что автомат не принимает «по пути» ни одно из состояний $z_{k+1}, z_{k+2}, \ldots, z_n$ (конечно, i и j — произвольные числа из $\{1, \ldots, n\}$). Докажите рекуррентную формулу

$$W_{ij}^k = W_{ij}^{k-1} \cup W_{ik}^{k-1}(W_{kk}^{k-1})^* W_{kj}^{k-1}$$

и выведите отсюда, что каждое из множеств W_{ij}^k рационально.]

2. Примените методы из п.1 и из доказательства теоремы 5.3.7 к НРС-автоматам из примеров 5.1.2—5.1.4 и 5.3.6.

3. (Эйленберг, Шютценбергер.) Множество $ERat(X)$ однозначных рациональных подмножеств моноида $F(X)$ есть наименьшее подмножество $\mathscr{R}$ булеана $\mathscr{P}(F(X))$ со следующими свойствами:

а) $\varnothing \in \mathscr{R}$ и $\{x\} \in \mathscr{R}$ для любого $x \in X$;

б) если $U, V \in \mathscr{R}$ и $U \cap V = \varnothing$, то $U \cup V \in \mathscr{R}$;

в) если $U, V \in \mathscr{R}$ и произведение UV однозначно (т. е. из $uv = u'v'$ при $u, u' \in U$ и $v, v' \in V$ вытекает, что $u = u'$ и $v = v'$), то $UV \in \mathscr{R}$;

г) если $U \in \mathscr{R}$ и $U^* = F(U)$ (т. е. если каждое произведение $U^i U$ однозначно при $i = 1, 2, \ldots$, иначе говоря, если каждое слово $w \in u^*$ обладает единственным разложением на множители из U), то $U^* \in \mathscr{R}$.

Докажите, что $ERat(X) = Rat(X)$. [Указание. Проанализируйте применение метода из п.1) к РС-автоматам.]

5.8. Пусть $X = \{0, 1\}$.

1. Пусть $M_1 = \{e, a, b\}$ — моноид с единичным элементом e, умножение в котором определяется равенствами $a = a^2 = ba$ и $b = b^2 = ab$. Пусть, далее, h — гомоморфизм из $F(X)$ на M_1, определяемый равенствами $h(0) = a$ и $h(1) = b$. Покажите, что $h^{-1}(a)$ — (различимое) множество всех слов из $F(X)$, оканчивающихся символом 0 Покажите далее, что M_1 является даже синтаксическим моноидом данного множества.

2. Пусть $M_2 = \{e, a, b, c\}$ — моноид с единичным элементом e и умножением, определяемым равенствами $a^2 = a$, $ab = b$, $ba = b^2 = c^2 = ca = ac = cb = bc = c$. Определите гомоморфизм h из $F(X)$ на M_2, для которого $h^{-1}(b) = 0^*1$, и докажите, что M_2 — синтаксический моноид множества 0^*1. Найдите, далее, $h^{-1}(a)$ и $h^{-1}(c)$ и синтаксический моноид для множества $h^{-1}(b) \cup h^{-1}(c)$.

3. (Шютценбергер.) Пусть $\mathbf{Z}$ аддитивная группа целых чисел и h — гомоморфизм из $F(X)$, на $\mathbf{Z}$, определяемый равенствами $h(0) = -1$ и $h(1) = 1$. Докажите, что:

1) $h^{-1}(0) = \{w \in F(X) \mid w$ содержит столько же единиц, сколько нулей$\}$;

2) отношение R на $F(X)$, определяемое условием «uRv тогда и только тогда, когда $h(u) = h(v)$», является синтаксической конгруэнцией по $h^{-1}(0)$ в смысле п.4 леммы 5.4.3;

3) $h^{-1}(0)$ не является допустимым множеством.

Задайте, далее, моноид M_1 и гомоморфизм h_1 из $F(\{a, b\})$ на M_1 такие, что $h_1^{-1}(e) = DYCK'_1$ (см. следствие 5.4.7).

[Замечание. $h^{-1}(0)$ называется языком Дика над одной парой скобок.]

5.9. Покажите, что следующие множества различимы.

1. Локально тестируемые множества (lokal testbare Mengen) [34]. Для того чтобы определить эти множества, нам понадобятся следующие обозначения. Для $k \in \mathbf{N}$ и $w \in F(X)$ таких, что $w = w'v$ и $|w'| = k$, пусть $\alpha_k(w) = w'$ (термин: k-префикс слова w) и $I_k(w) = \{u \in X^k \mid$ существуют $u', v' \in F(X)$ такие, что $w =$

$=u'uv'\}$ (термин: множество всех внутренних сегментов длины k). Пусть, далее, $\eta_k(w)$ — k-суффикс слова w (см. определение 2.6.6). Два слова w и w′ называются k-локально эквивалентными (обозначение: $w\sim_k w'$) только и только тогда, когда выполнены условия:

если $|w|<k$ или $|w'|<k$, то $w=w'$;

если $|w|\geqslant k$ и $|w'|\geqslant k$, то $\alpha_k(w)=\alpha_k(w')$, $I_k(w)=I_k(w')$ и $\eta_k(w)=\eta_k(w')$.

Подмножество L моноида F(X) называется локально тестируемым, если существует натуральное число k такое, что L оказывается объединением некоторых классов k-локальной эквивалентности. [Указание. Покажите, что отношение $\sim_k$ является конгруэнцией конечного индекса.]

2. Кусочно тестируемые множества (stückweise testbare Mengen) (Симон). Для того чтобы определить эти множества, нам понадобятся следующие обозначения. Слово u называется кусочным подсловом слова w (обозначение: $u\leqslant w$), если существуют слова $u_1, \ldots, u_n, w_0, w_1, \ldots, w_n$ такие, что $u=u_1u_2\ldots u_n$ и $w=w_0u_1w_1\ldots u_nw_n$. Пусть $k\in\mathbf{N}$. Два слова w и w′ из F(X) называются k-кусочно-эквивалентными (обозначение: $w\approx_k w'$), если и только если выполнено условие: для любого u из F(X), при $|u|\leqslant k$ соотношение $u\leqslant w$ выполняется тогда и только тогда, когда $u\leqslant w'$.

Подмножество L моноида F(X) называется кусочно-тестируемым, если существует натуральное число k такое, что L оказывается объединением некоторых классов эквивалентности по отношению $\approx_k$. [Указание. Покажите, что отношение $\approx_k$ является конгруэнцией конечного индекса.]

5.10. (Дитрих, Дешамп.) Пусть X — конечное множество; $r: F(X)\to F(X)$ — отображение, определенное следующим образом: $r(\Lambda)=\Lambda$, $r(x)=x$ при $x\in X$ и

$$r(ux)=\begin{cases} r(u), & \text{если } \eta_1(u)=x,\\ r(u)x & \text{в противном случае}\end{cases}$$

для всех u из $F^+(X)$ и x из X.

Здесь $\eta_1(u)$ — последний символ слова u (см. определение 2.6.6). Пусть R — отношение на F(X):

uRv тогда и только тогда, когда $r(u)=r(v)$.

Покажите, что R — конгруэнция на F(X). (Почему R не является конгруэнцией конечного индекса?)

Подмножество L моноида F(X) называется асинхронным языком, если оно стабильно относительно R (т. е. является объединением классов конгруэнтных относительно R слов). Приведите пример асинхронного языка, не являющегося допустимым множеством.

Для произвольного множества $L\subseteq F(X)$ пусть J(L) — пересечение всех содержащих L асинхронных языков из $\mathscr{P}(F(X))$.

Покажите, что если $L\in Rat(X)$, то и $J(L)\in Rat(X)$. [Указание. Найдите $J(\varnothing)$, $J(\Lambda)$ и $J(x)$ для $x\in X$ и покажите, что отображение J совместно с рациональными операциями.]

РС-автомат A называется асинхронным, если для любого его состояния z выполнено условие: если при некотором z′ из Z и некотором x из X выполняется равенство $f(z', x)=z$, то $f(z, x)=z$.

Покажите, что L допускается некоторым асинхронным РС-автоматом тогда и только тогда, когда $L=J(L)$.

5.11. Покажите, что для каждого конечного моноида M существует РС-автомат A, моноид переходов которого изоморфен M. [Указание. Просмотрите доказательство теоремы 5 4.4.]

5.12. Покажите, что не каждый конечный моноид является синтаксическим моноидом некоторого различимого множества, т. е. что не каждая конгруэнция конечного индекса на $F(X)$ является синтаксической конгруэнцией некоторого различимого подмножества $F(X)$. [Указание. Используйте часть доказательства леммы 5.4.3, в которой показано, что из п.3 вытекает п.4, и рассмотрите моноид $M_3=\{1, m_1, m_2, m_3\}$ с $m_i \cdot m_j = m_j$ при $1 \leqslant i, j \leqslant 3$ и единичным элементом 1. Проверьте, может ли подмоноид $M_2=\{1, m_1, m_2\}$ моноида M_3 быть синтаксическим моноидом — см. упражнение 5.8.]

5.13. Пусть $U \in Erk(X)$ и M_U — синтаксический моноид U (моноид классов эквивалентности относительно синтаксической конгруэнции по U — см. доказательство леммы 5.4.3). Покажите, что:

1) если h — гомоморфизм из $F(X)$ на конечный моноид M такой, что $h^{-1}(h(U))=U$, то существует гомоморфизм из M на M_U;

2) если A — алфавитный HPC-автомат с $L(A)=U$, то существует гомоморфизм из $T(A)$ на M_U;

3) если Y — конечное множество и h — гомоморфизм из $F(Y)$ на $F(X)$, то $h^{-1}(U) \in Erk(Y)$.

5.14. (Гинзбург.) Пусть A — частичный автомат Мили в обычных обозначениях. Покажите, что для всех z и z′ из Z и всех y из Y допустимы множества

$$W(A, z, y, z')=\{w \in F(X) \mid \widehat{g_z}(w)=y,\ f^*(z, w)=z'\},$$

$W(A, z, z', y)=\{w \in F(X) \mid$ существуют $u \in F(X)$ и $x \in X$, такие, что $w=ux$, $f^*(z, u)=z'$ и $g(z', x)=y\}$. [Указание. Доопределите автомат A и постройте равносильный автомат Мура.]

5.15. 1. С помощью uvw-теоремы или теоремы об итеративном подслове докажите следствие 5.4.7.

2. Покажите, что следующие множества не принадлежат $Rat(X)$:

$\{w\widetilde{w} \mid w \in F(X)\}$ при $|X| \geqslant 2$;

$\{ucv \mid u, v \in F(X'), u \neq v\}$ при $X=X' \cup \{c\}$, $|X'| \geqslant 1$;

$\{a^{n^2} \mid n \geqslant 0\}$ при $X=\{a\}$ (это множество квадратов целых чисел в унарном представлении);

$\{a^n b^m \mid m \geqslant n \geqslant 0\}$ при $X=\{a, b\}$.

3.* (Аллен, Хартманис, Шенк.) Покажите, что множество простых чисел как в унарном представлении (т. е. числу p соответствует слово x^p, $x \in X$), так и в любом k-ичном представлении не является допустимым. [Указание. Для унарного представления используйте теорему об итеративном подслове. В остальных случаях используйте следующую теорему Дирихле: если натуральные числа a и b взаимно просты, то в арифметической прогрессии $\{a+bi \mid i \in \mathbf{N}_0\}$ содержится бесконечно много простых чисел. Выведете отсюда, что для множества P_k k-представлений простых чисел (без дополнительных нулей) синтаксическая конгруэнция является отношением тождества.

Иное доказательство получается таким образом: по малой теореме Ферма $k^{p-1} \equiv 1 \pmod p$ при любом простом $p>k$. Пусть $uv^r w$ — k-ичное представление простого числа $p>k$, причем $k^{|v|} \not\equiv 1 \pmod p$. Покажите, что число, имеющее

представление $uv^rv^{p-1}w$, делится на p. Примените теперь теорему об итеративном подслове.]

4.* (Берстел.) Покажите, что ни одно k-ичное представление множества $(\mathbf{N}_0-\{0, 1\})^2=\{m\cdot n \mid m, n\in\mathbf{N}, m\neq 1, n\neq 1\}$ не является различимым. [Указание. Используйте п.3.]

5.16. 1. Дайте прямое доказательство следующих высказываний.

1) Akz(X) является булевой алгеброй. Используйте только построения РС-автоматов, в частности образуйте из двух РС-автоматов A и B РС-автомат, допускающий множество $L(A)\cap L(B)$. [Указание. В качестве множества состояний выберите декартово произведение множеств состояний автоматов A и B.]

2) Erk(X) является булевой алгеброй. [Указание. Используйте только определение множества Erk(X) и лемму 5.4.3.]

2. Пусть Boo(X) — наименьшая булева подалгебра булеана $\mathcal{P}(F(X))$, содержащая все конечные множества, т. е. все конечные множества принадлежат Boo(X) и вместе с любыми множествами U и V алгебре Boo(X) принадлежат и множества $U\cup V$, $U\cap V$ и $F(X)-U$. Докажите, что Boo(X) является собственным подмножеством множества Rat(X). [Указание. Покажите, что из $U\in$ $\in$Boo(X) всегда следует, что либо U, либо $F(X)-U$ — конечное множество.]

5.17. 1. (Гинзбург, Спаниер.) Для $U, V, W\subseteq F(X)$ докажите:

$U/(V\cup W)=U/V\cup U/W$;

$(U\cup V)/W=U/W\cup V/W$;

$U/(VW)=(U/W)/V$;

$UW/V=U(W/V)\cup U/(V/W)$.

2. Докажите, что множество всех префиксов (начальных отрезков) слов из рационального множества снова рационально. [Указание. Запишите это множество как частное.]

3. Докажите, что множество всех подслов слов из некоторого рационального множества рационально. [Указание. Запишите это множество как частное.]

4. ([50]) Докажите, что множество всех слов, возникающих при отбрасывании у слов некоторого рационального множества начальной десятой части и конечной (суффиксной) части длины, составляющей 3/7 от длины слова, рационально, т. е. докажите, что при любом U из Rat(X) рационально множество:

$\{w\in F(X) \mid$ существуют $u, v\in F(X)$ такие, что $uwv\in U$, $|u|/|uwv|=1/10$ и $|v|/|uwv|=3/7\}$.

5. (Янтцен.) Докажите, что $PAL/PAL=PAL\cdot PAL$ и $(PAL/PAL)PAL=$ $=(PAL)^3\neq PAL$.

5.18. 1. Приведите примеры множеств $U, V, W\subseteq F(X)$ таких, что:

1) $(U\cup V)^*\neq U^*\cup V^*$;
2) $(U\cup V)^*\neq U^*V^*$;
3) $UV\cap UW\neq U(V\cap W)$;
4) $(U\cap V)^*\neq U^*\cap V^*$;
5) из $U^*\in Rat(X)$ не следует, что $U\in Rat(X)$.

2. Получите системы равенств для НРС-автоматов из примеров 5.1.2, 5.1.3 и 5.1.6, найдите их решения и сравните эти решения с ранее полученными представлениями реакций данных автоматов.

3. (Арден.) Пусть A — PC-автомат с множеством состояний $Z=\{z_1, \ldots, z_n\}$. При $i=1, \ldots, n$ пусть, далее, A'_i — PC-автомат, возникающий при замене в автомате A множества финальных состояний F на $\{z_i\}$, так что

$$L(A'_i)=\{w\in F(X) \mid z_i=f^*(s, w)\}.$$

Получите систему равенств вида $y=yM+R$, имеющую решением вектор $(L(A'_1), L(A'_2), \ldots, L(A'_n))$.

5.19. (Арден, Боднарчук.) Докажите для системы равенств $y=yM+R$ теорему, аналогичную теореме 5.6.6.

2. (Боднарчук.) Покажите, что все решения системы $y=My+R$ имеют вид, определенный в первом высказывании п.2 теоремы 5.6.6 [т. е. $M^*(R+T)$, где $T_i=\varnothing$ при i, не входящих ни в одну LW-последовательность матрицы M].

Покажите, что аналогичное утверждение верно для решений уравнения $y=yM+R$.

3. * (Урпонен.) Покажите, что при $U, V\subseteq F^+(X)$ и $R\subseteq F(X)$ равенство $y=Uy+yV+R$ имеет решение $y=U^*RV^*$ и что $\{U^*(R+T)V^* \mid T\subseteq F(X)\}$ — множество всех решений в случае, когда U или V содержат пустое слово.

5.20. * (Саломаа.) 1. Пусть при $n\in\mathbf{N}$ $\xi(\alpha_1, \ldots, \alpha_n)$ — рациональное выражение, построенное из рациональных выражений $\alpha_1, \ldots, \alpha_n$. Докажите в $Ax(X)$:

$$\vdash(\alpha_1+\alpha_2+\ \ldots\ +\alpha_n)^*=(\alpha_1+\alpha_2+\ \ldots\ +\alpha_n+\xi(\alpha_1, \ldots, \alpha_n))^*;$$

$$\vdash(\alpha_1+\alpha_2+\ \ldots\ +\alpha_n)^*=(\alpha_1+\ \ldots\ +\alpha_n)^*+\xi(\alpha_1, \ldots, \alpha_n)(\alpha_1+\ \ldots\ +\alpha_n)^*.$$

2. Пусть $n\in\mathbf{N}$ и $\alpha_i, \beta_i, \delta_i, \gamma_{ij}$ при $i, j=1, \ldots, n$ — рациональные выражения такие, что ни одно из γ_{ij} не обладает свойством пустого слова и при $i=1, \ldots, n$

$$\vdash\alpha_i=\gamma_{i1}\alpha_1+\gamma_{i2}\alpha_2+\ \ldots\ +\gamma_{in}\alpha_n+\delta_i;$$

$$\vdash\beta_i=\gamma_{i1}\beta_1+\gamma_{i2}\beta_2+\ \ldots\ +\gamma_{in}\beta_n+\delta_i.$$ Докажите в $Ax(X)$: $\vdash\alpha_i=\beta_i$ при $i=1, \ldots, n$.

3. Рациональное выражение α из $RA(X)$ с $X=\{x_1, x_2, \ldots, x_n\}$ называется эквационально определимым (gleichungharakterisiert), если существует конечное число n рациональных выражений α_i таких, что $\alpha\equiv\alpha_1$ и $\vdash\alpha_i=x_1\alpha_{i1}+x_2\alpha_{i2}+\ldots+x_m\alpha_{im}+\delta(\alpha_i)$ при $i=1, \ldots, n$, причем для любой пары i, j существует $k(1\leqslant k\leqslant n)$ такое, что $\alpha_{ij}\equiv\alpha_k$, и $\delta(\alpha_i)\equiv\varnothing$ или $\delta(\alpha_i)\equiv\varnothing^*$.

Докажите, что каждое рациональное выражение над X эквационально определимо. [Указание. Используйте индукцию «по правильным подвыражениям».]

4. На базе полученных выше результатов и лемм из разд. 5.7 докажите полноту системы аксиом $Ax(X)$.

5. Определим длину доказательства в $Ax(X)$ как число встречающихся в этом доказательстве рациональных равенств. Выведите из доказательства п.4 верхнюю границу для длины кратчайшего доказательства произвольного равенства $\alpha=\beta$ и получите в качестве следствия, что множество выводимых в $Ax(X)$ равенств перечислимо.

6. Аналогичным образом докажите полноту системы аксиом, получающейся из системы $Ax(X)$ при изменении порядка сомножителей в произведениях в аксиомах (a_6)—(a_8) и правиле G.

ОБЗОР ЛИТЕРАТУРЫ

Идея рассмотрения вопросов, связанных с возникновением тупиковых ситуаций в параллельных конкурирующих процессах, с помощью взвешенных ориентированных графов высказана в [25]. Поставленные в конце примера 5.1.1 (и решенные в примере 5.5.11) проблемы разрабатывались средствами теории автоматов в [38]. Дополнительные сведения из этой области можно найти, например, в [42].

Идея примера 5.1.2 заимствована из [8], см. также [30].

Простой вариант примера 5.1.3 имеется в [4], там же можно найти и другие хорошие примеры. См. далее указанную в гл. 4 литературу к примеру 4.1.2. Определение из языка Паскаль (пример 5.1.4) содержится в [26].

Понятие НРС-автомата было введено в [41] (получено в 1957 г.). В этой очень трудной для чтения работе были доказаны (по большей части несколько иначе, чем в данной книге) теоремы 5.3.5, 5.3.7, 5.4.4, 5.5.3, 5.5.5, 5.5.9 и следствие 5.4.10. Приведенное здесь доказательство теоремы 5.3.5 взято из [39]; идея доказательства теоремы 5.3.7 заимствована из [30]; пункты 2 и 3 теоремы 5.5.9 и приведенное здесь доказательство получены в книге [1, ч. I] из списка литературы к гл. 2.

По поводу иной интерпретации недетерминированных автоматов см. [24].

В качестве абстрактных моделей нейронных сетей автоматы, допускающие множества слов, были введены уже в [31]. Они были подробно исследованы прежде всего в [27] (результаты получены в 1951 г.). Клини в этой работе определил рациональные множества и показал в основном, что выполняется равенство $\mathrm{Akz}(X)=\mathrm{Rat}(X)$. Он использовал при этом несколько иные операции и термин «регулярные события» (см. также [11]); введение термина «рациональные множества» и определения понятия «различимые множества» (см. определение 5.4.2) восходит к работе [15]; по этому поводу и по поводу упражнения 5.7, п.3 см. [16] и книгу [3] из списка литературы к гл. 2.

Полностью определенные детерминированные автоматы без выхода, т. е. РС-автоматы, были описаны уже в [37]. В этой работе были введены ставшие сегодня обычными определения регулярных (т. е. рациональных) множеств и доказано равенство $\mathrm{Akz}(X)=\mathrm{Rat}(X)$. Там же определено понятие моноида переходов (для РС-автоматов) и приведены теоремы 5.4.4 и 5.5.5 и их доказательства.

РС-автоматы были также определены в [35], причем как в том виде, в котором они заданы определением 5.4.1, т. е. как «читающие машины Тьюринга» (см. описание, приведенное в начале разд. 5.4), так и в виде машин, множеством состояний которых является моноид (см. доказательство теоремы 5.4.4). Там же было введено понятие моноида переходов и доказаны утверждения, близкие теоремам 5.4.5, п.1 и 5.4.4.

В несколько иных (но эквивалентных) терминах равенства $\mathrm{NAkz}(X)=\mathrm{Akz}(X)=\mathrm{Rat}(X)$ и теорема 5.5.5 были получены в [9] (вместо допускающих автоматов использовались праволинейные грамматики).

Теорема 5.4.5, п.2 была в основном доказана Гинзбургом [18] и Глушковым [21] — важнейшая часть работы Глушкова в качестве приложения к гл. 2 включена в книгу [8] из списка литературы к гл. 2.

Дополнительную информацию о моноидах переходов РС-автоматов, особенно о вычислении таких моноидов, можно найти в [40, 12 и 7].

Понятия синтаксического моноида и синтетической конгруэнции были введены

дены в [48], см. также [47 и 10]. Первое подробное рассмотрение синтаксических моноидов рациональных множеств дано в [33].

Понятие языков Дика (см. следствие 5.4.7 и п 3 упражнения 5.8) было введено в информатике Шютценбергером. Эти множества с алгебраической точки зрения исследовались уже В. ван Диком, см. [49 и 10]. Лемма 5.4.11 восходит к работе [29]. По этому поводу и по поводу теории равенств над свободными моноидами см. [28] и учебник [9] из списка литературы к гл. 4.

Операции образования частных и вторая часть теоремы 5.5.7 содержатся в [17], см. также [52]. Обобщение высказывания теоремы доказано в [19].

Следствие 5.5.8 и его доказательство получены в [44]. Дополнительная информация о теории допустимых и не допустимых числовых множеств содержится в [5].

Идея сопоставления РС-автоматам равенств восходит к [2 и 6]. В первой из работ дано решение равенства $y=yL+R$ при $\Lambda \notin L$, во второй — рассмотрен общий случай. См. по этому поводу, а также по поводу теоремы 5.6.1 книгу [24] из списка литературы к гл. 2.

Содержание разд. 5.7 взято в основном из [46]. То, что равенства $\alpha+\varnothing=\alpha$ и $\alpha+\alpha=\alpha$ можно не включать в число аксиом, и то, что система аксиом Ax(X) независима, показано в [54].

Относительно простой метод установления эквивалентности рациональных выражений можно найти в [20]. Оценка сложности таких методов содержится в [36] и [5] из списка литературы к гл. 4.

По поводу упражнения 5.1 см., например, [43, 53 и 55], по поводу упражнения 5.2 — [33, 34 и 40].

Методы из п.2 упражнения 5.6 использовались в [41]. Утверждение из п.3 упражнения 5.6 доказано в [3].

По поводу упражнения 5.7 см. [32], где был предложен первый алгоритм такого рода, а также [21 и 8] из списка литературы к гл. 2.

Утверждение из упражнения 5.12 установлено в [34].

По поводу упражнения 5.13 см. [33]. Пункт 3 упражнения 5.15 взят из [1] (первый способ доказательства) и из [22] (второй способ доказательства), см. также [5], и эту же работу — по поводу п.4 упражнения 5.15.

Упражнение 5.17, п.4 основано на частном случае общей теоремы из [50].

По поводу упражнения 5.20 см. [45, 46 и 24] из списка литературы к гл. 2.

Обзор состояния теории рациональных множеств и РС-автоматов на 1968 г. дан в [23].

ГЛАВА 6.

ПРЕОБРАЗОВАНИЯ АВТОМАТОВ

В предыдущей главе с помощью рациональных выражений и моноидов переходов было показано, как для произвольного НРС-автомата может быть построен эквивалентный РС-автомат. В этой главе будет дан прямой метод такого построения, состоящий в преобразованиях самих соответствующих автоматов. Кроме того, на этой основе будет исследована проблема минимизации числа состояний.

Как указывалось в гл. 5 при проектировании автоматов бывает очень удобно на первом этапе построить НРС-автомат, допускающий определенное (скажем, заданное рациональным выражением) множество, а потом преобразовать его в ДРС-автомат. Приведенные ниже примеры показывают, что при этом могут получиться удивительно большие (по числу состояний) ДРС-автоматы, хотя, с другой стороны, соответствующие зеркальные множества будут допустимыми для очень небольших (в том же смысле) ДРС-автоматов.

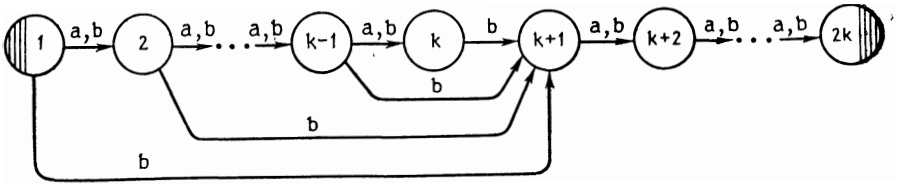


Рис. 6.1.1. Допускающий множество E_k НРС-автомат

Пример 6.1.1. Пусть $k \in \mathbf{N}$, $X=\{a, b\}$ и E_k — конечное множество всех слов из $F(X)$, имеющих длину, не превышающую $2k-1$, и таких, что в них на k-м месте справа стоит символ b, т. е.

$$E_k=\{ubv \in \{a, b\}^* \mid |u| \leqslant k-1, |v|=k-1\}.$$

Утверждение 1. E_k допускается НРС-автоматом с $2k$ состояниями.

Доказательство. Граф решающего задачу автомата изображен на рис. 6.1.1.

Утверждение 2. Каждый ДРС-автомат, допускающий множество E_k, должен иметь не менее 2^k состояний.

Доказательство. Пусть $A=(Z, X, f, s, F)$ — допускающий множество E_k ДРС-автомат.

Покажем прежде всего, что для 2^k-1 различных слов w из $F(X)$ длины, не большей $k-1$, состояния $f^*(s, w)$ должны быть попарно различны [поскольку каждое такое слово может быть продолжено до слова из E_k, функция f^* должна быть определена во всех точках (s, w)].

Итак, пусть w_1 и w_2 — различные слова длины, не большей $k-1$, из $F(X)$ с $|w_1|=r$ и $|w_2|=s$.

Если $r \neq s$, то без ограничения общности можно считать, что $r<s$. Положим $w'=a^{k-r-1}ba^{k-1}$. Тогда $w_1w' \in E_k$, так что должно выполняться включение $f^*(s, w_1w') \in F$, но $|w_2w'|>2k-1$, т. е. $w_2w' \notin E_k$, и поэтому должно быть $f^*(s, w_2w') \notin F$. Поскольку автомат A детерминирован, из сказанного вытекает, что $f^*(s, w_1) \neq f^*(s, w_2)$.

Пусть теперь $r=s \neq 0$, $w_1=x_rx_{r-1}\ldots x_2x_1$ и $w_2=y_ry_{r-1}\ldots y_2y_1$.

Так как $w_1 \neq w_2$, существует наименьший индекс j $(1 \leqslant j \leqslant k-1)$ такой, что $x_j \neq y_j$. Для этого j мы можем (не ограничивая общно-

сти) считать, что $x_j=b$ и $y_j=a$. Пусть $w'=a^{k-j}$. Тогда $w_1w'\in\tilde{E}_k$ и $w_2w'\notin E_k$, так что должны выполняться соотношения $f^*(s, w_1w')\in F$ и $f^*(s, w_1w')\notin F$, а потому и должно быть $f^*(s, w_1)\neq f^*(s, w_2)$.

Поскольку ни одно из слов w, длины, меньшей k, не принадлежит E_k, то автомат A должен иметь по меньшей мере еще одно состояние (финальное), т. е. всего он должен иметь не менее 2^k состояний.

Утверждение 3. Зеркальное множество $\tilde{E}_k=\{vbu \mid |v|=k-1, |u|\leqslant k-1\}$ для множества E_k допускается ДРС-автоматом с 2k состояниями.

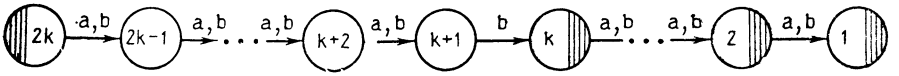


Рис. 6.1.2. Допускающий множество $\tilde{E}_k$ ДРС-автомат

Доказательство. Граф решающего эту задачу автомата изображен на рис. 6.1.2.

В результате обобщения вышесказанного легко получить следующий пример.

Пример 6.1.2. Пусть $k\geqslant 2$. Множество $U_k=\{a, b\}^*b\{a, b\}^{k-1}$ всех слов из F(X), в которых на k-м месте справа стоит b, допускается НРС-автоматом с k+1 состояниями (рис. 6.1.3). Каждый же ДРС-автомат, допускающий U_k, должен иметь по меньшей мере 2^k состояний (см. ниже). Зеркальное множество $\tilde{U}_k$, т. е. множество всех слов из F(X), в которых на k-м месте слева стоит символ b, допускается ДРС-автоматом с k+1 состояниями (рис. 6.1.4).

Итак, пусть $A=(Z, X, f, s, F)$ — допускающий множество U_k ДРС-автомат.

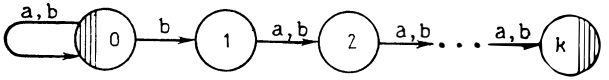


Рис. 6.1.3. Допускающий множество U_k НРС-автомат

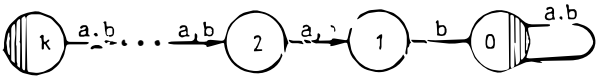


Рис. 6.1.4. Допускающий множество U_k ДРС-автомат

Пусть, далее, V_k — множество всех слов из F(X), начинающихся с символа b и имеющих длину, не большую k. Тогда $|V_k|=2^k-1$ и каждое слово w из V_k может быть продолжено до некоторого слова из U_k, так что всегда должно быть определено состояние $f^*(s, w)$.

Для каждого w из V_k верно соотношение $f^*(s, w)\neq s$. Действительно, если бы имелось слово w длины p в V_k такое, что $f^*(s, w)=s$, то мы бы имели $f^*(s, a^{k-p})=f^*(s, wa^{k-p})\in F$, т. е. $a^{k-p}\in U_k$, что неверно.

Пусть теперь w_1 и w_2 — произвольные различные слова из V_k. Если $|w_1|<|w_2|=p\leqslant k$, то $w_2a^{k-p}\in U_k$, и так как $|w_1a^{k-p}|<k$, то выполнено $w_1a^{k-p}\notin U_k$, так что $f^*(s, w_1)\neq f^*(s, w_2)$.

Пусть, наконец, $|w_1|=|w_2|$, $w_1=x_rx_{r-1}\ldots x_1$ и $w_2=y_ry_{r-1}\ldots y_1$. Тогда существует наибольший индекс j такой, что $x_j\neq y_j$. Будем считать, что $x_j=b$ и $y_j=a$, причем из $x_r=y_r=b$ следует $j<r\leqslant k$. В этом случае $w_1a^{k-j}\in U_k$, но $w_2a^{k-j}\notin U_k$, т. е. снова $f^*(s, w_1)\neq f^*(s, w_2)$.

Итак, автомат A имеет по меньшей мере $1+2^k-1=2^k$ различных состояний.

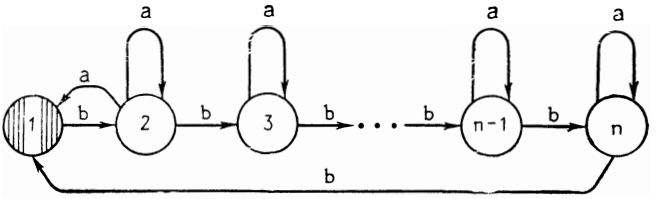


Рис. 6.1.5. НРС-автомат A_n'

Замечание. Отметим, что НРС-автомат, граф которого изображен на рис. 6.1.1, «допуская» слово длины $i+k$ из E_k, принимает «по пути» не более $i+1$ недетерминированных решений (о выборе одной из двух возможностей). Автомат же, граф которого изображен на рис. 6.1.3, обладает меньшей степенью недетерминированности, так как недетерминированное решение встречается в этом случае только в одном состоянии при одном входе и выбирается одна из двух альтернатив.

Для каждого $n\geqslant 3$ в п.1 упражнения 6.1 рассматривается множество, допускаемое НРС-автоматом с n состояниями, который только в одном состоянии и только при одном входе выбирает одну из двух альтернатив, причем множество, зеркальное для данного, допускается ДРС-автоматом с n состояниями. В то же время ни одни РС-автомат менее чем с 2^n состояниями не допускает это множество. Правда, при этом необходимы три входных символа.

НРС-автоматы только с двумя входными символами и с наименьшей возможной степенью недетерминированности рассматриваются в п.3 упражнения 6.1 и в доказательстве теоремы 6.3.7.

Пример 6.1.3. Если у НРС-автомата A_n из п.1 упражнения 6.1 отбросить вход c, то при $n\geqslant 3$ получится НРС-автомат A_n' (рис. 6.1.5), для которого зеркальный автомат $\tilde{A}_n'$ оказывается РС-автоматом.

Утверждение. Каждый ДРС-автомат, допускающий $L(A_n')$, имеет не менее $(n-1)n+1$ состояний.

Доказательство. Пусть A — допускающий множество $L_n=L(A_n')$ ДРС-автомат. Покажем, что для всех различных слов w вида $(ba)^{n-1}$ или $(ba)^ib^j$ с $0\leqslant i\leqslant n-2$ и $0\leqslant j\leqslant n-1$ состояния $f^*(s, w)$ [их имеется $(n-1)n+1$] различны. Поскольку каждое

такое слово w может быть продолжено до слова из L_n, то состояния $f^*(s, w)$ определены.

Пусть $0 \leqslant p, r \leqslant n-1$ и $0 \leqslant q, s \leqslant n-1$, причем $q=0$ $(s=0)$, если $p=n-1$ $(r=n-1)$. Пусть также $w_1=(ba)^p b^q$, $w_2=(ba)^r b^s$ и $w_1 \neq w_2$, т. е. $(p, q) \neq (r, s)$. Предположим еще, что $p+q \leqslant r+s$.

Как и выше, для каждой такой пары слов мы определим слово u такое, что $w_i u \in L_n$ и $w_j u \notin L_n$ при $i \neq j$. Для этого придется различать следующие случаи.

1. $p+q=r+s$. Тогда $p \neq r$, $q \neq s$, так что, например, $p<r$ и $q>s$. При этом $w_2 b^{n-s} \in L_n$. Так как $p+q+n-s=r+n<2n$ и $q+n-s>n$, то имеем $w_1 b^{n-1} \notin L_n$.

2. $p+q<r+s<n$. При $k=n-r-s$ выполнено неравенство $p+q+k<n$, так что $w_1 b^k \notin L_n$, но $w_2 b^k \in L_n$.

3. $p+q<n \leqslant r+s$. Тогда $w_2 \in L_n$, но $w_1 \notin L_n$.

4. $n \leqslant p+q<r+s \leqslant 2n-3$. Тогда $p \neq 0$, $r \neq 0$.

1) $r+s-q<n$. Тогда $n<2n-r-s+q<2n-r-s+p+q<2n$, так что при $k=2n-r-s$ выполнено $w_2 b^k \in L_n$, но $w_1 b^k \notin L_n$.

2) $n \leqslant r+s-q$, $r \neq n-1$. Пусть i выбрано так, что $r+s-q=n+i$. При $k=n-q-i-1$ в этом случае $r+s+k=2n-1$ и $s+k>n$, так что $w_2 b^k \notin L_n$. Так как $n+i-p=r+s-(p+q)<n$, т. е. $p>i$, то выполнено неравенство $p+q+k=p+n-i-1 \geqslant n$. Так как $q+k<n$, то отсюда следует, что $w_1 b^k \in L_n$.

3) $n \leqslant r+s-q$, $r=n-1$. Тогда $s=0$, так что $n<n-1+0-q$, т. е. этот случай встретиться не может. ■

Замечание. Автомат A_n' можно изменить так, что получится НРС-автомат, рассматриваемый в п.2 упражнения 6.1. Для этого достаточно провести ребро с меткой a из состояния 1 в состояние 3 (в графе, изображенном на рис. 6.1.5), ребро с меткой b — из состояния n в состояние 2, исключить все петли с меткой a и вместо них провести из каждого состояния i при $i=3, 4, \ldots, n-1$ ребро с меткой a в состояние $i+1$.

Если же изменить автомат A_n, проводя в графе, изображенном на рис. 6.1.5, ребра с меткой a из каждого состояния i при $i=3, 4, \ldots, n$ в состояние 1, то получится автомат, рассматриваемый в п. 3 упражнения 6.1 (с точностью до обозначения состояний).

Если в графе последнего НРС-автомата исключить петли с меткой a у вершин $2, 3, \ldots, n-1$ и дополнительно пометить вместо них при $i \geqslant 1$ ведущие из вершин i в вершины $i+1$ ребра меткой a, добавить у вершины 1 петлю с меткой a, убрать метку b на ребре, ведущем из n в 1, и сделать начальным и финальным состояние n вместо состояния 1, то будет получен граф рассматриваемого в п.4 упражнения 6.1 НРС-автомата, допускающего множество

$$W_n = aW_n'a\{a, b\}^{n-1} \cup a\{a, b\}^{n-1} \cup \{\Lambda\},$$

где $W_n' = \{w \in F(\{a, b\}) \mid w \text{ не содержит подслова } b^n\}$.

Во всех трех случаях (как требуется показать в упражнении 6.1) эквивалентные РС-автоматы имеют не менее 2^n состояний.

Метод исключения лишних состояний и спонтанных переходов основан на представлении НРС-автоматов в виде взвешенных ориентированных графов и соответствующем известном в теории графов алгоритме.

Приводимый в этом разделе способ преобразования в алфавитный полностью определенный детерминированный автомат (данного НРС-автомата) в большей степени ориентирован на теорию автоматов, в соответствии с чем особое внимание уделяется увеличению числа состояний.

Как и раньше, пусть далее, если не оговорено противное, A — НРС-автомат в обычных обозначениях.

ИСКЛЮЧЕНИЕ ЛИШНИХ СОСТОЯНИЙ

Состояние НРС-автомата является лишним, если оно не вносит вклада в реакцию этого автомата, т. е. если в графе автомата A не существует пути, ведущего хотя бы из одного начального состояния в это состояние, или если в нем не существует пути, ведущего из этого состояния в какое-либо финальное.

Определение 6.2.1. 1. Состояние z автомата A называется *достижимым,* если существуют слово $w \in F(X)$ и начальное состояние s автомата A такие, что $z \in t^*(s, w)$; в противном случае состояние z называется *недостижимым.*

Автомат A называется *инициально связным,* если все его состояния достижимы.

2. Состояние z автомата A называется *избыточным,* если его реакцией является пустое множество; в противном случае состояние z называется *неизбыточным.*

Автомат A называется *неизбыточным,* если каждое его состояние неизбыточно; в противном случае автомат A называется *избыточным.*

3. Состояние z автомата A называется *поглощающим,* если в графе автомата A из вершины z не исходит ни одно ребро, т. е. если из $(z, w, z') \in \tau$ всегда вытекает, что $z' = z$.

Замечание. Отметим, что не каждое избыточное состояние является поглощающим — см. по этому поводу упражнение 6.2 и следующую лемму.

Лемма 6.2.2. Состояние z автомата A является избыточным тогда и только тогда, когда оно является недостижимым в автомате $\bar{A}$, зеркальном для A (см. доказательство теоремы 5.3.5).

Доказательство. Реакцией состояния z оказывается пустое множество тогда и только тогда, когда в графе автомата A из вершины z ни один путь не ведет ни в одно финальное состояние, т. е. когда не существует слова w в F(X) такого что $f^*(z, w) \cap F \neq \neq \varnothing$. Это эквивалентно тому, что в зеркальном для A автомате состояние z не достижимо ни из одного состояния из F. ■

На основе этой леммы можно, таким образом, любой метод определения достижимых состояний (или метод построения экви-

валентного инициально связного НРС-автомата) использовать для определения неизбыточных состояний (или для построения эквивалентного неизбыточного НРС-автомата). Для этого достаточно применить данный метод к автомату, зеркальному для рассматриваемого.

Метод 6.2.3 (нахождение всех достижимых состояний автомата A.

Положить $E_0=\varnothing$, $E_1=S$ и $i=1$.

До тех пор, пока не будет выполнено равенство $E_i=E_{i-1}$, увеличивать i на 1 ($i:=i+1$) и строить по E_{i-1} множество E_i, присоединяя к E_{i-1} все состояния z, для которых в графе автомата A существует ребро, ведущее в z из какого-либо состояния из E_{i-1}:

$E_i=E_{i-1}\cup\{z\in Z|$ существует переход $(z', w, z)\in\tau$ такой, что $z'\in E_{i-1}\}$.

В момент остановки множество E_i будет содержать все достижимые состояния и только их.

Доказательство корректности. Так как $E_{i-1}\subseteq E_i\subseteq Z$ при $i\geqslant 1$, метод сходится (дает результат за конечное число шагов).

Очевидно, что $E_{i+1}=pr_3(\tau^i\cap S\times F(X)\times Z)$ при $i\geqslant 0$ и что $E=pr_3(\tau^*\cap S\times F(X)\times Z)$ — множество всех достижимых состояний автомата A. До тех пор, пока $E_{i-1}\neq E$, выполнено $E_{i-1}\neq E_i$. ■

Теорема 6.2.4. НРС-автомат $A'=(E', X, t', S\cap E', F\cap E')$ с $\tau'=\tau\cap E'\times F(X)\times E'$, полученный из автомата A в результате сужения τ, S и F на множество E' всех достижимых и неизбыточных состояний автомата A, является эквивалентным автомату A инициально связным неизбыточным НРС-автоматом.

Доказательство. Очевидно, что автомат A' — инициально связный и что $L(A')\subseteq L(A)$.

Пусть $w\in L(A)$. Тогда существует последовательность $(z_0, w_1, z_1), (z_1, w_2, z_2), \ldots, (z_{n-1}, w_n, z_n)$ переходов автомата A такая, что $z_0\in S$, $z_n\in F$ и $w_1w_2\ldots w_n=w$. Поскольку все состояния z_i при $i=0, 1, \ldots, n$ достижимы и неизбыточны, то $(z_{i-1}, w_i, z_i)\in\tau'$ при $i=1, \ldots, n$, $z_0\in S\cap E'$ и $z_n\in F\cap E'$. Поэтому $w\in L(A')$. ■

ИСКЛЮЧЕНИЕ СПОНТАННЫХ ПЕРЕХОДОВ

Теорема 6.2.5. Пусть $A=(Z, X, t, S, F)$ — НРС-автомат. Тогда автомат $A'=(Z, X, t', S, F')$ с множеством финальных состояний $F'=F\cup\{z\in S|$ существует состояние $z'\in F$ такое, что $(z, \Lambda, z')\in\tau^*\}$, и с $\tau'=\{(z, w, z')\in Z\times F^+(X)\times Z|$ существует переход $(z_0, w, z_0')\in\tau$ такой, что $w\neq\Lambda$, $(z, \Lambda, z_0)\in\tau^*$, $(z_0', \Lambda, z')\in\tau^*\}$ является эквивалентным автомату A НРС-автоматом без спонтанных переходов. Автомат A' может быть построен эффективно; пары (z_i, z_j) со свойством $(z_i, \Lambda, z_j)\in\tau^*$ могут быть определены с помощью метода 6.2.6.

Доказательство. Автомат A' может быть построен эффективно, так как для каждой пары состояний z, z' за конечное число шагов можно определить, выполняется ли включение $(z, \Lambda, z')\in$

$\in\tau^*$. Действительно, для этого достаточно рассмотреть конечное множество последовательностей состояний $z_0=z, z_1, z_2, \ldots, z_k$, где $k<|Z|$, таких, что $(z_{i-1}, \Lambda, z_i)\in\tau$ при $i=1, \ldots, k$. Очевидно, что $(z, \Lambda, z')\in\tau^*$ тогда и только тогда, когда z' входит в одну из таких последовательностей. Более детально этот процесс представлен в методе 6.2.6.

Ясно, что $L(A')\subseteq L(A)$, поскольку из $(z, w, z')\in\tau'^*\cap S\times L(A')\times F'$ следует, что $z'\in F$ или что существует состояние $z''\in F$ такое, что $(z', \Lambda, z'')\in\tau^*$, т. е. $(z, w, z'')\in\tau^*$.

Нам осталось показать, что выполняется включение $L(A)\subseteq L(A')$.

Если $\Lambda\in L(A)$, то существуют состояния $z\in S$ и $z'\in F$ такие, что $(z, \Lambda, z')\in\tau^*$, так что в этом случае $z\in F'$ и потому $\Lambda\in L(A')$.

Пусть теперь $w\in L(A)$ и $w\neq\Lambda$. Тогда в графе автомата A существует путь из некоторого начального состояния z_0 в некоторое финальное состояние z_p' такой, что последовательность меток на проходимых ребрах составляет слово w. При этом отдельные ребра или группы последовательно проходимых ребер могут иметь метки Λ, т. е. соответствовать спонтанным переходам. Пусть существуют состояния z_i и z_i' при $i=0, \ldots, p$ и непустые слова $w_1, \ldots, w_p$ такие, что $z_0\in S$, $z_p'\in F$, $(z_i, \Lambda, z_i')\in\tau^*$ при $i=0, \ldots, p$, $(z_{i-1}', w_i, z_i)\in\tau$ при $i=1, \ldots, p$ и $w_1w_2 \ldots w_p=w$.

В таком случае $(z_{i-1}, w_i, z_i)\in\tau'^*$ при $i=1, \ldots, p-1$ и $(z_{p-1}, w_p, z_p')\in\tau'^*$. Поэтому $w\in L(A')$. ■

Если в графе автомата A исключить все ребра, имеющие отличные от Λ метки, то будет получен граф соответствия t_A. Его можно рассматривать уже как просто ориентированный граф (не взвешенный). Определение пары состояний (z_i, z_j) такой, что $(z_i, \Lambda, z_j)\in\tau^*$, означает тогда не что иное, как решение вопроса, существует ли в графе соответствия t_A путь из z_i в z_j? Таким образом, можно пользоваться известным алгоритмом Варшалла для поиска всех путей в ориентированном графе (см. также п.1 упражнения 5.7).

Метод 6.2.6 (определение связанных последовательностями спонтанных переходов состояний).

Пусть $Z=\{z_1, z_2, \ldots, z_n\}$ — множество состояний исследуемого НРС-автомата. Введем при $1\leqslant i, j\leqslant n$ и $0\leqslant k\leqslant n$ булевы переменные B^k_{ij}, т. е. переменные, которые могут принимать значения 0 и 1. Пусть, далее, $\wedge$ и $\vee$ — обычные булевы операции, т. е. пусть $0\wedge 0=0\wedge 1=1\wedge 0=0\vee 0=0$ и $1\wedge 1=0\vee 1=1\vee 0=1\vee 1=1$. Значения B^k_{ij} определяются следующим образом.

1. При i, пробегающем значения от 1 до n, выполнить следующее:

при j, пробегающем значения от 1 до n, положить

$$B^0_{ij}=\begin{cases}1, & \text{если } i=j \text{ или } (z_i, \Lambda, z_j)\in\tau.\\ 0 & \text{в противном случае.}\end{cases}$$

2. При k, пробегающем значения от 1 по n, выполнить следующее:

при i, пробегающем значения от 1 до n, выполнить следующее:

при j, пробегающем значения от 1 до n, положить

$$B^k_{ij} = B^{k-1}_{ij} \vee (B^{k-1}_{ik} \wedge B^{k-1}_{kj}).$$

Включение $(z_i, \Lambda, z_j) \in \tau^*$ выполняется тогда и только тогда, когда $B^n{}_{ij}=1$.

Доказательство корректности. То, что метод дает результат за конечное число шагов, очевидно. Справедливость утверждения о значениях $B^n{}_{ij}$ немедленно вытекает из следующего промежуточного утверждения.

Промежуточное утверждение. $B^k{}_{ij}=1$ тогда и только тогда, когда в графе соответствия $t^*{}_A$ существует (возможно, тривиальный) путь из z_i в z_j через состояния из $\{z_1, ..., z_k\}$, т. е. когда существует последовательность спонтанных переходов автомата A, переводящая его из состояния z_i в состояние z_j через состояния из $\{z_1, \ldots, z_k\}$ (ср. п.1 упражнения 5.7).

Доказательство промежуточного утверждения. При $k=0$ утверждение очевидно, так как $B^0{}_{ij}=1$ тогда и только тогда, когда $(z_i, \Lambda, z_j) \in \tau^0 \cup \tau$.

Допустим, что утверждение выполнено при $k=p$.

а) Если $B^{p+1}_{ij} = 1$, то $B^p_{ij} = 1$ или $B^p{}_{i,p+1} \wedge B^p{}_{p+1,j}=1$. По предположению индукции в этом случае в графе соответствия t^*_A существует путь из z_i в z_j или существуют два пути — один из z_i в z_{p+1} и второй из z_{p+1} в z_j, причем все эти пути могут проходить только через вершины, соответствующие состояниям из множества $\{z_1, ..., z_p\}$, так что в любом случае существует путь из z_i в z_j, проходящий через вершины, соответствующие состояниям из множества $\{z_1, \ldots, z_{p+1}\}$.

б) Пусть теперь существует путь из z_i в z_j, проходящий только через состояния из множества $\{z_1, ..., z_{p+1}\}$. Тогда возможны два случая.

Если путь не проходит через вершину z_{p+1}, то по предположению индукции $B^p{}_{ij}=1$.

Допустим, что рассматриваемый путь проходит через вершину z_{p+1}. В этом случае он может включать в себя циклы (подпути, имеющие одну вершину в качестве начальной и конечной), ведущие из z_{p+1} в z_{p+1}. Если исключить из рассматриваемого пути все такие циклы, то останется путь, допускающий разбиение на два пути, один из которых ведет из z_i в z_{p+1} и второй — из z_{p+1} в z_j, причем оба эти пути проходят только через состояния из $\{z_1, \ldots, z_p\}$, так что по предположению индукции $B^p{}_{i,p+1} \wedge B^p{}_{p+1,j} = 1$. ■

АЛФАВИТИЗАЦИЯ И ДООПРЕДЕЛЕНИЕ

Не являющийся алфавитным НРС-автомат — это по сути дела сокращенное представление некоторого алфавитного НРС-автомата, в котором исключены состояния, лежащие на некотором

единственном пути из одного состояния в другое. Доопределение НРС-автомата целесообразно только в том случае, когда этот автомат алфавитный. Оно проводится совершенно так же, как в случае частичных автоматов Мили (см. лемму 4.3.5), т. е. добавлением некоторого поглощающего состояния.

Теорема 6.2.7. 1. Для каждого НРС-автомата A может быть эффективно построен эквивалентный алфавитный НРС-автомат A′, причем так, что все ребра из графа автомата A, имеющие метки Λ или x (где $x \in X$), будут входить в граф автомата A′.

2. Для каждого не полностью определенного алфавитного НРС-автомата A может быть эффективно построен эквивалентный НРС-автомат $\bar{A} = (\bar{Z}, \bar{X}, \bar{t}, S, F)$ (называемый доопределением автомата A), обладающий следующими свойствами:

$\bar{A}$ является полностью определенным, т. е. $\bar{t}(z, x) \neq \varnothing$ для любой пары $(z, x) \in \bar{Z} \times X$);

граф автомата $\bar{A}$ содержит граф автомата A в качестве подграфа;

$\bar{A}$ имеет ровно на одно состояние больше, чем автомат A, причем это состояние является поглощающим.

Доказательство. 1. Если $(z, w, z') \in \tau$ при $w = x_1 x_2 \ldots x_k$, $x_i \in X$, $k \geqslant 2$, то дополним множество Z новыми состояниями $z_1, z_2, \ldots, z_{k-1}$ и заменим переход (z, w, z') на совокупность переходов (z, x_1, z_1), (z_1, x_2, z_2), $\ldots$, (z_{k-1}, x_k, z'). Остальное ясно.

2. Доопределением A является НРС-автомат $\bar{A} = (\bar{Z}, X, \bar{t}, S, F)$ с $\bar{Z} = Z \cup \bar{z}$, где $\bar{z} \notin Z$, и $\bar{\tau} = \tau \cup \{(\bar{z}, x, \bar{z}) \mid x \in X\} \cup \{(z, x, \bar{z}) \mid t(z, x) = \varnothing\}$.

Очевидно, что для каждой пары (z, x) из $\bar{Z} \times X$ в $\bar{\tau}$ содержится переход (z, x, z'), т. е. автомат $\bar{A}$ является полностью определенным.

Далее, состояние $\bar{z}$ — поглощающее, а потому и избыточное, так как оно не является финальным. Из леммы 6.2.2 и теоремы 6.2.4 вытекает поэтому, что $\bar{A}$ имеет ту же реакцию, что и A. ■

ПОСТРОЕНИЕ ЭКСПОНЕНЦИАЛЬНОГО АВТОМАТА

Как можно увидеть в примерах из разд. 6.1 и из упражнения 6.1, эквивалентный данному НРС-автомату РС-автомат может нуждаться в числе состояний, не меньшем, чем число подмножеств множества состояний Z исходного автомата A, т. е. для построения такого РС-автомата может понадобиться не менее $2^{|Z|}$ состояний.

Теорема 6.2.8 (Рабин, Скотт). Пусть A — алфавитный НРС-автомат. Тогда для него может быть построен эквивалентный так называемый *экспоненциальный автомат* A_p, являющийся РС-автоматом: $A_p = (\mathcal{P}(Z), X, f_p, \{S\}, F_p)$, где $f(M, x) = t^*(M, x) = \{z \in Z \mid$ существует состояние $z' \in M$ такое, что $(z' x, z) \in \tau^*\}$ для всех x из X и $F_p = \{M \in \mathcal{P}(Z) \mid M \cap F \neq \varnothing\}$.

Методом 6.2.9 можно непосредственно построить эквивалентный автомату A подавтомат $A_{p'}$ экспоненциального автомата, имеющий только достижимые состояния, т. е. для этого можно не применять метод 6.2.3.

Замечания. 1. Если автомат A побуквенный, то $t^*(M, x) = t(M, x)$.

2. Состояние $\varnothing$ автомата A_p — поглощающее. Если автомат A определен полностью, то это состояние недостижимо.

Доказательство. Автомат A_p — это, очевидно, РС-автомат, который с использованием метода 6.2.6 может быть построен эффективно, поскольку $t^*(M, x) = t^*(t(t^*(M, \Lambda), x), \Lambda)$.

Промежуточное утверждение 1. $L(A) \subseteq L(A_p)$.

Доказательство. Пусть $w \in L(A)$. Тогда существуют $z_0, z_1, \ldots, z_k$ из Z и $x_1, \ldots, x_k$ из X такие, что $z_0 \in S$, $z_k \in F$, $w = x_1 x_2 \ldots x_k$ и $(z_{i-1}, x_i, z_i) \in \tau^*$ при $i = 1, \ldots, k$.

Пусть тогда $M_0 = S$, $M_i = t^*(M_{i-1}, x_i)$ при $i = 1, \ldots, k$. В этом случае $z_k \in M_k \cap F$, так что $w \in L(A_p)$.

Промежуточное утверждение 2. $L(A_p) \subseteq L(A)$.

Доказательство. Пусть $w \in L(A_p)$. Тогда существуют $M_0 = S, M_1, \ldots, M_k$ из $\mathcal{P}(Z)$ и $x_1, \ldots, x_k$ из X такие, что $M_k \cap F \neq \varnothing$ и $f_p(M_{i-1}, x) = M_i$ при $i = 1, \ldots, k$. Но в этом случае существует и последовательность состояний $z_0, z_1, \ldots, z_k$ такая, что $z_i \in M_i$ при $i = 0, 1, \ldots, k-1$ и $z_k \in M_k \cap F$. так что $(z_{i-1}, x_i, z) \in \tau^*$ при $i = 1, \ldots, k$, $z_0 \in S$ и $z_k \in F$, т. е. $w \in L(A)$. ■

Замечание. В бесконечно многих случаях конструкция экспоненциального автомата оказывается оптимальной, что вытекает из упражнения 6.1 и будет показано в теореме 6.3.7.

Метод 6.2.9 (построение «достижимой части» экспоненциального автомата).

1) Положить $\mathcal{M} = \{S\}$ и $\mathcal{M}' = \varnothing$.

2) До тех пор, пока не будет выполнено равенство $\mathcal{M} = \mathcal{M}'$, полагать $\mathcal{M} = \mathcal{M}'$ и строить

$\mathcal{M} = \{M \in \mathcal{P}(Z) \mid$ существуют $M' \in \mathcal{M}'$ и $x \in X$ такие, что $t^*(M', x) = M\} \cup \mathcal{M}'$.

3) В момент окончания работы $\mathcal{M}$ является множеством всех достижимых состояний автомата A_p.

4) Положить $A_{p'} = (\mathcal{M}, X, f_{p'}, \{S\}, F_p \cap \mathcal{M})$ с $f_{p'} = f_p / \mathcal{M}$.

Доказательство корректности. Метод дает результат за конечное число шагов, так как всегда $\mathcal{M}' \subseteq \mathcal{M} \subseteq \mathcal{P}(Z)$.

Остальная часть доказательства аналогична доказательству корректности метода 6.2.3.

Замечания. 1. Для того чтобы построить эквивалентный данному НРС-автомату РС-автомат, достаточно, таким образом, построить по автомату A алфавитный НРС-автомат (по теореме 6.2.7, п.1) и применить потом метод 6.2.9.

2. С практической точки зрения не всегда целесообразно при построении РС-автомата, который должен допускать определенное множество, сначала просто строить НРС-автомат, а потом применять метод из данного раздела. Этот метод очень трудо-

емок и может привести к построению слишком больших (по числу состояний) автоматов. Часто бывает возможно прямо при построении НРС-автомата использовать некоторые специальные свойства рассматриваемого множества, чтобы уже на первом шаге получить небольшой и «почти детерминированный» НРС-автомат. На это рекомендуется обратить внимание при выполнении упражнения 6.3.

6.3. МИНИМИЗАЦИЯ ДЕТЕРМИНИРОВАННЫХ АВТОМАТОВ

Как и в случаях рассмотренных выше типов автоматов, может встретиться ситуация, когда два состояния НРС-автомата имеют одинаковые реакции (см., скажем, пример 5.6.2). Поэтому, как и раньше, необходимо ответить на вопросы: что собой представляет «наименьший» автомат с заданной реакцией? Как его построить? Однозначно ли он определен?

Для РС- и ДРС-автоматов ответы на эти вопросы легко можно получить по аналогии или на базе полученных выше результатов. В случае же НРС-автоматов возникают сложные проблемы.

Поскольку НРС-автоматы с пустой реакцией неинтересны с точки зрения минимизации, неалфавитные НРС-автоматы являются просто сокращенными представлениями алфавитных и спонтанные переходы могут быть исключены без изменения числа состояний, то с настоящего момента мы будем считать выполненным **общее предположение:** все рассматриваемые ниже НРС-автоматы побуквенные и имеют непустую реакцию.

НЕКОТОРЫЕ ПОНЯТИЯ И РЕЗУЛЬТАТЫ, КАСАЮЩИЕСЯ РАЗРЕШИМОСТИ

Определение 6.3.1. 1. Пусть z — состояние и Z'—некоторое подмножество множества состояний НРС-автомата A.

Символом $L(A, z)$ будем обозначать реакцию состояния z (см. п.1 определения 5.6.3).

Реакцией множества состояний Z' называется совокупность реакций состояний, входящих в Z', т. е.

$$L(A, Z') = \cup\{L(A, z) \mid z \in Z'\}.$$

Два состояния или два множества состояний автомата A называются *эквивалентными*, если их реакции равны.

НРС-автомат называется *сокращенным,* если он инициально связен и никакие его два различных состояния не эквивалентны.

2. Пусть A' — еще один НРС-автомат в обычных обозначениях.

Автоматы A и A' называются *локально эквивалентными,* если множества реакций их состояний равны, т. е. если

$$\{L(A, z) \mid z \in Z\} = \{L(A', z') \mid z' \in Z'\}.$$

Автоматы A и A′ называются *изоморфными*, если они совпадают с точностью до обозначения состояний, т. е. если существует биекция b из Z на Z′ со свойствами $b(S)=S'$, $b(F)=F'$, $(z, w, z_1)\in\tau$ тогда и только тогда, когда $(b(z), w, b(z_1))\in\tau'$, — для всех z и z_1 из Z и всех w из F(X). Такая биекция b называется *изоморфизмом* A на A′.

3. Автомат A называется *N-минимальным* (*D-минимальным*, *минимальным*), если не существует эквивалентного автомату A НРС-автомата (ДРС-автомата, РС-автомата соответственно) с меньшим, чем у A, числом состояний.

Замечания. 1. Реакцией НРС-автомата является, таким образом, реакция множества его начальных состояний.

2. Сокращенный НРС-автомат может иметь не более одного избыточного состояния.

3. Локально эквивалентные НРС-автоматы эквивалентны.

Поскольку вопрос об эквивалентности НРС-автоматов разрешим (см. теорему 5.5.9, п.1), немедленно получаем следующую теорему.

Теорема 6.3.2. Разрешимы следующие вопросы.

1. Являются ли два состояния или два множества состояний некоторого НРС-автомата эквивалентными?

2. Является ли данный НРС-автомат сокращенным или нет?

3. Являются ли два данных НРС-автомата локально эквивалентными?

4. Является ли данный НРС-автомат N-минимальным (или D-минимальным, или минимальным)?

Доказательство. 1. Пусть A — НРС-автомат, а Z_1 и Z_2 — подмножества множества Z. Z_1 и Z_2 эквивалентны тогда и только тогда, когда НРС-автоматы $A_i=(Z, X, t, Z_i, F)$, $i=1, 2$, эквивалентны. Поэтому можно использовать п.1 теоремы 5.5.9 (см. также упражнения 6.4 и 6.5).

Пункты 2 и 3 вытекают непосредственно из п.1.

4. Пусть A — НРС-автомат с n состояниями. Чтобы выяснить, является ли A N-минимальным, возьмем множество $\{z_1, ..., z_{n-1}\}$ и для каждого множества $Z_i=\{z_1, ..., z_i\}$ при $i=1, 2, ..., n-1$ построим все возможные НРС-автоматы, имеющие Z_i множеством состояний и X множеством входов. Эта процедура порождает конечное множество НРС-автоматов, для каждого из которых на основе п.1 теоремы 5.5.9 может быть решен вопрос об эквивалентности автомату A. Если один из этих автоматов эквивалентен A, то A не N-минимален. Аналогично можно поступить и в случае ДРС или РС-автоматов. Очевидно, каждый НРС-автомат с не более чем n—1 состояниями эквивалентен одному из построенных выше НРС-автоматов с n—1 состоянием. ■

ПОСТРОЕНИЕ МИНИМАЛЬНОГО РС-АВТОМАТА

Существенной частью способа построения минимального РС-автомата, как и в случае автоматов Мили и Мура, является метод определения классов эквивалентных состояний (впрочем, прежде

всего должны быть исключены все недостижимые состояния). Минимальный РС-автомат при известных классах эквивалентных состояний строится с помощью выбора в качестве состояний классов эквивалентных состояний и переноса функции переходов на эти классы, как и в случае построения экспоненциального автомата (см. упражнение 6.4, п.1).

Используя следствия 5.4.6 и равносильность автоматов Мили и Мура, можно перенести методы, рассмотренные в разд. 2.4 и 2.5 на случай РС-автоматов (см. упражнение 6.4, пп. 2 и 3). Ниже будет представлен метод, являющийся компромиссом между этими двумя методами: он, вообще говоря, менее трудоемок, чем первый, но более трудоемок, чем второй; в то же время при реализации этого метода нужна память бо́льшая, чем в обоих предыдущих случаях.

Пусть рассматриваемый РС-автомат A имеет n состояний, причем все эти состояния достижимы. Метод состоит в построении ориентированного графа, вершинами которого являются все двухэлементные подмножества множества состояний автомата A [их $\frac{1}{2}n(n-1)$], ребра которого соответствуют парам переходов, а каждая вершина окрашена в белый или черный цвет. После применения метода в черный цвет оказываются окрашенными в точности те вершины, которые отвечают парам неэквивалентных состояний.

Метод 6.3.3 (определение всех пар эквивалентных состояний инициально связного РС-автомата с m входами и n состояниями).

Начальный этап. Образовать вершины $\{z, z'\}$ с $z \neq z'$ при $z, z' \in Z$ и окрасить все вершины $\{z, z'\}$ с $z \in F$ и $z' \notin F$ в черный цвет.

Построение окрашенного графа. До тех пор, пока существует хотя бы одна неокрашенная вершина, делать следующее.

1. Выбрать произвольную неокрашенную вершину и окрасить ее в белый цвет.

2. Для каждого $x \in X$ проверить, если $f(z, x) \neq f(z', x)$, окрашена ли вершина $\{f(z, x), f(z', x)\}$ в черный цвет.

1) Если эта вершина не окрашена в черный цвет, то провести в графе направленное ребро из $\{f(z, x), f(z', x)\}$ в $\{z, z'\}$.

2) Если эта вершина окрашена в черный цвет, то окрасить вершину $\{z, z'\}$ и все достижимые из нее вершины (т. е. те, в которые ведут направленные пути) также в черный цвет. При этом удалить все ребра, начала и концы которых окрашены в черный цвет.

После выполнения метода все пары эквивалентных состояний автомата A соответствуют всем вершинам, окрашенным в белый цвет.

Доказательство корректности. Цикл «до тех пор, пока» выполняется конечное число раз, так как каждая вершина

не более одного раза может быть окрашена в белый и не более одного раза в черный цвет.

Необходимо теперь доказать следующие два утверждения.

1. Если вершина $\{z, z'\}$ окрашена (в результате выполнения метода) в черный цвет, то состояния z и z' не эквивалентны.

2. Если состояния z и z' не эквивалентны, то в результате выполнения метода вершина $\{z, z'\}$ будет окрашена в черный цвет.

Чтобы доказать это, убедимся, что при начале и после выполнения каждого цикла «до тех пор, пока» (следовательно, и после всех выполнений цикла) истинны утверждения 1, 2′ и 3 (см. ниже).

2′. Если состояния p и q не эквивалентны и вершина $\{p, q\}$ не окрашена в черный цвет, то существуют $x \in X$, $w \in F(X)$ и не окрашенная вершина $\{z, z'\}$ такие, что $f^*(p, w) = z$, $f^*(q, w) = z'$, а также существует вершина $\{f(z, x), f(z', x)\}$, причем она окрашена в черный цвет.

3. Если существует (направленный) путь из вершины $\{z, z'\}$ в вершину $\{p, q\}$, то существует и $u \in F(X)$ такое, что $\{z, z'\} = \{f^*(p, u), f^*(q, u)\}$.

1) Рассмотрим прежде всего ситуацию, возникающую после начального этапа, т. е. при входе в цикл.

Если $p \in F$ и $q \notin F$, то $\Lambda \in L(A, p)$, но $\Lambda \notin L(A, q)$, так что состояния p и q в таком случае не эквивалентны. Утверждение 1 выполнено.

Если, с другой стороны, p и q не эквивалентны и вершина $\{p, q\}$ не окрашена в черный цвет, то существует слово $w' \neq \Lambda$ такое, что $w' \in L(A, p) \cup L(A, q)$, но $w' \notin L(A, p) \cap L(A, q)$.

Пусть w_0' — одно из таких слов минимальной длины. Тогда существует $w \in F(X)$ и $x \in X$ такие, что $w_0' = wx$, и для $z = f^*(p, w)$ и $z' = f^*(q, w)$ выполнены условия: $z \neq z'$ и $\{z, z'\} \subseteq F$ или $\{z, z'\} \subseteq Z - F$ и, скажем, $\bar{z} = f(f^*(p, w), x) = f^*(p, w_0') \in F$ и $\bar{z}' = f(f^*(q, w), x) = f^*(q, w_0') \notin F$.

Тогда на начальном этапе вершина $\{\bar{z}, \bar{z}'\}$ будет окрашена в черный цвет, а вершина $\{z, z'\}$ (существующая) не будет окрашена. Так что при входе в цикл будет выполнено и утверждение 2′.

Истинность утверждения 3 после выполнения начального этапа очевидна.

2) Рассмотрим теперь ситуацию, возникающую после очередного выполнения цикла, считая, что перед началом его выполнения утверждения 1, 2′ и 3 были истинны.

Рассмотрим утверждение 1. Некоторая вершина $\{p, q\}$ при выполнении цикла окрашивается в черный цвет, если существует вершина $\{z, z'\}$ такая, что вершина $\{f(z, x), f(z', x)\}$ уже окрашена в черный цвет, и если, кроме того, существует путь из $\{z, z'\}$ в $\{p, q\}$, т. е. если по утверждению 3 существует слово $u \in F(X)$ такое, что $\{z, z'\} = \{f^*(p, u), f^*(q, u)\}$. При этом допускается, что $u = \Lambda$, т. е. что $\{z, z'\} = \{p, q\}$.

Если бы состояния z и z′ были эквивалентны, то и состояния f(z, x) и f(z′, x) должны были бы быть эквивалентны.

Если бы p и q были эквивалентны, то и состояния f*(p, u) и f*(q, u) тоже должны были бы быть эквивалентны.

Из сказанного вытекает истинность утверждения 1.

Рассмотрим утверждение 2′. Пусть состояния p и q не эквивалентны, а вершина {p, q} после рассматриваемого выполнения цикла осталась не окрашенной в черный цвет. Тогда существует непустое слово w такое, что существует окрашенная в черный цвет вершина E={f*(p, w′), f*(q, w′)}. Действительно, в п. 1) доказательства было показано, что имеется по меньшей мере одно слово w′∈F(X), при котором |E∩F|=1, так что E оказывается окрашенной в черной цвет уже на начальном этапе.

Пусть w′ — одно из слов с описанным выше свойством, причем минимальной длины. Тогда существуют w∈F(X) и x∈X такие, что w′=wx, вершина {z, z′}={f*(p, w), f*(q, w)} существует и не окрашена в черный цвет, а вершина E={f(z, x), f(z′, x)} — окрашена в черный цвет.

Если бы вершина {z, z′} была окрашена в белый цвет, то это означало бы, что она была выбрана при рассматриваемом или при одном из предыдущих выполнений цикла, но тогда она должна бы была быть окрашена в черный цвет, поскольку E окрашена в черный цвет. Итак, вершина {z, z′} не окрашена и утверждение 2′ выполнено.

Рассмотрим утверждение 3. Пусть {p, q} и {p′, q′} — вершины графа такие, что существует путь из {p, q} в {p′, q′}. Нам следует рассмотреть только случай, когда этот путь возник в результате того, что на шаге 2 при некотором x из X было добавлено ребро, ведущее из {f(z, x), f(z′, x)} в {z, z′}. В этом случае можно предположить, что существуют слова u, v∈F(X) такие, что u соответствует пути из {p, q} в {f(z, x), f(z′, x)}, а v — пути из {z, z′} в {p′, q′}, т. е. что {f*(f(z, x), u), f*(f(z′, x), u)}={p, q} и {f*(p′, v), f*(q′, v)}={z, z′}.

Отсюда вытекает равенство {f*(p′, vxu), f*(q′, vxu)} = = {p, q}, т. е. утверждение 3 остается верным.

3) В момент выхода из цикла больше не остается неокрашенных вершин, так что из 2′ тогда вытекает 2). Итак, доказано, что в момент окончания работы утверждения 1 и 2 истинны. ■

Теорема 6.3.4. При применении метода 6.3.3 необходимы c_1mn^2 ячеек памяти, а число актов выбора вершин графа (обращений к памяти) ограничено величиной c_2mn^2.

Доказательство. Место в памяти необходимо для записи вершин графа и для записи не более чем по m ребер для каждой вершины.

На начальном этапе порождаются $\frac{1}{2}n(n-1)$ вершин.

Суммируя по всем выполнениям цикла «до тех пор, пока», получаем следующие оценки максимального числа актов выбора:

на шаге $1-\frac{1}{2}n^2$ актов выбора;

на шаге $2-\frac{1}{2}mn^2$ актов выбора при проверке, окрашена ли вершина $\{f(z, x), f(z', x)\}$ в черный цвет;

$\frac{1}{2}mn^2$ обращений к памяти при построении ребер, проходящих из $\{f(z, x), f(z', x)\}$ в $\{z, z'\}$, или при окрашивании вершин $\{z, z'\}$ и достижимых из них вершин, а также при удалении ведущих в них ребер, поскольку каждая вершина может быть лишь однажды окрашена в черный цвет и в графе всегда имеются лишь ребра, ведущие в неокрашенные в черный цвет вершины. ■

Другие применения данного метода содержатся в упражнениях 6.4, пп. 4, 5 и 6.5; читателю рекомендуется также выполнить упражнение 6.4, п.6.

МИНИМАЛЬНЫЕ РС-АВТОМАТЫ И D-МИНИМАЛЬНЫЕ ДРС-АВТОМАТЫ

Для РС-автоматов из теоремы 6.2.4 и теоремы об однозначности минимального автомата Мура (теорема 3.6.4) на основании следствия 5.4.6 непосредственно вытекает следующая теорема (см. также упражнения 6.4, 6.6 и 6.7).

Теорема 6.3.5 (теорема об однозначности минимального РС-автомата). РС-автомат является минимальным тогда и только тогда, когда он сокращенный. Любые два эквивалентных минимальных РС-автомата изоморфны и локально эквивалентны. Таким образом, для каждого РС-автомата A существует единственный с точностью до изоморфизма эквивалентный РС-автомат, называемый *минимальным для* A; этот автомат может быть построен эффективным образом.

Доказательство. Достаточно показать, что изоморфные НРС-автоматы A и A′ локально эквивалентны.

Итак, пусть b — изоморфизм, заданный в п.2 определения 6.3.1. Нам необходимо показать, что состояния z и $b(z)$ имеют одинаковые реакции. Поскольку обратное отображение b^{-1} A′ на A является изоморфизмом, то достаточно доказать, что $L(A, z)\subseteq L(A', b(z))$.

Допустим, что $w\in L(A, z)$, где $w=x_1x_2, \ldots, x_n$, $n\geqslant 0$, $x_i\in X\cup\Lambda$.

Тогда существуют состояния $z_0, z_1, \ldots, z_n$ из Z такие, что $z_0=z$, $z_n\in F$ и $(z_{i-1}, x_i, z_i)\in\tau$ при $i=1, \ldots, n$. Поэтому $b(z_n)\in F'$ и $(b(z_{i-1}), x_i, b(z_i))\in\tau'$ при $i=1, \ldots, n$, так что $w\in L(A', b(z))$. ■

Замечания. Мы показали, что изоморфные НРС-автоматы локально эквивалентны, а потому и просто эквивалентны. С помощью аналогичных рассуждений можно показать, что неизбыточные сокращенные локальные эквивалентные ДРС-автоматы изоморфны — в качестве подходящей биекции достаточно выбрать отображение, при котором образом состояния одного авто-

мата оказывается состояние другого автомата, имеющее ту же реакцию.

Результат для случая ДРС-автоматов может быть получен из результата для полностью определенных автоматов еще проще, чем при рассмотрении частичных автоматов Мили, — достаточно ввести дополнительное поглощающее состояние (ср. п.2 теоремы 6.2.7).

Следствие 6.3.6 (однозначность минимального ДРС-автомата). ДРС-автомат является D-минимальным тогда и только тогда, когда он является сокращенным и неизбыточным. Любые два эквивалентных D-минимальных ДРС-автомата изоморфны и локально эквивалентны. Таким образом, для каждого ДРС-автомата A существует единственный с точностью до изоморфизма эквивалентный D-минимальный ДРС-автомат, называемый *D-минимальным* для A; этот автомат может быть построен эффективным образом. D-минимальный для A автомат имеет на одно состояние меньше, чем минимальный эквивалентный A РС-автомат A′ тогда и только тогда, когда он не является полностью определенным, т. е. когда автомат A′ избыточный.

Доказательство. Пусть A представляет собой D-минимальный ДРС-автомат, не являющийся полностью определенным. Тогда A неизбыточен, так как в противном случае могли бы быть исключены состояния с пустой реакцией.

Пусть теперь $\bar{A}$ — доопределение автомата A в смысле п.2 доказательства теоремы 6.2.7, т. е. $A=(Z\cup\bar{z}, X, \bar{f}, S, F)$, где $\bar{z}\notin Z$, $f(\bar{z}, x)=\bar{z}$ и

$$\bar{f}(z, x) = \begin{cases} f(z, x), & \text{если это состояние определено,} \\ \bar{z} & \text{в противном случае} \end{cases}$$

при всех x из X и z из Z.

Так как $L(A, \bar{z})=\varnothing$, то $\bar{z}$ не эквивалентно ни одному состоянию z из Z. Далее, любые два состояния z и z′ из Z как состояния автомата Λ не эквивалентны, поскольку в противном случае по теореме 6.3.5 имелся бы локально эквивалентный автомату $\bar{A}$ сокращенный РС-автомат A_0 с меньшим, чем у $\bar{A}$, числом состояний; некоторое состояние автомата A_0 должно было бы иметь такую же реакцию, как и состояние $\bar{z}$, его можно было бы исключить и получить эквивалентный автомату A ДРС-автомат с меньшим, чем у A, числом состояний, чего быть не может.

Итак, автомат A — сокращенный, а вместе с ним — и автомат A.

Пусть, далее, A_1 — некоторый D-минимальный эквивалентный автомату A ДРС-автомат. Если бы автомат A_1 был определен полностью, то по теореме 6.3.5 он был бы эквивалентен автомату $\bar{A}$. Поэтому и автомат A должен был бы быть определен полностью, так как иначе A_1 имел бы на одно состояние (с пустой реакцией) больше, чем автомат $\bar{A}$. Итак, автомат A_1 определен не полностью.

Построим теперь доопределение $\bar{A}_1$ автомата A_1. По теореме 6.3.5 автоматы $\bar{A}_1$ и $\bar{A}$ изоморфны. Поскольку, как показано в доказательстве теоремы 6.3.5, любые два состояния, отображающиеся одно на другое при изоморфизме $\bar{A}$ на $\bar{A}_1$, имеют одинаковые реакции, то и автоматы $\bar{A}$ и A_1 изоморфны — сужение рассматриваемого изоморфизма на множество Z является изоморфизмом A на A_1.

Ясно, что в данном случае A и A_1 локально эквивалентны.

Если, наконец, A_2 — не полностью определенный неизбыточный сокращенный и эквивалентный автомату A ДРС-автомат, то автомат $\bar{A}_2$ тоже сокращенный, так что A_2 изоморфен и локально эквивалентен автомату A.

Далее, мы уже видели, что если D-минимальный ДРС-автомат A′ определен полностью, то и все эквивалентные ему D-минимальные автоматы тоже определены полностью. Аналогичное высказывание верно и для неизбыточных сокращенных ДРС-автоматов. Таким образом, в этих случаях может быть использована теорема 6.3.5.

Оставшаяся часть утверждения теоремы вытекает из того, что D-минимальные РС-автоматы являются неизбыточными. ■

Замечание. Из теорем 5.5.3 и 6.2.8 вытекает, что для каждого НРС-автомата существуют единственные с точностью до изоморфизма минимальный РС-автомат и D-минимальный ДРС-автомат.

ОПТИМАЛЬНОСТЬ КОНСТРУКЦИИ ЭКСПОНЕНЦИАЛЬНЫХ АВТОМАТОВ

Теперь будет показано, что для каждого $n \geqslant 2$ существует по меньшей мере один НРС-автомат A_n с n состояниями такой, что минимальный эквивалентный автомату A_n РС-автомат имеет 2^n состояний (об этом уже говорилось в разд. 6.2).

Метод, используемый в доказательстве этой теоремы, рекомендуется применить при выполнении пп. 2—4 упражнения 6.1.

Теорема 6.3.7. При каждом $n \geqslant 2$ применение метода построения экспоненциального автомата к описанному ниже автомату A_n приводит к построению минимального РС-автомата:

$A_n = (\{1, 2, ..., n\}, \{a, b\}, t, \{1\}, \{n\})$, где

$t(i, a) = \{i+1\}$ при $i = 1, 2, ..., n-1$,

$t(n, a) = \{1, 2\}$, $t(1, b) = \{1\}$, $t(i, b) = \{i+1\}$ при $i = 2, 3, ...$ $..., n-1$, $t(n, b) = \varnothing$.

Доказательство. Покажем, что экспоненциальный автомат A_{np} для A_n является сокращенным.

Промежуточное утверждение 1. Состояния P и Q автомата A_{np} эквивалентны тогда и только тогда, когда они равны как подмножества множества $\{1, ..., n\}$.

Доказательство. Из $P=Q$ вытекает, конечно, эквивалентность P и Q. Пусть $P\neq Q$. Тогда существует i такое, что $i\in P\cup Q$ и $i\notin P\cap Q$. Пусть, скажем, $i\in Q$. Если $i\geqslant 2$, то $\{n\}=t^*(i, a^{n-i})$ и $n\notin t^*(j, a^{n-i})$ при любом $j\neq i$, так что $n\in t^*(Q, a^{n-i})$ и $n\notin t^*(P, a^{n-i})$. Если же $i=1$, то $n\in t^*(Q, ba^{n-1})$ и $n\notin t^*(P, ba^{n-1})=\varnothing$. Итак, в обоих случаях состояния P и Q не эквивалентны.

Промежуточное утверждение 2. A_{np} инициально связен.

Доказательство. Пусть $Q=\{i_1, \ldots, i_r\}$ при $1\leqslant i_1\leqslant i_2\leqslant \ldots \leqslant i_r\leqslant n$ — произвольное состояние автомата A_{np}.

Построим состояние $P=\{j_3, j_4, \ldots, j_r, n\}$, которое имеет (как множество) на один элемент меньше, чем Q, и из которого при определенном входном слове w автомат A_{np} переходит в состояние Q: пусть $j_k=i_k-i_2+1$ при $k=3, 4, \ldots, r$, $d=i_2-i_1$ и $w=ab^{d-1}a^{i_1-1}$; тогда $t^*(j_k, w)=\{j_k+1+d-1+i_1-1\}=\{i_k\}$ при $k=3, \ldots, r$ и $t^*(n, w)=t^*(\{1, 2\}, b^{d-1}a^{i_1-1})=t^*(\{1, d+1\}, a^{i_1-1})=\{i_1, i_2\}$, так что $Q=t^*(P, w)$.

Поскольку каждое одноэлементное состояние $\{i\}$ автомата A_{np} на основании равенства $\{i\}=t^*(1, a^{i-1})$ достижимо, то из сказанного полной индукцией по числу элементов состояний автомата A_{np} получаем, что A_{np} — инициально связный автомат. ■

6.4. ПРОБЛЕМА МИНИМИЗАЦИИ ДЛЯ НРС-АВТОМАТОВ

Теперь должна быть решена *проблема минимизации для НРС-автоматов,* т. е. должны быть получены ответы на следующие вопросы.

1. Существует ли для каждого НРС-автомата эквивалентный N-минимальный НРС-автомат?

2. Определены ли N-минимальные НРС-автоматы однозначно (с точностью до изоморфизма), т. е. изоморфны ли эквивалентные N-минимальные НРС-автоматы?

3. Существуют ли свойства НРС-автоматов, характеризующие N-минимальные НРС-автоматы (аналогично тому, как свойство сокращенности характеризует минимальные РС-автоматы)?

4. Существуют ли регулярные методы построения эквивалентного произвольно заданному НРС-автомату N-минимального НРС-автомата?

Мы не можем действовать так же, как в случае частичных автоматов Мили, поскольку в данной ситуации мы не имеем в своем распоряжении понятия покрытия. Только некоторые результаты (прежде всего — отрицательные) аналогичны результатам, полученным для частичных автоматов Мили.

Важную роль в построении НРС-автоматов с насколько возможно малым числом состояний и в рассматриваемых ниже примерах играют зеркальные автоматы, определенные в доказательстве теоремы Клини (теорема 5.3.5).

Ответы на вопросы 1 и 2 могут быть получены довольно легко, полные ответы на вопросы 3 и 4 ниже получены не будут.

Теорема 6.4.1. 1. Для каждого НРС-автомата эффективным образом может быть построен эквивалентный N-минимальный НРС-автомат. Каждый N-минимальный НРС-автомат является неизбыточным и сокращенным. НРС-автомат, зеркальный для N-минимального НРС-автомата, также является N-минимальным.

2. Пусть A — НРС-автомат, A_1 — эквивалентный автомату A D-минимальный ДРС-автомат и A_2 — эквивалентный автомату A НРС-автомат, для которого зеркальный автомат является D-минимальным ДРС-автоматом. Тогда числа состояний автоматов A_1 и A_2 не обязательно равны между собой и эти автоматы не обязательно являются N-минимальными.

3. Существуют D-минимальные ДРС-автоматы, которые хотя и эквивалентны своим зеркальным автоматам, но не изоморфны или не локально эквивалентны им.

4. Автомат, зеркальный для неизбыточного сокращенного НРС-автомата, может не быть сокращенным.

Доказательство. 1. а) Способ (очень трудоемкий и требующий чрезвычайно большого времени) построения N-минимального НРС-автомата, эквивалентного данному НРС-автомату A, состоит в применении метода из доказательства п.4 теоремы 6.3.2. Если Z — множество состояний и X — множество входов автомата A, то следует построить для каждого собственного подмножества Z' множества Z все НРС-автоматы, имеющие Z' множеством состояний и X множеством входов, и проверить, эквивалентны ли они (каждый в отдельности) автомату A. Число таких автоматов A' по сделанному ранее общему предположению, конечно, а каждый НРС-автомат с входным множеством X и менее чем с $n=|Z|$ состояниями изоморфен какому-либо из этих автоматов A'. Итак, либо сам автомат A является N-минимальным, либо один из построенных автоматов A' эквивалентен автомату A и N-минимален.

б) Пусть теперь A представляет собой N-минимальный НРС-автомат. Тогда A по теореме 6.2.4 неизбыточен и инициально связен.

1) Допустим, что автомат A не является сокращенным. Тогда должны иметься по меньшей мере два различных эквивалентных состояния z' и z'' автомата A. Если бы это действительно было так, то автомат A мог бы быть сокращен. Для доказательства этого построим новый НРС-автомат $A'=(Z', X, t', S', F')$, отбрасывая состояние z'' и заменяя во всех переходах z'' на z' (т. е. объединяя z' и z'' в одно состояние). При этом можно считать, что z'' не принадлежит множеству начальных состояний S, если S одноэлементно. Итак, положим $Z'=Z-z''$, $S'=S-z''$, $F'=F-z''$, $\tau'=\{(\bar{z}_1, w, \bar{z}_2) \mid (z_1, w, z_2)\in\tau\}$, где

$$\bar{z}_i = \begin{cases} z_i, & \text{если } z_i \neq z'', \\ z', & \text{если } z_i = z'' \end{cases}$$

при i=1, 2.

Промежуточное утверждение. Автомат A' эквивалентен автомату A.

Доказательство. Поскольку при объединении состояний z' и z'' возникает, вообще говоря, больше возможностей для перехода из некоторого начального в некоторое финальное состояние, то $L(A) \subseteq L(A')$.

Пусть $u \in L(A')$. Тогда существуют натуральное число n, состояния $z_0, z_1, \ldots, z_n$ из Z' и слова $w_1, \ldots, w_n$ из $X \cup \Lambda$ такие, что $z_0 \in S'$, $z_n \in F'$, $w_1 w_2 \ldots w_n = u$ и $(z_{i-1}, w_i, z_i) \in \tau'$ при $i = 1, \ldots, n$.

Пусть, далее, $u_j = w_{j+1} w_{j+2} \ldots w_n$ при $j = 0, 1, \ldots, n$ (так что $u_n = \Lambda$).

Если бы слово u не принадлежало $L(A)$, то включения $u_j \in L(A, z_j)$ не могли бы выполняться при всех $j = 0, 1, \ldots, n$. Пусть k — минимальное число такое, что $u_k \in L(A, z_k)$. Тогда переход (z_{k-1}, w, z_k) не может принадлежать τ, так как иначе слово $u_{k-1} = w_k u_k$ принадлежало бы $L(A, z_{k-1})$, что противоречит минимальности числа k. Это означает, что не могут одновременно выполняться соотношения $z_{k-1} \neq z'$ и $z_k \neq z'$.

Пусть, например, $z_{k-1} = z_k = z'$ и $(z', w_k, z') \in \tau$. Тогда по построению $(z', w_k, z'') \in \tau$, или $(z'', w_k, z'') \in \tau$, или $(z'', w_k, z') \in \tau$, и вследствие эквивалентности z' и z'' слово u_k принадлежит $L(A, z'')$. Поэтому $u_{k-1} = w_k u_k$ принадлежит $L(A, z'') = L(A, z') = L(A, z_{k-1})$, что противоречит минимальности числа k.

Аналогичным образом и предположения $z_{k-1} = z'$ и $z_k \neq z'$ или $z_{k-1} \neq z'$ и $z_k = z'$ приводят к противоречию, так что гипотеза о том, что u не принадлежит $L(A)$, ложна.

Итак, A и A' эквивалентны.

То, что автомат A' имеет меньше состояний, чем A, противоречит предположению о N-минимальности A. Итак, автомат A должен быть сокращенным.

2) Предположение: автомат $\tilde{A}$ не N-минимален. Тогда существует эквивалентный автомату $\tilde{A}$ НРС-автомат A' с меньшим, чем у $\tilde{A}$, числом состояний. Поэтому автомат, зеркальный для A', эквивалентен автомату A и имеет меньшее, чем у A, число состояний. Это противоречит предположению о N-минимальности автомата A.

2. Для доказательства рассмотрим НРС-автоматы A, A_1 и A_2, заданные графами, изображенными на рис. 6.4.1—6.4.3.

Очевидно, что A_1 и $\tilde{A}_2$ — ДРС-автоматы. На основании следствия 6.3.6 нам необходимо только показать, что автоматы A_1 и $\tilde{A}_2$ — неизбыточные и сокращенные и что автомат A_1 эквивалентен автомату A, а A_2 — автомату $\tilde{A}$.

В качестве доказательства приведем реакции отдельных состояний:

$L(A_1, 1) = a^*$, $L(A_1, 2) = ba^*$,

$L(A_1, 3) = \Lambda$, $L(A_1, 4) = a^*b$,

$L(A_1, 5) = \Lambda \cup b \cup aa^*b = \Lambda \cup a^*b$,

$L(A_1, 6) = b \cup aL(A_1, 5) = b \cup a \cup aa^*b = a \cup a^*b$,

$L(A_1, 7) = aL(A_1, 6) \cup bL(A_1, 2) = a^2 \cup aa^*b \cup b^2a^* = L(A)$,

$L(\tilde{A}_2, 1) = a^*$, $L(\tilde{A}_2, 2) = aa^* \cup b$,

$L(\tilde{A}_2, 3) = \Lambda$, $L(\tilde{A}_2, 4) = b$,

$L(\tilde{A}_2, 5) = a^*b^2$, $L(\tilde{A}_2, 6) = \Lambda \cup aa^*b^2 \cup b^2 = \Lambda \cup a^*b^2$,

$L(\tilde{A}_2, 7) = aL(\tilde{A}_2, 6) \cup b^2 = a \cup aa^*b^2 \cup b^2 = a \cup a^*b^2$,

$L(\tilde{A}_2, 8) = bL(\tilde{A}_2, 2) \cup aL(\tilde{A}_2, 7) = baa^* \cup b^2 \cup a^2 \cup aa^*b^2 =$

$= baa^* \cup a^2 \cup a^*b^2 = \overbrace{L(A)} = L(\tilde{A})$.

3. Для доказательства рассмотрим автоматы A_3 и $\tilde{A}_3$, заданные графами, изображенными на рис. 6.4.4.

Нетрудно получить, что $L(A_3) = \{ab, bb, ba\} = L(\tilde{A}_3)$.

Автомат A_3, очевидно, неизбыточный и сокращенный, а потому (см. следствие 6.3.6) и D-минимальный.

Автоматы A_3 и $\tilde{A}_3$ не изоморфны, так как $\tilde{A}_3$ не ДРС-автомат.

Автоматы $\tilde{A}_3$ и $\tilde{A}_3$ также и не локально эквивалентны, поскольку, в частности, ни одно из состояний автомата A_3 не имеет реакции $\{a\}$, которой обладает одно из состояний автомата $\tilde{A}_3$.

4. Для доказательства рассмотрим автоматы A_4 и $\tilde{A}_4$, заданные графами, изображенными на рис. 6.4.5.

Легко видеть, что автомат A_4 — неизбыточный и сокращенный, но автомат $\tilde{A}_4$ — не сокращенный. ■

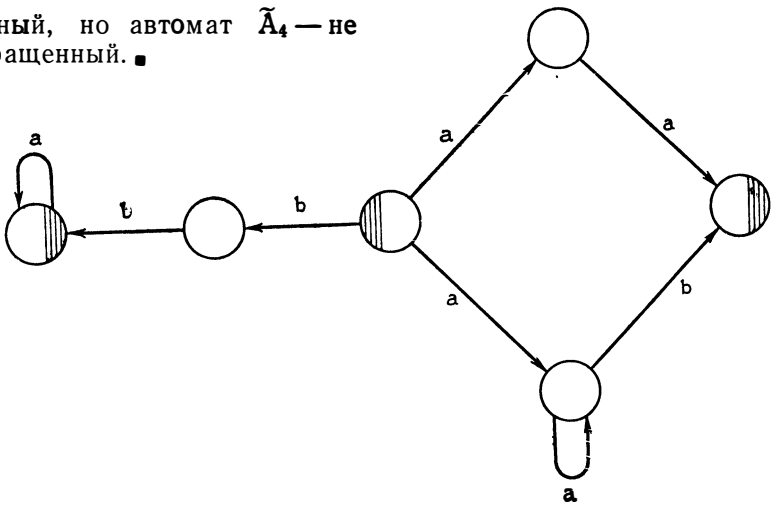


Рис. 6.4.1. НРС-автомат A с $L(A) = b^2a^* \cup a^2 \cup aa^*b$

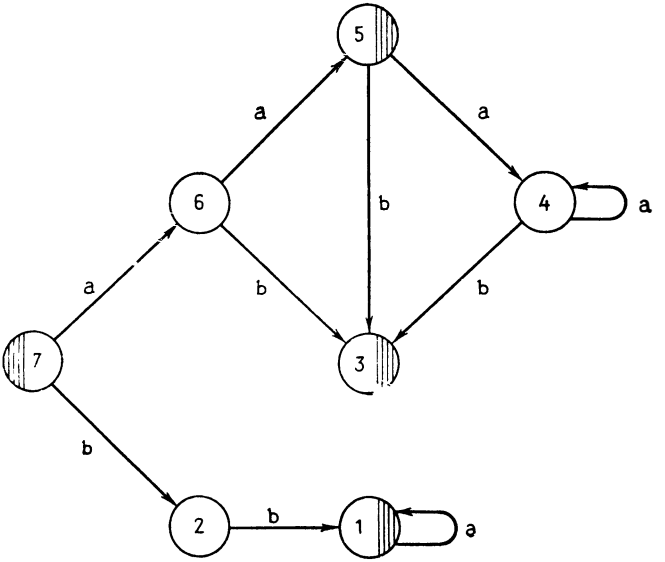


Рис. 6.4.2. Эквивалентный автомату A D-минимальный ДРС-автомат A_1

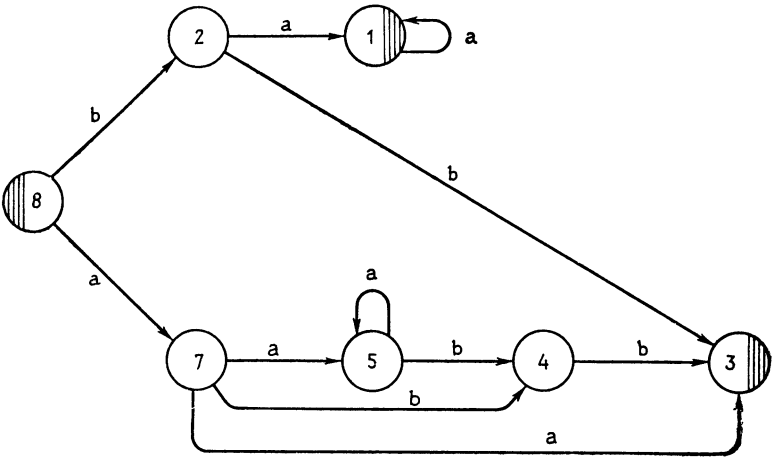


Рис. 6.4.3. Эквивалентный автомату A HPC-автомат A_2, зеркальный для которого автомат является D-минимальным

Замечание. Используя рис. 6.4.4, можно получить, что локально эквивалентные HPC-автоматы не обязательно изоморфны: если изменить граф автомата A_3 на рис. 6.4.4, заменив метку a на ребре, исходящем из начального состояния, на метку a, b, то будет получен граф автомата, локально эквивалентного автомату A_3, но не изоморфного ему.

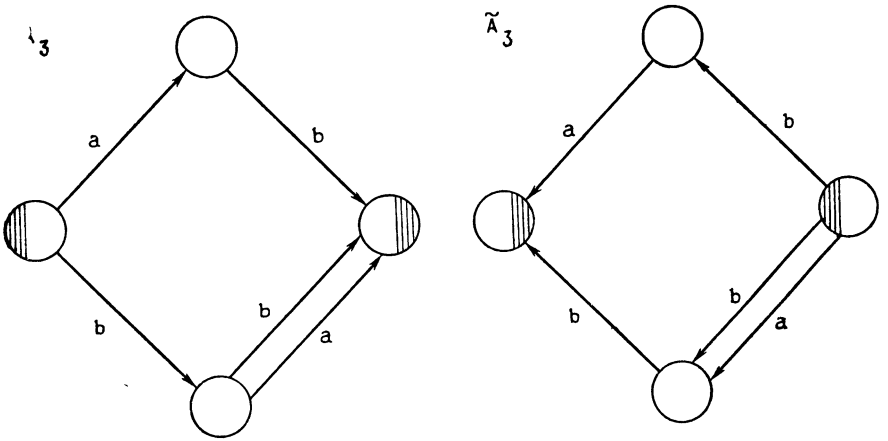


Рис. 6.4.4. D-минимальный ДРС-автомат A_3 эквивалентный, но не локально эквивалентный своему зеркальному автомату

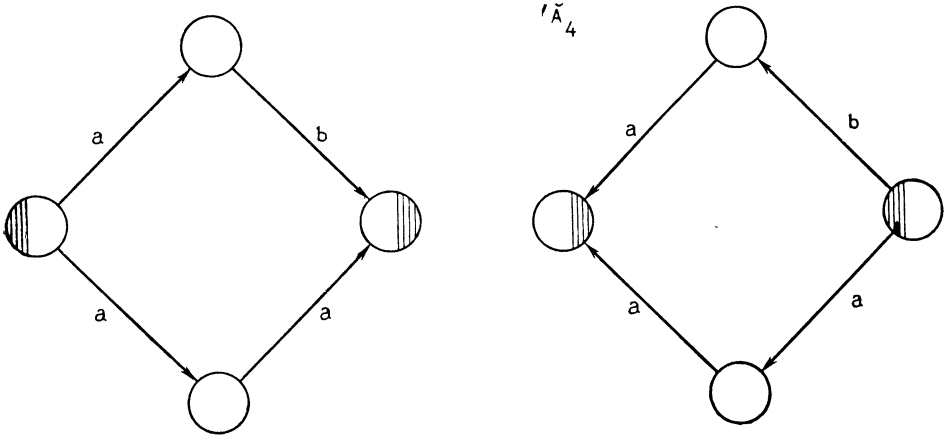


Рис. 6.4.5. Неизбыточный сокращенный НРС-автомат A_4 с несокращенным зеркальным автоматом

СУЩЕСТВОВАНИЕ НЕИЗОМОРФНЫХ ЭКВИВАЛЕНТНЫХ N-МИНИМАЛЬНЫХ НРС-АВТОМАТОВ

Следствие 6.4.2. 1. Минимальный РС-автомат или D-минимальный ДРС-автомат не обязательно является и N-минимальным НРС-автоматом.

2. Если A — неизбыточный сокращенный НРС-автомат, то A может не быть N-минимальным автоматом. Более того, в этом случае может существовать и эквивалентный автомату A ДРС-автомат с меньшим, чем у A, числом состояний.

3. Эквивалентные N-минимальные (или неизбыточные, сокра-

щенные) НРС-автоматы могут не быть ни изоморфными, ни локально эквивалентными.

Доказательство. 1. Автомат A_1, граф которого изображен на рис. 6.4.2, является не полностью определенным D-минимальным ДРС-автоматом, не N-минимальным. Его доопределение $\bar{A}_1$ в смысле доказательства следствия 6.3.6 также не является N-минимальным автоматом.

2. Автомат A_4, граф которого изображен на рис. 6.4.5, является неизбыточным и сокращенным, но не N-минимальным, поскольку автомат, граф которого изображен на рис. 6.4.6, эквивалентен автомату A_4. Этот автомат, более того, оказывается D-минимальным ДРС-автоматом. Его можно получить, производя сокращение автомата $\tilde{A}_4$ и переходя к зеркальному автомату.

3. Автоматы A_3 и $\tilde{A}_3$, графы которых изображены на рис. 6.4.4, эквивалентны, но не локально эквивалентны и не изоморфны. На основании п.1 теоремы 6.4.1 нам остается только показать, что A_3 является N-минимальным автоматом.

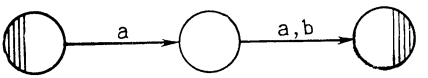


Рис. 6.4.6. Эквивалентный автомату A_4 D-минимальный ДРС-автомат

Допустим, что A — эквивалентный автомату A_3 N-минимальный НРС-автомат. Поскольку множество L(A) конечно, то граф автомата A не может содержать замкнутых путей. Пусть z_0 — некоторое начальное состояние автомата A. Так как $ab \in L(A)$, то A должен иметь состояние $z_1 \neq z_0$ такое, что $(z_0, a, z_1) \in \tau$, и финальное состояние z_2 такое, что $(z_1, b, z_2) \in \tau$, причем $z_0 \neq z_2$ и $z_1 \neq z_2$. Поскольку и $ba \in L(A)$, то у A должны быть состояния z_3, z_4 и z_5 такие, что z_3 — начальное состояние, z_5 — финальное состояние $(z_3, b, z_4) \in \tau$ и $(z_4, a, z_5) \in \tau$.

Если бы выполнялось равенство $z_0 = z_4$ (или $z_1 = z_4$, или $z_2 = z_4$), то было верно и включение $a \in L(A)$ [или $a^2 \in L(A)$, или $b \in L(A)$ соответственно]. Так что автомат A должен иметь по меньшей мере четыре различных состояния: z_0, z_2, z_3 и z_4. Поскольку A_3 имеет только четыре состояния, то он является N-минимальным. ■

6.5. МЕТОДЫ УМЕНЬШЕНИЯ ЧИСЛА СОСТОЯНИЙ

Теорема 6.4.1 и ее доказательство демонстрируют различные возможности, используя которые часто можно для данного НРС-автомата A получить эквивалентный НРС-автомат с меньшим числом состояний.

Метод 6.5.1. 1. Построить эквивалентный автомату A (или $\bar{A}$) D-минимальный автомат A_d (или соответственно ${}_dA$). По теореме 6.4.1, п.2 ${}_dA$ может иметь меньше состояний, чем A_d, а этот автомат может иметь меньше состояний, чем A (этого, конечно, может и не быть). Автомат ${}_d\bar{A}$ эквивалентен автомату A.

2. Если автомат A избыточен или не является сокращенным, то построить в соответствии с теоремой 6.4.2 эквивалентный автомату A неизбыточный инициально связный НРС-автомат и провести его сокращение (как описано в подпункте 1) доказательства теоремы 6.4.1, п.1) путем объединения эквивалентных состояний, получив в результате неизбыточный сокращенный НРС-автомат A_1. **Автомат, зеркальный для A_1 может по теореме 6.4.1, п.4** оказаться несокращенным, так что к нему можно применить ту же процедуру и так далее до тех пор, пока не будет получен НРС-автомат A_i такой, что и A_i и $\bar{A}_i$ будут неизбыточными сокращенны-

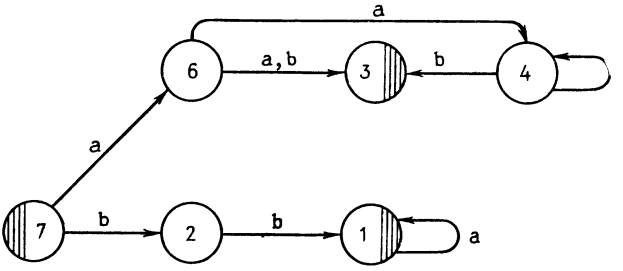


Рис. 6.5.1. Эквивалентный автомату A_1 НРС-автомат

ми НРС-автоматами. Отметим, однако, что A_i все еще может не быть N-минимальным.

Дальнейшие возможности уменьшения числа состояний показаны в следующем примере.

Пример 6.5.2. Доказательство п.2 теоремы 6.4.1 показывает, что число состояний НРС-автомата может быть уменьшено и иным способом.

1. Для автомата A_1, граф которого изображен на рис. 6.4.2, выполняется равенство $L(A_1, 5) = L(A_1, 3) \cup L(A_1, 4)$. Поэтому состояние 5 может быть исключено (*элиминировано*), если все ведущие в это состояние переходы (ребра) «переключить» на состояния 3 и 4. В результате получается эквивалентный автомату A_1 НРС-автомат, граф которого изображен на рис. 6.5.1.

2. Как и у A_1, у автомата $\bar{A}_2$ может быть элиминировано одно состояние, поскольку $L(\bar{A}_2, 6) = L(\bar{A}_2, 3) \cup L(\bar{A}_2, 5)$. Таким образом возникает НРС-автомат A_5, граф которого изображен на рис. 6.5.2.

Поскольку (как можно усмотреть из доказательства п.2 теоремы 6.4.1) ни одно состояние z автомата A_5 не эквивалентно ни одному не содержащему z подмножеству множества состояний автомата A_5, то A_5 не может быть более сокращен при использовании описанных выше средств (заметим, что автомат A_5 — неизбыточный и сокращенный).

В данной ситуации можно использовать новый прием: мы *дополним* рассматриваемый автомат (здесь — A_5), добавляя новые переходы и изменяя множества начальных или финальных состояний, таким образом, чтобы реакция автомата осталась неизмен-

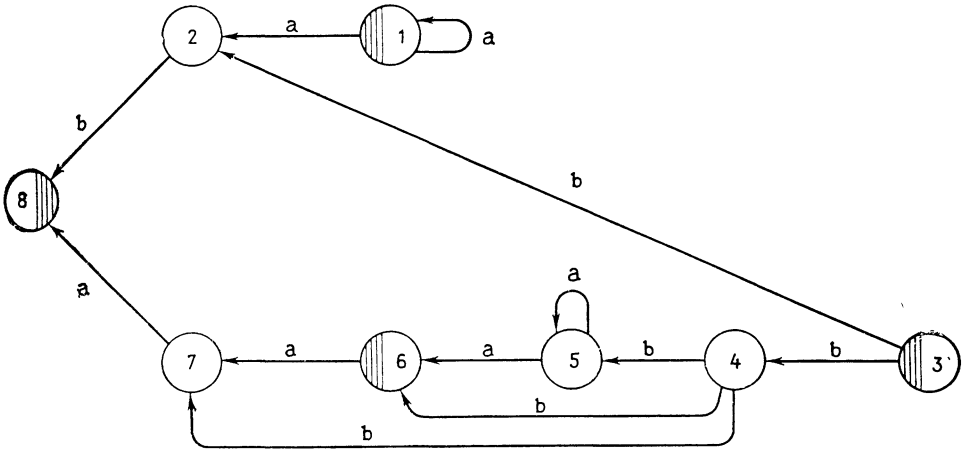


Рис. 6.5.2. Эквивалентный автомату $\tilde{A}_2$ НРС-автомат A_5

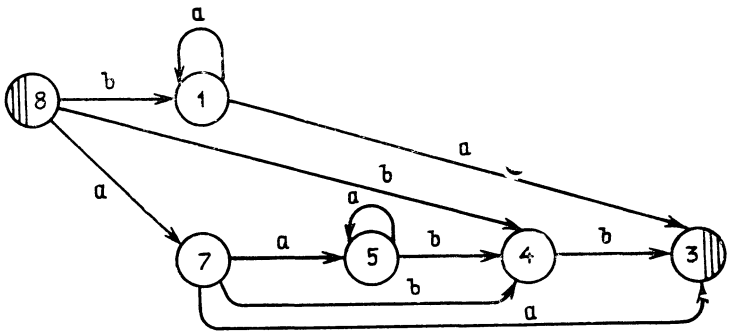


Рис. 6.5.3. Эквивалентный автомату $\tilde{A}_1$ НРС-автомат A_6

ной, и попытаемся после этого элиминировать какое-нибудь из состояний. Добавим, например, в случае автомата A_5 переходы (1, a, 3) и (2, a, 3) и исключим состояние 1 из множества финальных состояний (так что единственным финальным состоянием останется состояние 3). В результате будет получен НРС-автомат A_5' с $L(A_5', 2) = a \cup b \cup aa^*a = b \cup aa^* = L(A_5', 4) \cup L(A_5', 1)$. На основании этого равенства состояние 2 может быть элиминировано и возникнет НРС-автомат A_6, у которого зеркальный автомат эквивалентен автомату A_1. Граф автомата A_6 изображен на рис. 6.5.3.

Нетрудно проверить, что автомат A_6, так же, как и автомат, граф которого изображен на рис. 6.5.1, является N-минимальным. Итак, в данном случае мы с помощью дополнения и элиминации из D-минимальных автоматов A_1 и $\tilde{A}_2$ получили N-минимальные НРС-автоматы (эквивалентные НРС-автомату A, граф которого изображен на рис. 6.4.1).

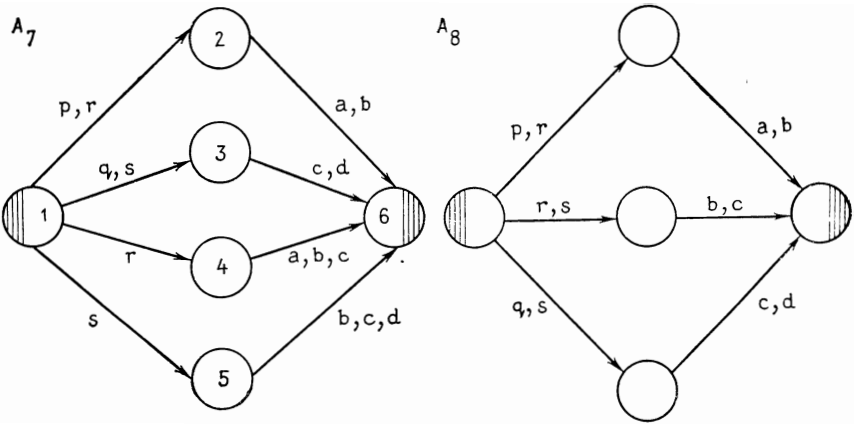


Рис. 6.5.4. Эквивалентные НРС-автоматы A_7 и A_8

Отметим, однако, что таким способом N-минимальный НРС-автомат можно построить не всегда.

3. НРС-автомат A_7, граф которого изображен на рис. 6.5.4, не допускает дополнения в описанном выше смысле и ни одно его состояние не эквивалентно никакому не содержащему это состояние подмножеству множества состояний автомата A_7 (т. е. ни одно состояние не может быть элиминировано). В то же время автомат A_7 не является N-минимальным, поскольку НРС-автомат A_8, граф которого также изображен на рис. 6.5.4, эквивалентен автомату A_7.

В этой ситуации оказывается полезным, как и при минимизации частичных автоматов Мили, *расширение*, т. е. введение нового состояния, реакция которого оказывается подмножеством реакций по меньшей мере двух имеющихся состояний. Это введение осуществляется таким образом, чтобы реакция автомата осталась неизменной. В случае автомата A_7 имеется пересечение {b, c} реакций состояний 4 и 5. Это позволяет построить НРС-автомат A_9, граф которого приведен на рис. 6.5.5. Данный автомат после элиминации состояний 4 и 5 сокращается до автомата A_8.

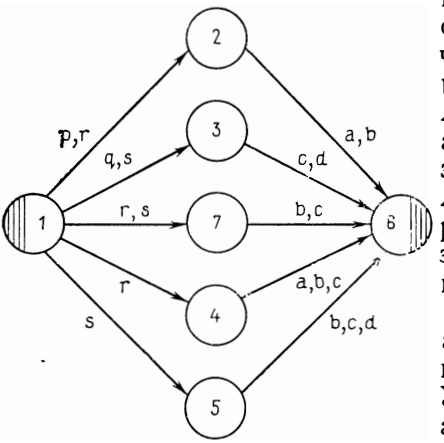


Рис. 6.5.5. Расширение A_9 автомата A_7

4. Для того чтобы перейти от автомата A_7 к автомату A_8, можно использовать и иной способ. У автомата A_7 без изменения реакции могут быть исключены переходы (4, a, 6) и (5, d, 6). В результате возникает несокра-

щенный НРС-автомат, в котором имеющие одинаковые реакции состояния 4 и 5 могут быть объединены в одно состояние, что приводит к построению автомата A_8.

Для более точного и формального ознакомления с построением N-минимальных НРС-автоматов и с используемыми для этого операциями, а именно:

построением эквивалентных (или эквивалентных для зеркальных автоматов) D-минимальных автоматов,

сокращением [способом из доказательства подпункта 1 теоремы 6.4.1, п.1],

элиминацией (как в примере 6.5.2, пп. 1 и 2),

дополнением (как в примере 6.5.2, п. 2),

расширением (как в примере 6.5.2, п. 3),

исключением переходов (как в примере 6.5.2, п. 4)

читателю рекомендуется обратиться к упражнению 6.8 и к указанной в списке литературе.

6.6. ЧАСТНЫЕ И ПРОИЗВОДНЫЕ

Прежде всего мы докажем важную, лежащую в основе всех известных методов минимизации НРС-автоматов, теорему Индермарка, Камеды и Вайнера. При этом существенную роль будет играть понятие левого частного множества по одноэлементному множеству $\{w\}$ (см. определение 5.5.6). Вместо $\{w\}\backslash L$ будем ниже использовать упрощенную запись $w\backslash L$. Для того чтобы сформулировать теорему, нам понадобятся два определения.

Определение 6.6.1. 1. Пусть $M=\{M_1, M_2, \ldots, M_m\}$ и $M'=\{M_1', M_2', \ldots, M_n'\}$ — конечные множества множеств. M *порождает* M' тогда и только тогда, когда каждое множество M_i' при $i=1, \ldots, n$ является объединением некоторых множеств из M:

$$M_i' = M_{j_1} \cup M_{j_2} \cup \ldots \cup M_{j_k},\ \{j_1, \ldots, j_k\} \subset \{1, \ldots, m\},\ i = 1, \ldots, n.$$

2. Пусть A — НРС-автомат. Множество $LL(A)=\{L(A, z) \mid z \in Z\}$, где Z — множество состояний автомата A, называется *локальной реакцией* автомата A.

На основании п.2 определения 6.3.1 два НРС-автомата оказываются, таким образом, эквивалентными тогда и только тогда, когда их локальные реакции равны.

Теорема 6.6.2 (Индермарк, Камеда, Вайнер). 1. Пусть A — НРС-автомат и A_d (или ${}_dA$) — эквивалентный автомату A (соответственно автомату $\bar{A}$) D-минимальный ДРС-автомат. Тогда локальная реакция автомата A (или $\bar{A}$) порождает локальную реакцию автомата A_d (или ${}_dA$).

2. Множество $\{L_1, L_2, \ldots, L_n\}$ подмножеств моноида $F(X)$ является локальной реакцией некоторого НРС-автомата тогда и только тогда, когда оно порождает множество $\{x\backslash L_i \mid x \in X,\ 1 \leqslant i \leqslant n\}$, т. е. когда каждое левое частное любого множества L_i по любому входу x является объединением подходящих множеств L_j.

Доказательство. 1. Пусть $A=(Z, X, t, S, F)$, $A_d=(Z', X, f, s', F')$, $L=L(A)=L(A_d)$ и z' — некоторое состояние автомата A_d. Поскольку автомат A_d инициально связен, то в $F(X)$ существует слово w такое, что $f^*(s', w)=z'$.

Так как автомат A_d D-минимален и на основании общего предположения из разд. 6.3 реакция L не пуста, то и реакция L' состояния z' не пуста. При любом слове v из L' слово wv принадлежит L. Это означает, что выполнено включение $L'\subseteq w\backslash L$.

Если, с другой стороны, $u\in w\backslash L$, то $wu\in L$, а поскольку автомат A_d — побуквенный и детерминированный, то и $u\in L'$.

Итак, $L(A_d, z')=w\backslash L$.

Так как на основании общего предположения из разд. 6.3 автомат A — алфавитный, то для каждого слова v из L' существуют состояние z в Z и начальное состояние s в S такие, что $z\in t^*(s, w)$ и $v\in L(A, z)$. Отсюда, с одной стороны, вытекает включение $wL(A, z)\subseteq L$, т. е. $L(A, z)\subseteq w\backslash L=L'$, и, с другой стороны, вытекает, что каждое слово v из L' принадлежит одному из множеств $L(A, z)$, так что $L'=\bigcup\{L(A, z)\,|\,z\in t^*(s, w), s\in S\}$, т. е. L' является объединением определенных множеств $L(A, z)$.

Утверждение об автоматах $\bar{A}$ и ${}_dA$ доказывается аналогично.

2. а) Пусть $\{L_1, ..., L_n\}$ — локальная реакция НРС-автомата A, причем нумерация такова, что $L_i=L(A, z_i)$ при $i=1, ..., n$. При $x\in X$ в этом случае $x\backslash L_i$ оказывается объединением реакций всех состояний z автомата A, в которые он переходит из состояния z_i при входе x:

$$x\backslash L_i=x\backslash L(A, z_i)=\bigcup\{L(A, z)\,|\,(z_i, x, z)\in\tau\}.$$

б) Если $M=\{L_1, ..., L_n\}$ — множество, обладающее свойством, определенным в формулировке утверждения 2, то НРС-автомат A, имеющий локальную реакцию M, может быть построен следующим образом: пусть $z=\{z_1, ..., z_n\}$, S — произвольное подмножество множества Z, скажем,

$$S=Z,\ F=\{z_i\in Z\,|\,\Lambda\in L_i\},$$

$$\tau=\{(z_i, x, z_j)\,|\,L_j\subseteq x\backslash L_i,\ x\in X\},\ t=(Z\times X, Z, \tau)$$

и $A=(Z, X, t, S, F)$.

Промежуточное утверждение 1. $F\neq\varnothing$ тогда и только тогда, когда существует k такое, что $L_k\neq\varnothing$.

Доказательство. Если $F\neq\varnothing$, то по определению F существует L_k, содержащее Λ.

Пусть в то же время хотя бы одно из множеств L_i не пусто. Пусть тогда w кратчайшее слово, содержащееся в каком-либо из множеств L_i (скажем, в L_k).

Предположение: $w\neq\Lambda$, т. е. $w=xw'$, где $x\in X$.

Тогда $w'\in x\backslash L_k$, так что w' должно содержаться в одном из множеств L_j. Это противоречит предположению, поскольку w' короче слова w. Итак, $w=\Lambda$ и потому в данном случае $F\neq\varnothing$.

Промежуточное утверждение 2. $L(A, z_i)=L_i$.

Доказательство. Пусть $i \in \{1, \ldots, n\}$ и $w = x_1, \ldots, x_m$, где $m \in \mathbf{N}_0$ и $x_1, \ldots, x_m \in X$. Нам нужно показать, что равносильны следующие высказывания:

1) $w \in L(A, z_i)$;

2) существуют $z_{j_0} = z_i, z_{j_1}, \ldots, z_{j_m}$ в Z такие, что $z_{j_m} \in F$ и $(Z_{j_{k-1}}, x_k, z_{j_k}) \in \tau$ при $k = 1, \ldots, m$;

3) существуют $j_0, j_1, \ldots, j_m$ в $\{1, \ldots, n\}$ такие, что $j_0 = i$, $\Lambda \in L_{j_m}$ и $L_{j_k} \subseteq x_k \backslash L_{j_{k-1}}$ при $k = 1, \ldots, m$;

4) существуют $j_0, j_1, \ldots, j_m$ в $\{1, \ldots, n\}$ такие, что $j_0 = i$, $\Lambda \in L_{j_m}$ и при $k = 1, \ldots, m$

$$(x_{k+1} \ldots x_m) \backslash L_{jk} \subseteq (x_{k+1} \ldots x_m) \backslash (x_k \backslash L_{j_{k-1}}) = (x_k x_{k+1} \ldots x_m) \backslash L_{j_{k-1}};$$

5) существуют $j_0, j_1, \ldots, j_m$ в $\{1, \ldots, n\}$ такие, что $j_0 = i$ и

$$\Lambda \in L_{j_m} \subseteq x_m \backslash L_{j_{m-1}} \subseteq (x_m x_{m-1}) \backslash L_{j_{m-2}} \subseteq \ldots \subseteq (x_1 \ldots x_m) \backslash L_{j_0} = w \backslash L_i;$$

6) $w \in L_i$.

Равносильность высказываний 1) и 2) и высказываний 2) и 3) вытекает непосредственно из способа построения автомата A.

Высказывания 4) и 5) означают, очевидно, одно и то же.

По определению левого частного множества высказывание 6) является следствием высказывания 5).

Из предположения о множестве M и высказывания 6) полной индукцией по k доказывается существование последовательности $j_0, j_1, \ldots, j_m$ из $\{1, \ldots, n\}$ такой, что $j_0 = i$ и $x_{k+1} \ldots x_m \in L_{j_k} \subseteq x_k \backslash L_{j_{k-1}}$ при $k = 1, \ldots, m-1$. Отсюда сразу вытекает высказывание 3).

Остается показать, что из высказывания 3) вытекает 4). Для этого мы используем следующее легко проверяемое утверждение (см. п. 1 упражнения 5.17); для произвольных слов u и v из $F(X)$ и произвольного множества $L \subseteq F(X)$ выполнены равенства $u \backslash (v \backslash L) = \{w \mid uw \in v \backslash L\} = \{w \mid vuw \in L\} = vu \backslash L$.

Полагая $u = x_{k+1} \ldots x_m$, $v = x_k$ и $L = L_{j_{k-1}}$ и образовывая левые частные по u, из 3) получаем 4). ■

Замечание. Проблема поиска для данного HPC-автомата эквивалентного N-минимального автомата равносильна, таким образом, задаче поиска минимальной порождающей системы для локальной реакции D-минимального автомата, эквивалентного автомату A (или D-минимального автомата, эквивалентного автомату $\tilde{A}$), удовлетворяющей условию из утверждения 2 теоремы 6.6.2. При этом вместо D-минимального можно выбирать эквивалентный инициально связный неизбыточный ДРС-автомат, поскольку такой автомат на основании следствия 6.3.6 и упражнения 6.6 локально эквивалентен эквивалентному D-минимальному автомату.

Из доказательства теоремы вытекают еще два важных результата: характеризация локальных реакций минимальных РС-автоматов и новая характеризация допустимых множеств (см. также упражнение 6.9).

Следствие 6.6.3. Пусть $L \subseteq F(X)$.

1. L допустимо тогда и только тогда, когда множество $LQ(L)$ всех левых частных $w \backslash L$ множества L по w из $F(X)$ [или множество $RQ(L)$ всех правых частных L/w множества L по w из $F(X)$] конечно.

2. Если множество L допустимо, то $LQ(L)$ [или $RQ(L)$] является локальной реакцией некоторого минимального РС-автомата с реакцией L (или с реакцией $\tilde{L}$ соответственно).

Доказательство. Пусть $L \in Akz(X)$ и A — минимальный РС-автомат с реакцией L. Выполнение при этом равенства $LQ(L) = LL(A)$ [а потому конечность $LQ(L)$] вытекает из п.1 доказательства теоремы 6.6.2. Действительно, заметим, что любое слово w из $F(X)$, не являющееся начальным отрезком (префиксом) какого-либо слова из L, т. е. слово w, для которого $w \backslash L = \varnothing$, приводит к переходу автомата из начального состояния в некоторое состояние с пустой реакцией. Любое же иное слово w приводит к переходу в состояние z′, реакция которого в точности равна $w \backslash L$.

Если, напротив, множество $LQ(L)$ при некотором $L \subseteq F(X)$ конечно, т. е., скажем, $LO(L) = \{L_1, \ldots, L_n\}$, то $LQ(L)$ удовлетворяет условию 2 теоремы 6.6.2, так как для каждого x из X и каждого L_i существует в точности одно L_j такое, что $x \backslash L_i = L_j$. Конструкция из подпункта б) доказательства теоремы 6.6.2, п. 2 при этом показывает, что $LQ(L)$ является локальной реакцией некоторого РС-автомата, если в качестве начального состояния этого автомата выбрать состояние с реакцией L [отметим, что L принадлежит $LQ(L)$]. Этот РС-автомат, как следует из первой части доказательства п.2 теоремы 6.6.2, оказывается минимальным, поскольку РС-автомат с меньшим числом состояний не может иметь множество $LQ(L)$ своей локальной реакцией.

Утверждения о $RQ(L)$ вытекает из соответствующих утверждений о $LQ(L)$, поскольку по теореме Клини $\tilde{L}$ допустимо в точности тогда, когда допустимо L. ■

Из этого следствия и из теоремы 5.6.4 вытекает, что при допустимом множестве L множество $LQ(L)$ всех левых частных вида $w \backslash L$ удовлетворяет системе равенств вида $Y = MY + \delta$, а именно системе, соответствующей минимальному РС-автомату с реакцией L.

Чтобы показать, каким образом можно по рациональному выражению для L непосредственно (минуя стадию построения РС-автомата) получить систему равенств, которой удовлетворяет $LQ(L)$, распространим сначала понятие левого частного по некоторому слову на рациональные выражения. Аналогичным образом это может быть сделано и в случае правых частных (см. упражнение 6.10).

Определение 6.6.4. Пусть X — конечное множество и RA(X) — множество всех рациональных выражений над X.

1. Отображение δ: RA(X)→RA(X) задается равенством

$$\delta(\alpha)=\begin{cases}\varnothing^*, & \text{если } \alpha \text{ обладает свойством пустого слова (см. лемму 5.7.8),}\\ \varnothing & \text{в противном случае.}\end{cases}$$

2. Для любого слова w из F(X) пусть D_w — отображение из RA(X) в себя, удовлетворяющее следующим условиям:

а) если $w=\Lambda$, то D_w — тождественное отображение;

б) если $w\in X$, то $D_w(\varnothing)=\varnothing$,

$$D_w(x)=\begin{cases}\varnothing^*, & \text{если } w=x\in X,\\ \varnothing & \text{в противном случае,}\end{cases}$$

$$D_w(\alpha+\beta)=D_w(\alpha)+D_w(\beta) \text{ и } D_w(\alpha\cdot\beta)=D_w(\alpha)\cdot\beta+\delta(\alpha)\cdot D_w(\beta)$$

для всех α и β из RA (X), а $D_w(\alpha^*)=D_w(\alpha)\cdot\alpha^*$

для всех α из RA(X);

в) если $w=uv$, то $D_w=D_v\cdot D_u$, т. е. для любого α из RA(X) выполняется равенство $D_{uv}(\alpha)=D_v(D_u(\alpha))$.

3. Для любого α из RA(X) рациональное выражение $D_w(\alpha)$ называется *левым производным* α *по* w.

Лемма 6.6.5. Отображение D_w при любом w из F(X) определено корректно, для любого α из RA(X) значение $D_w(\alpha)$ может быть определено эффективным образом, и диаграмма на рис. 6.6.1 коммутативна.

Здесь r — заданная в п.1 определения 5.7.6 стандартная семантика рациональных выражений, а $w\backslash$ — отображение, соответствующее операции образования левых частных по w, т. е. при любом L из Rat(X) считается выполненным равенство $w\backslash(L)=\{w\}\backslash L$.

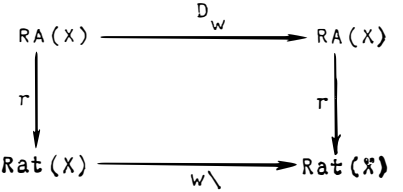


Рис. 6.6.1

Доказательство. Полной индукцией по длине слова w покажем, что значение $D_w(\gamma)$ при любом γ из RA(X) может быть определено эффективным образом и что $r(D_w(\gamma))=w\backslash r(\gamma)$.

При $|w|=0$ утверждение вытекает из условия а).

При $|w|=1$ мы докажем требуемое утверждение на базе леммы 5.7.2 полной индукцией «по подвыражениям» выражения γ.

В случаях 1) и 2) из леммы 5.7.2, т. е. при $\gamma=\varnothing$ и $\gamma\in X$, утверждение немедленно вытекает из первых двух равенств условия б).

Для случая $\gamma=\alpha\cdot\beta$ или $\gamma=\alpha^*$ мы используем тот факт, что по лемме 5.7.16 и п.1 определения 6.6.4 для каждого α из RA(X) существует в RA(X) выражение α_1 такое, что $\alpha=\alpha_1+\delta(\alpha)$ и $\delta(\alpha_1)=\varnothing$.

Таким образом при любом x из X и любом β из RA(X) выполнены равенства

$$x\backslash r(\alpha)=x\backslash r(\alpha_1) \text{ и } (x\backslash r(\alpha_1))r(\beta)=x\backslash r(\alpha_1\cdot\beta).$$

Допустим, что доказываемое высказывание верно для α и β. Для любого x из X из равенств в условии б) и легко доказываемых свойств операции образования левых частных (см. упражнение 5.17) получаем:

$$r(D_x(\alpha+\beta))=r(D_x(\alpha))+r(D_x(\beta))=x\backslash r(\alpha)+x\backslash r(\beta)=$$
$$=x\backslash r(\alpha+\beta);$$
$$r(D_x(\alpha\cdot\beta))=r(D_x(\alpha))r(\beta)+r(\delta(\alpha))r(D_x(\beta))=$$
$$=(x\backslash r(\alpha))r(\beta)+r(\delta(\alpha))(x\backslash r(\beta))=$$
$$=(x\backslash r(\alpha_1))r(\beta)+x\backslash(r(\delta(\alpha))r(\beta))=$$
$$=x\backslash r(\alpha_1\cdot\beta)+x\backslash r(\delta(\alpha)\cdot\beta)=$$
$$=x\backslash r((\alpha_1+\delta(\alpha))\cdot\beta)=x\backslash r(\alpha\cdot\beta);$$
$$r(D_x(\alpha^*))=r(D_x(\alpha))r(\alpha^*)=(x\backslash r(\alpha))r(\alpha^*)=$$
$$=(x\backslash r(\alpha_1))r(\alpha_1^*)=$$
$$=x\backslash r(\alpha_1\cdot\alpha_1^*)=x\backslash r(\alpha_1^*)=x\backslash r(\alpha^*).$$

Если w — произвольное слово и доказываемое утверждение истинно для всех слов u и v из F(X), более коротких, чем w, то истинность этого утверждения для слова w вытекает из условия в) и из высказывания, приведенного в конце доказательства теоремы 6.6.2. ■

Замечания. 1. Для $w\in F(X)$ и $\alpha\in RA(X)$ включение $w\in r(\alpha)$ выполняется тогда и только тогда, когда $D_w(\alpha)$ обладает свойством пустого слова (поскольку это выполняется в точности тогда, когда $r(\alpha)=r(\alpha)\cup\{w\}$).

2. Левые производные эквивалентных рациональных выражений по одному и тому же слову w эквивалентны.

3. На основании п.1 следствия 6.6.3 множество всех левых производных некоторого рационального выражения α (по всем словам w) состоит из конечного числа классов K_i эквивалентных рациональных выражений. Для каждого такого класса K_i существует кратчайшее слово w_i такое, что этот класс состоит из всех левых производных α_i выражения α, для которых выполнено равенство $r(\alpha_i)=w_i\backslash r(\alpha)$.

4. Система представителей всех классов эквивалентности левых производных некоторого рационального выражения α — так называемая *система характеристических левых производных* — может быть найдена следующим образом. Необходимо последовательно при $i=0, 1, 2, \ldots$ строить левые производные выражения α по словам длины i до тех пор, пока не будет обнаружено i_0, при котором все левые производные по словам длины i_0 окажутся эквивалентными ранее построенным (при меньших i) производным.

Ясно, что i_0+1 не должно быть больше числа состояний минимального РС-автомата с реакцией $r(\alpha)$, так что на основании п. 2 следствия 6.6.3 i_0+1 не превышает числа различных классов эквивалентных левых производных выражения α.

Теорема 6.6.6 (Бжозовски, Спивак). Пусть $X=\{x_1, \ldots, x_n\}$ и $\alpha \in RA(X)$. Тогда

1. $\alpha = \delta(\alpha) + x_1 D_{x_1}(\alpha) + \ldots + x_n D_{x_n}(\alpha)$,

причем представляемые слагаемыми рациональные множества попарно дизъюнктны (не пересекаются).

2. Пусть $C(\alpha) = \{D_{w_1}(\alpha), \ldots, D_{w_{k(\alpha)}}(\alpha)\}$ — система характеристических левых производных α. Тогда $k(\alpha)$ есть число состояний минимального РС-автомата $A(\alpha)$ с реакцией $r(\alpha)$ и выполнены следующие, называемые характеристическими, равенства (при $i=1, \ldots, k(\alpha)$), которые образуют соответствующую автомату $A(\alpha)$ систему равенств (в смысле п.2 определения 5.6.3):

$$D_{w_i}(\alpha) = \delta(D_{w_i}(\alpha)) + x_1 \cdot D_{u_{i_1}}(\alpha) + \ldots + x_n D_{u_{i_n}}(\alpha),$$

где $D_{u_{ij}}(\alpha) = D_{w_i x_j}(\alpha)$ и $D_{u_{ij}}(\alpha) \in C(\alpha)$ при $j = 1, \ldots, n$.

Множество $C(\alpha)$ может быть, в частности, выбрано таким образом, что при $i=1, \ldots, k(\alpha)$ будут выполняться неравенства $|w_i| \leqslant k(\alpha)-1$, т. е. в качестве w_i могут быть выбраны кратчайшие слова, переводящие $A(\alpha)$ из начального состояния в различные другие.

Далее, всегда $LQ(r(\alpha)) = \{r(D) \mid D \in C(\alpha)\}$.

Доказательство. 1. Для любого x_i из X множество $r(\alpha)$ может быть следующим образом разложено на дизъюнктные подмножества:

$$r(\alpha) = r(\delta(\alpha)) \cup \{w \in r(\alpha) \mid w \text{ начинается символом } x_i\} \cup \{u \in r(\alpha) \mid u \text{ начинается символом } x_j,\ j \neq i\}.$$

Отсюда с помощью леммы 6.6.5 немедленно получаем нужное утверждение.

2. Равенства для $D_{w_i}(\alpha)$ получаются из п.1 при последовательной замене α на все элементы множества $C(\alpha)$ с учетом того, что $D_{x_j}(D_{w_i}(\alpha)) = D_{w_i x_j}(\alpha)$. Остальное вытекает из пп. 3 и 4 предыдущего замечания и следствия 6.6.3. ■

Замечания. 1. Теорема 6.6.6 вместе со сделанным выше замечанием и с п. 2,б) доказательства теоремы 6.6.2 является основой новых методов построения минимального РС-автомата $A(\alpha)$, допускающего представленное рациональным выражением α множество:

1) Построить $C(\alpha)$ и по нему $A(\alpha)$ методом из доказательства теоремы 6.6.2.

2) Построить $C(\alpha)$ и по нему систему характеристических равенств (по теореме 6.6.6); после этого построить НРС-автомат такой, что соответствующая ему система равенств совпадает с этой системой (см. упражнение 6.11).

2. Проверка эквивалентности рациональных выражений является весьма трудоемким процессом. Поэтому описанный в общих чертах в предыдущем замечании метод построения системы характеристических левых производных для данного рационального выражения α и составление системы характеристических равенств оказываются мало полезными с практической точки зрения. Если не ставится задача поиска непременно минимального РС-автомата с реакцией $r(\alpha)$, то можно отказаться от требования попарной неэквивалентности элементов множества $C(\alpha)$, т. е. можно использовать ослабленное понятие эквивалентности, допускающее более легкую проверку, например понятие сходства (см. упражнение 6.12), и получать таким образом, вообще говоря, больше равенств для α.

3. Из теоремы 5.4.5 следствия 5.4.6 и упражнения 5.14 вытекает, что автомат Мура (или автомат Мили) с m выходами может быть описан совокупностью из m рациональных выражений — каждому выходу y сопоставляется рациональное выражение α_y, которое определяет входные последовательности, приводящие к появлению выхода y.

Если же заданы m рациональных выражений, то возникает вопрос о построении автомата Мура (или автомата Мили), описываемого в указанном выше смысле данными выражениями. Этот вопрос рассматривается в упражнении 6.13. Для случая $m=1$ метод из упражнения 6.13 позволяет строить минимальный РС-автомат, реакция которого представляется данным рациональным выражением.

4. При построении (кратчайших) рациональных выражений часто используются и дополнительные знаки операций, соответствующие булевым операциям пересечения, дополнения и разности (а иногда и симметрической разности) и операции образования подполугруппы. Порожденные таким образом выражения называются *обобщенными рациональными выражениями*. Понятия левого (правого) производного выражения и описанные выше методы могут быть очевидным образом распространены на случай обобщенных рациональных выражений — см. упражнение 6.14.

УПРАЖНЕНИЯ

6.1. 1. (Лупанов.) Пусть $X=\{a, b, c\}$, $n\geqslant 3$ и $\tilde{A}_n=(\{1, \ldots, n\}, X, f, 1, 1)$, где $f(1, a)=2$, $f(1, b)=n$, $f(1, c)=2$, $f(i, a)=i$, $f(i, b)=i-1$ при $i=2, \ldots, n$, $f(2, c)=1$, $f(j, c)=j$ при $j=3, \ldots, n$.

Для автомата $A_n=\tilde{\tilde{A}}_n$, зеркального для $\tilde{A}_n$, докажите, что РС-автомат с реакцией $L(A_n)$ должен иметь не менее 2^n состояний.

2. (Лупанов.) Пусть $X=\{a, b\}$. Докажите, что для каждого $n\geqslant 3$ минималь-

ный РС-автомат, эквивалентный описанному ниже автомату $\overline{A}_n$, обладает 2^n состояниями:

$\overline{A}_n = (\{1, \ldots, n\}, X, t, 1, 1)$, $t(i, a) = t(i, b) = \{i+1\}$ при $i = 3, 4, \ldots, n-1$, $t(1, a) = \{3\}$, $t(2, a) = \{1\}$, $t(j, b) = j+1$ при $j = 1, 2$, $t(n, b) = \{1, 2\}$.

3. (Мейер, Фишер.) Пусть при $n \geqslant 1$

$B_n = (\{0, 1, \ldots, n-1\}, \{a, b\}, t, 0, 0)$ — НРС-автомат с $t(i, b) = (i+1) \bmod n$ при $i = 0, 1, \ldots, n-1$ и $t(j, a) = \{0, j\}$ при $j = 1, \ldots, n-1$.

Докажите, что РС-автомат, допускающий множество $L(B_n)$, должен иметь по меньшей мере 2^n состояний, и что множество слов, зеркальное для $L(B_n)$, может допускаться РС-автоматом с $2n$ состояниями.

4. (Янтцен.) Пусть при $n \geqslant 1$ $C_n = (\{1, \ldots, n\}, \{a, b\}, t, n, n)$ — НРС-автомат с $t(i, a) = \{1, i+1\}$, $t(i, b) = \{i+1\}$ при $i = 1, \ldots, n-1$ и $t(n, a) = \{1\}$.

Докажите, что допускающий множество $L(C_n)$ РС-автомат должен иметь по меньшей мере 2^n состояний. [Указание. Покажите сначала, что $L(C_n)$ совпадает с определенным в замечании к примеру 6.1.3 множеством W_n, и выведите отсюда, что при всех $w \in a\{a, b\}^{n-1}$ состояния $f^*(s, w)$ отличны друг от друга и от начального состояния s.]

6.2. 1. Некоторое состояние автомата A называется определенно недостижимым, если оно не является начальным и если в графе автомата A нет ребер, входящих в соответствующую этому состоянию вершину и исходящих из какой-либо другой вершины.

Обладает ли каждое недостижимое состояние автомата A этим свойством? [Указание. См. пример 5.1.2.]

2. Какими свойствами обладает граф, получаемый из графа автомата A при применении описываемого ниже метода?

Метод: до тех пор, пока в графе имеется хотя бы одна вершина (состояние) $z \notin S$, для которой не существует ни одного перехода $(z', w, z) \in \tau$ с $z' \neq z$, исключать такую вершину z и все исходящие из нее ребра.

3 Предложите метод, с помощью которого можно установить для произвольного НРС-автомата A и произвольного слова w из $F(X)$, выполняется ли включение $w \in L(A)$, причем не более чем за $|Z| \cdot |w| \cdot \max |t(z, x)|$ шагов, где максимум берется по всем $z \in Z$ и $x \in X \cup \Lambda$.

6.3. Примените метод из разд. 6.2 к автоматам из примеров в разд. 5.1 и 6.1 и из упражнений 5.3 и 6.1.

6.4. Пусть A — инициально связный РС-автомат. Покажите, что применение описываемого ниже метода приводит к построению минимального эквивалентного автомату A автомата.

1) Положить $k = 1$ и построить следующее отношение N_0 на Z:

zN_0z' тогда и только тогда, когда как z, так и z' принадлежат F или когда как z, так и z' не принадлежат F.

2) Построить следующее отношение N_k на Z:

zN_kz' тогда и только тогда, когда $zN_{k-1}z'$ и при каждом x из X выполнено $f(z, x) N_{k-1} f(z', x)$.

3) Если $N_k \neq N_{k-1}$, то увеличить k на 1 и перейти к шагу 2); в противном случае — перейти к шагу 4).

4) Пусть $N = N_k$ и Z' — множество всех классов эквивалентных состояний по N (показать, что N_k при всех k отношение эквивалентности, т. е. рефлексивное, симметричное и транзитивное отношение). Пусть, далее, s' — класс эквивалентности, содержащий s, и F' — множество всех классов эквивалентности, содер-

жащихся в F. Пусть, наконец, для любого z' из Z' и любого x из X функция f' определяется условием: $f'(z', x)$ есть класс, содержащий $f(z', x)$. Доказать, что $A' = (Z', X, f', s', F')$ —автомат, минимальный для A.

Покажите, кроме того, что значение, которого достигает параметр k, не превышает $|Z|$, но что при этом время работы алгоритма растет, вообще говоря, как третья степень числа состояний автомата A. Исследуйте, далее, что происходит, если метод применяется к РС-автоматам с недостижимыми состояниями. [Указание. Модифицируйте доказательство теоремы 2.3.3.]

2. Модифицируйте метод из разд. 2.4 так, чтобы получить улучшенный вариант метода из п.1.

3. Перенесите метод Хопкрофта — Гриса из разд. 2.5 на случай РС-автоматов.

4. Выведите из пп. 1—3 и из метода 6.3.3 метод для определения эквивалентности состояний побуквенного НРС-автомата. [Указание. Примите во внимание, что у НРС-автомата из некоторого состояния могут исходить два пути, отвечающие одному и тому же входному слову, такие, что один из этих путей ведет в финальное состояние, а второй — нет.]

5. Докажите, что методы из пп. 1—3 и метод 6.3.3 можно применять для решения вопроса об эквивалентности двух заданных РС-автоматов. [Указание. Заметьте, что начальные состояния не играют роли в рассматриваемых методах, так что можно использовать объединение автоматов.]

6. Примените методы из пп. 1—3 и метод 6.3.3 к одному из описанных в примерах или упражнениях автоматов и сравните затраты времени и необходимую память.

6.5.* (Брандт.) 1. Используя теорему 6.2.8 и упражнение 6.4, постройте алгоритм, с помощью которого можно определить, являются ли эквивалентными два подмножества состояний некоторого НРС-автомата.

2. Из п.1 выведите, что два подмножества множества состояний некоторого НРС-автомата с n состояниями эквивалентны уже тогда, когда их реакции на входные последовательности длины, не большей $2^n—3$, совпадают, и что эта граница не может быть улучшена.

6.6.* (Бючи). Распространите понятия гомоморфизма, введенные для автоматов Мура (см. определение 3.6.1), на случай РС-автоматов и покажите, что:

а) каждый инициально связный РС-автомат может быть гомоморфно отображен на эквивалентный минимальный РС-автомат. [Указание. Покажите, что определенное в п.1 упражнения 6.4 отношение $\mathbb{N}$ задает нужный гомоморфизм: $h(z) = h(z')$ тогда и только тогда, когда $z\mathbb{N}z'$.];

б) инициально связный РС-автомат A является сокращенным в точности тогда, когда он гомоморфно сокращен, т. е. когда каждый Z-гомоморфный образ A оказывается изоморфным A.

6.7. Пусть A — инициально связный РС-автомат и A' — эквивалентный ему минимальный РС-автомат. Покажите, что моноид переходов автомата A' является гомоморфным образом моноида переходов автомата A и изоморфен синтаксическому моноиду по $L(A)$. [Указание. Используйте упражнения 5.13 и 6.6.]

Сопоставьте, далее, это утверждение с утверждением из упражнения 5.12.

6.8. 1. (Индермарк, Брандт.) Пусть A — сокращенный НРС-автомат, z — состояние автомата A и T — подмножество множества состояний автомата A такое, что $z \notin T$ и $L(A, z) = L(A, T)$. Тогда состояние z называется элиминируемым.

Докажите, что определенный ниже НРС-автомат A′ эквивалентен автомату A: $A'=(Z-z, X, t', S', F-z)$, где $S'=T \cup S-z$, если $z \in S$, и $S'=S$ в противном случае,

$$t'(z', x) = t(z', x) - z \cup \begin{cases} T, & \text{если } z \in t(z', x), \\ \varnothing & \text{в противном случае.} \end{cases}$$

2. Постройте не N-минимальный НРС-автомат A, для которого будет выполнено условие: автоматы A и $\widetilde{A}$ — сокращенные, неизбыточные и изоморфные; ни одно состояние автомата A (или $\widetilde{A}$) не является элиминируемым (в смысле п. 1). [Указание. Пусть, например, $L(A)=bb^*b \cup a^2 \cup ab \cup ba$.]

3. Докажите, что эквивалентные неизбыточные сокращенные НРС-автоматы не обязательно должны иметь одинаковое число состояний.

4. Докажите, что существует N-минимальный НРС-автомат, множество состояний которого обладает двумя различными, но эквивалентными подмножествами; при этом одно из подмножеств может быть одноэлементным или пересечение этих подмножеств может быть пусто.

6.9.* (Рейни, Нерод, Бючи, Индермарк.) Отношение эквивалентности R на F(X) называется правой конгруэнцией (соответственно — левой конгруэнцией), если для всех слов u и v из F(X) и всех x из X выполнено условие: из uRv следует uxRvx (соответственно — xuRxv).

Пусть $L \subseteq F(X)$. Определяемое ниже отношение R^r_L (соответственно R^l_L) называется синтаксической правой (левой) конгруэнцией по L; для произвольных u и v из F(X) соотношение uR^r_Lv (uR^l_Lv) справедливо тогда и только тогда, когда выполнено условие:

для каждого слова w из F(X) слово uw (соответственно — wu) принадлежит L в том и только в том случае, когда vw (соответственно wv) принадлежит L.

Докажите следующее.

1. Синтаксическая правая (левая) конгруэнция по $L \subseteq F(X)$ является правой (левой) конгруэнцией в описанном выше смысле.

2. Отношение R на F(X) является конгруэнцией тогда и только тогда, когда оно является левой и правой конгруэнцией (ср. лемму 5.4.3).

3. Для каждого $L \subseteq F(X)$ и произвольных u и v из X выполнены условия:

а) uR^r_Lv тогда и только тогда, когда $u \setminus L = v \setminus L$;

б) uR^l_Lv тогда и только тогда, когда $L/u = L/v$.

4. Пусть A — PC-автомат (или $\widetilde{A}$ — зеркальный для A PC-автомат с начальным состоянием $\widetilde{s}$). Тогда определяемое ниже отношение R^r_A (соответственно R^l_A) является правой (левой) конгруэнцией над F(X): для u и v из F(X) соотношение uR^r_Av (соответственно uR^l_Av) выполняется тогда и только тогда, когда $f^*(s, u)=f^*(s, v)$ [$\widetilde{f}^*(\widetilde{s}, \widetilde{u})=\widetilde{f}^*(\widetilde{s}, \widetilde{v})$].

5. Подмножество L моноида F(X) допустимо тогда и только тогда, когда оно является объединением классов эквивалентности относительно некоторой правой (левой) конгруэнции конечного индекса (т. е. имеющей только конечное число таких классов) над F(X); это верно в том и только в том случае, когда R^r_L (R^l_L) имеет конечный индекс.

6. Пусть A — PC-автомат (или $\widetilde{A}$ — PC-автомат). Тогда автомат A ($\widetilde{A}$) является минимальным в том и только в том случае, если $R^r_A = R^r_{L(A)}$ ($R^l_A =$

$=R^1_{L(A)}$). [Указание. Используйте следствие 6.6.3 или доказательство теоремы Майхилла (теорема 5.4.4), см. также упражнение 2.7.]

6.10. По аналогии с определением 6.6.4 определите понятие правого производного (выражения), докажите для этого случая лемму 6.6.5 и теорему 6.6.6 и перенесите на этот случай соответствующие замечания, заменяя везде «левое» на «правое» и полностью проводя все рассуждения.

6.11. Точно определите второй описанный в общих чертах в замечании к теореме 6.6.6 метод построения $A(\alpha)$ по α и докажите его корректность.

6.12. (Бжозовски.) Два рациональных выражения α и β из $RA(X)$ называются *сходными*, если равенство $\alpha=\beta$ может быть доказано в описываемой ниже системе аксиом $\overline{Ax}(X)$ (термин «доказательство» понимается так же, как в определении 5.7.11).

$\overline{Ax}(X)$ содержит в качестве аксиом аксиомы (a_1), (a_3), (a_6) и (a_7) из определения 5.7.9 и равенства 1)—4) из теоремы 5.7.15, а в качестве единственного правила вывода — правило замены из п.2 определения 5.7.9.

1. Предложите (по возможности быстрый) метод, с помощью которого можно определять, являются ли два данных рациональных выражения сходными.

2. Докажите, что отношение сходства на алгебре $(Ra(X); +, \cdot, *)$ является отношением конгруэнтности (т. е. рефлексивным, симметричным и транзитивным отношением, с которым совместимы все три операции).

3. Докажите, что число $k'(\alpha)$ различных классов сходных левых производных данного рационального выражения α конечно, причем $k'(\alpha)$, вообще говоря, больше, чем $k(\alpha)$; см. п.2 теоремы 6.6.6.). [Указание. Используйте индукцию «по подвыражениям» и, в частности, докажите, что

$$k'(\alpha+\beta)\leqslant k'(\alpha)\cdot k'(\beta);$$

$$k'(\alpha\cdot\beta)\leqslant k'(\alpha)\cdot 2^{k'(\beta)},$$

$$k'(\alpha^*)\leqslant 2^{k'(\alpha)}+1.]$$

Обратите внимание на то, что это доказательство является также прямым доказательством того, что число $k(\alpha)$ классов эквивалентных левых производных рационального выражения α конечно.

4. Пусть $C'(\alpha)$ — максимальная система попарно несходных левых производных рационального выражения α (т. е. система представителей классов сходных левых производных α). Покажите, что п.2 теоремы 6.6.6 остается справедливым — за исключением утверждения о $LQ(r(\alpha))$ — при замене $C(\alpha)$ на $C'(\alpha)$ и $k(\alpha)$ на $k'(\alpha)$, если опустить указание на свойство «минимальности».

6.13. Пусть заданы $m\geqslant 1$ рациональных выражений $\alpha_1, \ldots, \alpha_m$ таких, что представляемые ими множества образуют разбиение моноида $F(X)$, т. е. таких, что $r(\alpha_i)\cap r(\alpha_j)=\varnothing$ при $i\neq j$ и $r(\alpha_1)\cup r(\alpha_2)\cup\ldots\cup r(\alpha_m)=F(X)$.

Докажите, что методы, определяемые описываемыми ниже конструкциями (см. пп. 1 и 2), позволяют строить автомат Мура $A=(Z, X, Y, f, h)$ с $Y=\{y_1, \ldots, y_m\}$, удовлетворяющий следующему условию: A имеет выделенное состояние s такое, что при любом z из Z равенство $h(z)=y_i$ выполняется тогда и только тогда, когда существует слово w_i в $r(\alpha_i)$ такое, что $f^*(s, w_i)=z$.

1. (Бжозовски.) Вместо алгебры $(RA(X); +, \cdot, *)$ рассмотрите алгебру $(RA(X)^m; +, \cdot, *)=(RA(X)\times\ldots\times RA(X), +, \cdot, *)$, носителем которой является m-кратное декартово произведение $RA(X)$ на себя, т. е. множество всех m-ок

рациональных выражений над X, а операции — покомпонентны. Распространите семантическое отображение r и отображение D_w, определяющее левые производные по w, на m-ки из множества $RA(X)^m$ и покажите, что на этот случай могут быть перенесены высказывания леммы 6.6.5, теоремы 6.6.6 и соответствующих замечаний. При этом место минимального РС-автомата с реакцией $r(\alpha)$ занимает обобщенный РС-автомат $A=(Z, X, f, s, S_1, \ldots, S_m)$ с m различными множествами финальных состояний, обладающий следующим свойством: реакцией РС-автомата $A_i=(Z, X, f, s, S_i)$ является $r(\alpha_i)$ [где $(\alpha_1, \ldots, \alpha_m)$ — заданная m-ка рациональных выражений], и A — минимальный автомат с этим свойством. Если заданная m-ка рациональных выражений удовлетворяет приведенному в начале упражнения условию, то обобщенный РС-автомат A может рассматриваться как искомый автомат Мура.

2. (Глушков.) По данным m рациональным выражениям $\alpha_1, \ldots, \alpha_m$ постройте описанным ниже способом обобщенный в смысле п.1 РС-автомат A.

1) Для каждого x из X занумеруйте вхождения x во все α_i при $i=1, \ldots, m$ [скажем, индексами $1, \ldots, p(x)$, если x встречается всего $p(x)$ раз] и замените i-е слева вхождение x в рассматриваемые выражения на x_i [при $i=1, \ldots, p(x)$]. Получите таким образом m рациональных выражений $\alpha'_1, \ldots, \alpha'_m$ над $X'=\{x_i \mid x\in X, 1\leqslant i\leqslant p(x)\}$, содержащих только различные буквы из X'.

2) В качестве состояний автомата A возьмите начальное состояние s и некоторые подмножества множества X', так что A будет иметь не более 2^p+1 состояния, где p — сумма $p(x)$ по всем x из X.

3) Функцию переходов f и состояния z определите по индукции следующим образом:

при x из X полагаем

$f(s, x)=\{x_i\in X' \mid$ существует α'_j такое, что $D_{x_i}(\alpha'_j)\neq\varnothing\}$;

если $z\subseteq X'$ — уже определенное в виде значения функции переходов состояние (причем может быть, что $z=\varnothing$), то $f(z, x)=\{x_i\in X' \mid$ существуют α'_j, $y_k\in z$, u и v из $F(X')$ такие, что $uy_kx_iv\in r(\alpha'_j)\}$.

4) Множество финальных состояний S_i, которое должно «допускать» $r(a_j)$, получите из множества

$S'_i=\{z\in Z' \mid$ существуют $x_j\in z$ и $u\in F(X')$ такие, что $ux_j\in r(\alpha'_j)\}$, полагая

$$S_i=\begin{cases} S_i' \cup \{s\}, & \text{если } \Lambda\in r(\alpha_i), \\ S_i' & \text{в противном случае.}\end{cases}$$

Покажите, что полученный автомат обладает минимальным числом состояний.

3. Используйте метод из п.2 для доказательства того, что множество $Akz(X)$ замкнуто относительно булевых операций. Выведите, далее, из этого метода алгоритм определения эквивалентности двух рациональных выражений.

6.14. Определите так называемые обобщенные рациональные выражения, присоединяя к K функциональные константы $\cap$ (для пересечения), c (для дополнения), — (для разности), $\oplus$ (для симметричной разности) и $^+$ (для операции образования подполугруппы) и дополняя соответствующим образом п.1 определения 5.7.1. Задайте семантику таких выражений соответственно определению 5.7.6, доопределяя отображение r (см. также теорему 5.7.5). Предложите метод, с помощью которого из обобщенного рационального выражения можно получить эквивалентное рациональное выражение обычного вида. Распространи-

те определение левого производного (выражения) на случай обобщенных рациональных выражений. Дополните соответствующим образом лемму 6.6.5 и обобщите теорему 6.6.6.

ОБЗОР ЛИТЕРАТУРЫ

Первые примеры НРС-автоматов с n состояниями, для которых не существует эквивалентных РС-автоматов с менее чем 2^n состояниями (см. пп. 1 и 2 упражнения 6.1), были построены в [15], см. также [17]. Независимо такие примеры были построены в [21, 18, 19]. Пример из [18, 19] приведен в теореме 6.3.7, пример из [21] (в упрощенном виде из [16]) — в п. 3 упражнения 6.1, при n=4 этот пример в качестве задания дан в [8]. Почти оптимальный пример 6.1.2 заимствован из [16], пример 6.1.1 — из [14].

Конструкция экспоненциального автомата 6.2.9 (и теорема 6.2.8), а также теорема 6.3.5 получены уже в [41] из списка литературы к гл. 5.

Метод 6.3.3 описан в [9].

По поводу следствия 6.3.6 см. [3].

Первый метод решения проблемы минимизации для НРС-автоматов был дан в [12] и усовершенствован в [11]. Следствие 6.4.2, примеры автоматов, графы которых изображены на рис. 6.4.4 и 6.4.5, и теорема 6.6.2 заимствованы из [10]. Иное усовершенствование метода из [12] получено в [13], там же доказано, что автомат, зеркальный для N-минимального, является N-минимальным.

Класс НРС-автоматов, для которых зеркальные автоматы являются ДРС-автоматами, рассматривался уже в [2] из списка литературы к гл. 5. Тот факт, что D-минимальный для A и D-минимальный для $\tilde{A}$ автоматы не обязательно имеют одинаковое число состояний, упоминался уже в [5].

Методы элиминации и дополнения (см. пп. 1—3 в примере 6.5.2) заимствованы из [10].

По поводу следствия 6.6.3 см. [41, 52] из списка литературы к гл. 5 и [4].

Понятие левого производного (выражения), лемма 6.6.5, теорема 6.6.6 и замечания к ним, а также упражнения 6.12 и 6.13, п.1 основаны на работе [4]. Родственные идеи и результаты содержатся в [22—24] (см. также [17, 24] из списка литературы к гл. 2).

По поводу п.3 упражнения 6.2 см. [1].

Упражнение 6.9 в основном базируется на [23] из списка литературы к гл. 2 и на [20]; см. также [5, 10, 17].

Упражнения 6.13, пп. 2 и 3 заимствованы из [7]; см. также [8, 24] из списка литературы к гл. 2.

ГЛАВА 7.
ДАЛЬНЕЙШИЕ ХАРАКТЕРИЗАЦИИ ДОПУСТИМЫХ МНОЖЕСТВ

Программы для вычислительных машин, работа автоматов и процессы применения алгоритмов во многих случаях очень просто могут быть представлены ориентированными графами со взвешенными (помеченными) вершинами. По таким графам

сразу можно видеть множество всех последовательностей команд в программах, всех последовательностей состояний автоматов или всех элементарных шагов алгоритмов, приводящих к получению искомого результата.

Большая часть утверждений о допустимых или рациональных множествах может быть получена только лишь с помощью таких ориентированных графов со взвешенными вершинами. Это будет показано в некоторых проводимых ниже построениях. При этом, прежде всего с помощью этого нового представления, будет получено новое описание и будут выведены новые свойства допустимых или рациональных множеств.

7.1. ПОСЛЕДОВАТЕЛЬНОСТИ ВЫЧИСЛЕНИЙ ПРОГРАММ, СХЕМЫ ЯНОВА

Пример 7.1.1. Функционирование любой последовательностной дискретной системы, задачей которой является переработка определенных данных за конечное число шагов в желаемый результат, может быть упрощенно описано следующим образом.

Пусть набор данных в начале работы (т. е. вход) задается константой a. Состояние данных в текущий момент работы пусть описывается переменной y, а состояние данных в конце работы (результат) — переменной z.

Допустим также, что над совокупностью данных могут производиться операции из некоторого конечного множества (естественно, любое число раз). Пусть эти операции представлены совокупностью одноместных функциональных констант $f_1, \ldots, f_m$.

В зависимости от конечного числа логических условий (тестов), представленных набором одноместных предикатных констант $p_1, \ldots, p_n$, могут возникать разветвления вычислительного процесса.

Тогда функционирование рассматриваемых систем может быть описанию с помощью блок-схем, составленных из представленных на рис. 7.1.1 элементов (такие блок-схемы называют обычно *схемами Янова*).

Элементы соединяются между собой как в обычных блок-схемах. При этом, конечно, допускается только один элемент «Начало», но, вообще говоря, несколько элементов «Стоп». В элементе «Стоп» допускается также присвоение $z := y$. Далее, требуется, чтобы применение логических условий было обоснованным, т. е. чтобы в блок-схеме не существовало путей, в которых встречается два раза одно и то же логическое условие p_i, а между вхождениями p_i нет ни одного присвоения вида $y := f_k(y)$.

В качестве примера рассмотрим схему Янова, изображенную на рис. 7.1.2.

При подходящей интерпретации, т. е. при задании областей значений для a и y и фиксации функций $f_1, \ldots, f_5$ и предикатов $p_1 \ldots p_4$, схема GGT порождает программу для вычисления наи-

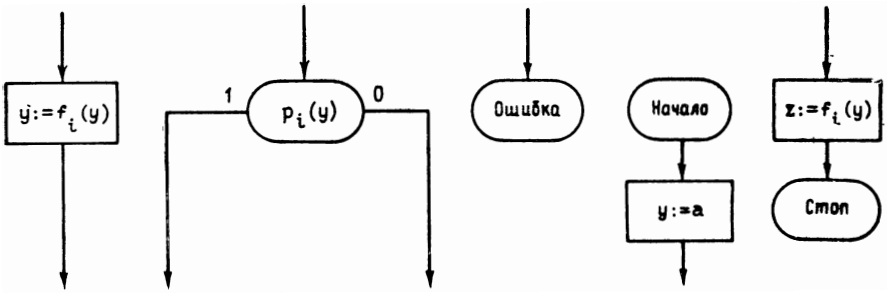


Рис. 7.1.1. Элементы схемы Янова

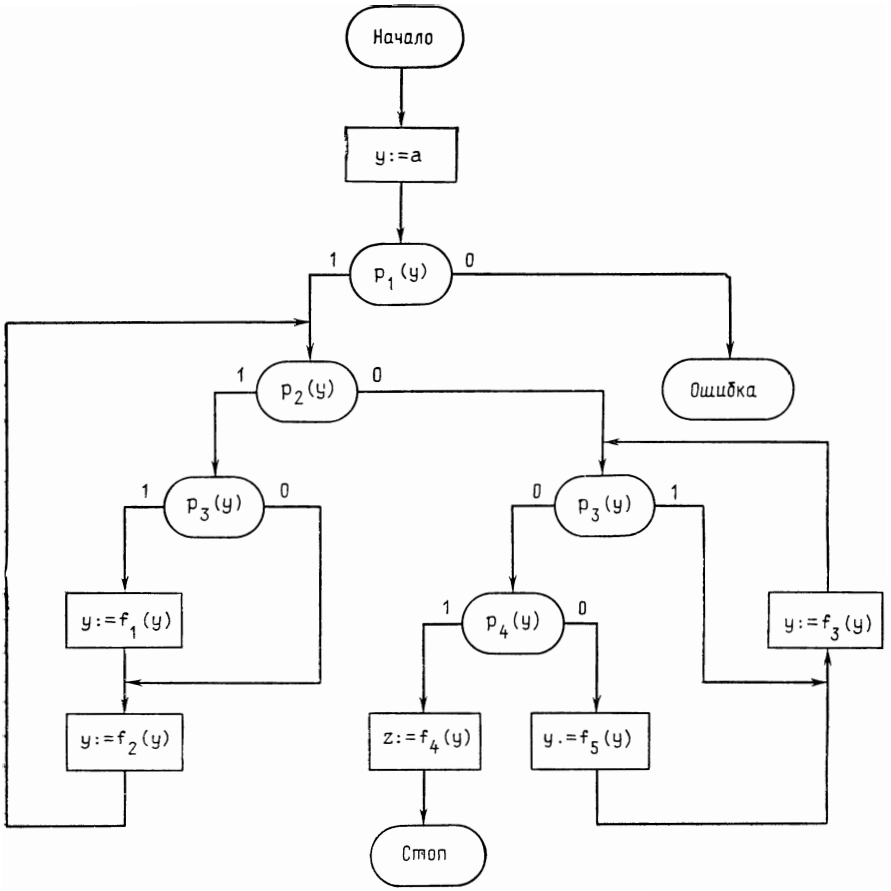


Рис. 7.1.2. Схема Янова GGT

большего общего делителя (x_1, x_2) двух натуральных чисел x_1 и x_2.

Выберем в качестве множества данных множество $\mathbf{Z}^3$ всех троек целых чисел, так что $y=(y_1, y_2, y_3)$ и $z=(z_1, z_2, z_3)$. Пусть далее, $a=(x_1, x_2, 1)$.

Допустим, что функции и предикаты определены следующим образом:

$$f_1((y_1, y_2, y_3))=(y_1, y_2/2, 2y_3),\ f_2((y_1, y_2, y_3))=(y_1/2, y_2, y_3),$$

$$f_3((y_1, y_2, y_3))=(y_1, y_2/2, y_3),\ f_4((y_1, y_2, y_3))=(y_1, y_2, y_1y_3),$$

$$f_5((y_1, y_2, y_3))=(y_2, |y_2-y_1|, y_3),$$

где $|x|$ — абсолютная величина числа x;

$p_1((y_1, y_2, y_3))=1$ тогда и только тогда, когда $y_1>0$ и $y_2>0$.

$p_2((y_1, y_2, y_3))=1$ тогда и только тогда, когда y_1 — четное число;

$p_3((y_1, y_2, y_3))=1$ тогда и только тогда, когда y_2 — четное число;

$p_4((y_1, y_2, y_3))=1$ тогда и только тогда, когда $y_1=y_2$.

Выход получается в виде z_3, т. е. $z_3=(x_1, x_2)$.

Для доказательства заметим, что перед применением логического условия $p_2(y)$ выполняются соотношения $x_1\cdot x_2>0$, $y_1\cdot y_2>0$ и $y_3\cdot(y_1, y_2)=(x_1, x_2)$.

Перед применением логического условия $p_3(y)$, стоящего в схеме справа, т. е. логического условия, которое проверяется в случае, когда логическое условие $p_2(y)$ не выполнено, всегда $y_1\cdot y_2>0$, y_1— нечетное число и выполнено равенство $y_3\cdot(y_1, y_2)=(x_1, x_2)$. Остальное вытекает из известного равенства $(y_1, y_2)=(y_2, |y_2-y_1|)$.

Для двух программ, которые должны делать одно и то же, бывает желательно регулярным образом решить вопрос, действительно ли это так. Нетрудное обобщение приводит к постановке следующей проблемы: если даны две различные схемы Янова, то требуется установить, порождают ли они одинаковый результат при одинаковой интерпретации и одном входе, т. е. являются ли они *«эквивалентными»*. При этом, конечно, должно предполагаться, что обе схемы имеют одинаковые функциональные и предикатные константы. Две такие схемы Янова P и P′, очевидно, эквивалентны, если для каждого пути от вершины «Начало» к вершине «Стоп» в P существует путь от вершины «Начало» к вершине «Стоп» в P′ такой, что на обоих путях производятся одинаковые присвоения и проверяются одинаковые логические условия, причем в одинаковой последовательности, и наоборот.

Множество таких *«последовательностей вычислений»*, т. е. последовательностей присвоений и логических условий, может быть представлено ориентированным графом с взвешенными вершинами (*«графом вычислений»*). При этом элементы схемы Янова заменяются на приводимые на рис. 7.1.3 подграфы.

Если элемент «Стоп» содержит только присвоение вида $z:=y$, то он заменяется на заштрихованную справа вершину с меткой S.

Из схемы на рис. 7.1.2 получается при этом граф вычислений, приведенный на рис. 7.1.4.

Следует отметить, что различные вершины графа вычислений могут иметь одинаковые метки. Все последовательности вычислений заданной схемы Янова можно, очевидно, получить, если для каждого пути в графе вычислений этой схемы, ведущего из начальной (заштрихованной слева) вершины в конечную (заштрихованную справа), выписать последовательность меток на проходимых вершинах.

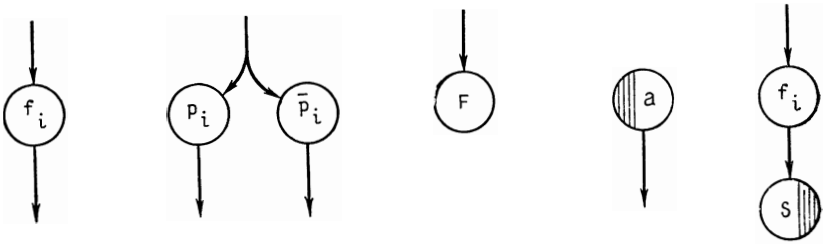


Рис. 7.1.3. Элементы графов вычислений

Легко видеть, что из графа вычислений можно получить граф некоторого НРС-автомата, если присоединить к нему одну непомеченную заштрихованную справа вершину S, убрать штриховку (правую) из всех помеченных вершин и провести из таких вершин ребра в вершину S. Кроме этого, следует каждое ребро, исходящее из вершины с меткой x, пометить символом x и убрать метку вершины. Наконец, следует отбросить все вершины, из которых никакой путь не ведет в конечную вершину.

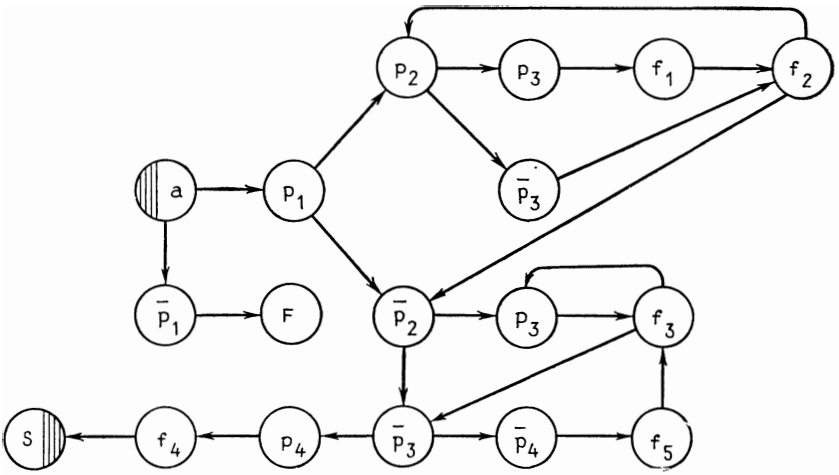


Рис. 7.1.4. Граф вычислений схемы GGT

Итак, для каждой схемы Янова можно построить некоторый НРС-автомат, допускающий в точности множество последовательностей вычислений этой схемы. Проблема эквивалентности для схем Янова сводится, таким образом, к проблеме эквивалентности НРС-автоматов и является потому разрешимой (см. теорему 5.5.9). Читателю рекомендуется также просмотреть упражнение 5.1.2 и выполнить упражнения 7.1 и 7.2.

Вопрос об эквивалентности программ — это вопрос о результатах работы программ, а не о способе и пути получения результатов. Поэтому в схеме GGT не делалось различия между двумя вхождениями логического условия p_3. При более точном исследовании функционирования программ может потребоваться различение отдельных вхождений функциональных и предикатных констант в некоторую схему Янова (скажем, с помощью верхних индексов). Получаемый таким образом граф вычислений содержит вершины, имеющие попарно различные метки (за исключением вершин, имеющих метки F и S). Очевидно, что все вершины с меткой F (и все вершины с меткой S) могут быть заменены единственной вершиной с той же меткой. Полученный в результате *«дифференциальный граф вычислений»* можно рассматривать как невзвешенный ориентированный граф, считая метки на вершинах просто обозначениями самих вершин, поскольку все эти метки попарно различны. Допустимое множество, сопоставляемое описанным способом некоторому такому графу, является так называемым стандартным множеством (см. определение 7.3.1).

7.2. ГРАФЫ МАЙХИЛЛА

В данном разделе будут подробно исследованы ориентированные графы и ориентированные графы со взвешенными вершинами, соответствующие им НРС-автоматы (см. пример, 7.1.1) и допускаемые такими автоматами множества.

Определение 7.2.1. Пусть X — конечное множество.

1. *Граф Майхилла над X* — это ориентированный граф G, для которого X — *множество вершин* и который имеет выделенные множества S и F *начальных* и соответственно *конечных вершин*, а также, *множество ребер* K, т. е. граф Майхилла — это упорядоченная четверка $G=(X, K, S, F)$, где $K \subseteq X \times X$, $S \subseteq X$ и $F \subseteq X$.

Маршрутным множеством $W(G)$ графа Майхилла G называется множество слов из $F(X)$, которое возникает при выписывании для каждого пути из какой-либо начальной в какую-либо конечную вершину последовательности проходимых в графе G вершин $W(G)=\{x_1, \ldots, x_n \mid n \in \mathbf{N}, x_1 \in S, x_n \in F$ и $(x_i, x_{i+1}) \in K$ при $i=1, \ldots, n-1\}$.

2. *Взвешенный (помеченный) граф Майхилла над X* — это граф Майхилла над некоторым конечным множеством E, *вершины* которого *помечены* элементами из множества $X \cup \Lambda$, т. е. это шестерка $G=(E, K, X, b, S, F)$ такая, что $G'=(E, K, S, F)$ — граф Майхилла и $b: E \to X \cup \Lambda$ — отображение (*взвешивающая функ-*

ция) такое, что $X \subseteq b(E)$ (так что X не содержит «лишних» элементов).

Взвешенный граф Майхилла G называется Λ-*свободным,* если $b(E) = X$.

Взвешенным марштрутным множеством $WB(G)$ графа G называется множество слов из $F(X)$, которое возникает при выписывании последовательностей весов вершин для каждого элемента маршрутного множества графа G':

$$WB(G) = \{b(e_1)b(e_2) \ldots b(e_n) \mid e_1 \ldots e_n \in W(G')\}.$$

Замечания. 1. Любой граф Майхилла над X можно рассматривать и как взвешенный граф Майхилла над X, множеством вершин которого является само множество X, а взвешивающей функцией — тождественное отображение X на себя. В то же время любой взвешенный граф Майхилла, взвешивающая функция которого Λ-свободна и инъективна, т. е. граф, в котором все вершины имеют разные и отличные от Λ метки, может рассматриваться как граф Майхилла.

2. Поскольку в случае взвешенных графов Майхилла вершины сами по себе, вообще говоря, не представляют интереса, мы будем представлять такие графы, как на рис. 7.1.4, приводя только метки, но не обозначения вершин.

3. Если G — взвешенный граф Майхилла в смысле определения 7.2.1 и h_b — задаваемый отображением b гомоморфизм из $F(E)$ в $F(X)$, то выполняется равенство

$$WB(G) = \{h_b(w) \mid w \in W(G')\} = h_b(W(G')).$$

Пример 7.2.2. 1. Граф вычислений некоторой схемы Янова представляет собой взвешенный граф Майхилла, а дифференциальный граф вычислений — граф Майхилла.

2. Если A — автомат Мили, автомат Мура, частичный автомат Мили или НРС-автомат, то из графа автомата A можно получить граф Майхилла над Z, опуская все входные и выходные символы (и вводя имена состояний, а в случаях автоматов Мили, Мура или частичных автоматов Мили — выделяя определенные вершины в качестве начальных и конечных). В частности, при этом для НРС-автомата A множество всех последовательностей состояний, которые автомат A проходит при поступлении на вход всех допустимых слов, оказывается маршрутным множеством.

3. Если G—Λ-свободный взвешенный граф Майхилла в смысле определения 7.2.1, то $A_G = (E, E, X, f, b)$ [где $f(e, e') = e'$ тогда и только тогда, когда $(e, e') \in K$] — частично определенный автомат Мура, для которого выполнено условие

$WB(G) = \{v \in F(X) \mid$ существуют $e \in S$, $e' \in F$ и $u \in F(E)$ такие, что $f^*(e, u) = e'$ и $b_e(u) = v\}$, где f^* и b_e понимаются также, как в случае частичных автоматов Мили (см. пп. 1, 2 определения 4.2.7). Если граф G не является Λ-свободным, то аналогичным образом по нему может быть построен обобщенный автомат Мура, порождающий в некоторых состояниях пустой выход Λ.

Пример 7.2.3. Известный пример взвешенных графов Майхилла представляют собой так называемые *синтаксические диаграммы,* используемые для наглядного изображения синтаксиса языков программирования.

Синтаксической диаграммой для некоторой синтаксической конструкции (например, для заголовка процедуры в языке Паскаль—см. пример 5.1.4) является блок-схема, описывающая процедуру порождения корректных относительно данной синтаксической конструкции последовательностей символов (например, правильно построенных заголовков процедур в языке Паскаль). Точнее говоря, синтаксическая диаграмма для некоторой синтаксической конструкции SK — это взвешенный граф Майхилла, взвешенным маршрутным множеством которого является множество всех корректных относительно SK последовательностей символов.

Чтобы избежать использования слишком больших синтаксических диаграмм и сделать возможным рекурсивное описание, применяется несложная конструкция, в которой допускаются два различных типа меток на вершинах. Для наглядности вершины с метками разных типов изображаются в различной форме:

округлая форма: меткой является основной символ языка или слово LETTER или DIGIT (или аналогичные обозначения для букв или цифр); метка этого типа означает, что если в процессе применения процедуры встречается данная вершина, то следует выписывать соответствующий основной символ или же знак требуемого вида;

прямоугольная форма: меткой является имя некоторой синтаксической диаграммы; эта метка означает, что прохождение данной вершины требует перехода к синтаксической диаграмме и после ее прохождения — возврата «на выход» из данной вершины.

Каждая синтаксическая диаграмма имеет единственную начальную и единственную конечную вершины. Обе эти вершины имеют метку Λ. Их обычно опускают, т. е. показывают только исходящее из начальной вершины и входящее в конечную вершину ребра.

СИНТАКСИЧЕСКАЯ ДИАГРАММА

Для пояснения сказанного, используя пример 5.1.4, мы приведем синтаксическую диаграмму для заголовка процедуры в языке Паскаль.

Синтаксическая диаграмма для заголовка процедуры может быть составлена из синтаксических диаграмм для идентификатора (IDENTIFIER) и для списка параметров (PARAMETER LIST) (рис. 7.2.1—7.2.3).

Полный взвешенный граф Майхилла для заголовка процедуры получается при последовательной замене «прямоугольных» вершин соответствующими диаграммами.

Отметим, однако, что для произвольных синтаксических диаграмм описанный выше процесс замены может не привести к по-

строению диаграммы, обладающей только «округлыми» вершинами, поскольку возможен случай, когда в диаграмме содержится прямоугольник с именем самой этой диаграммы. Описываемые такими диаграммами последовательности основных символов являются, вообще говоря, элементами множества, для которого не существует допускающего его НРС-автомата.

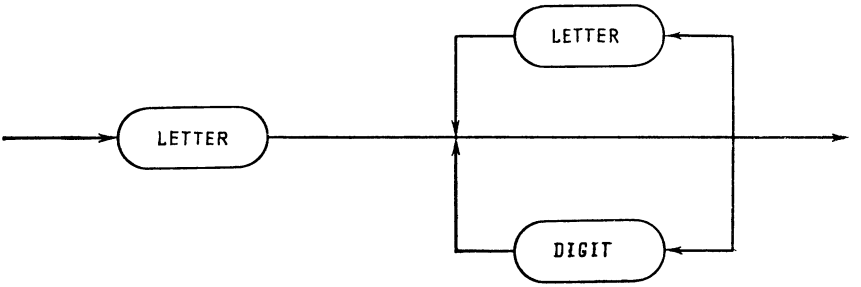


Рис. 7.2.1. Синтаксическая диаграмма для идентификатора

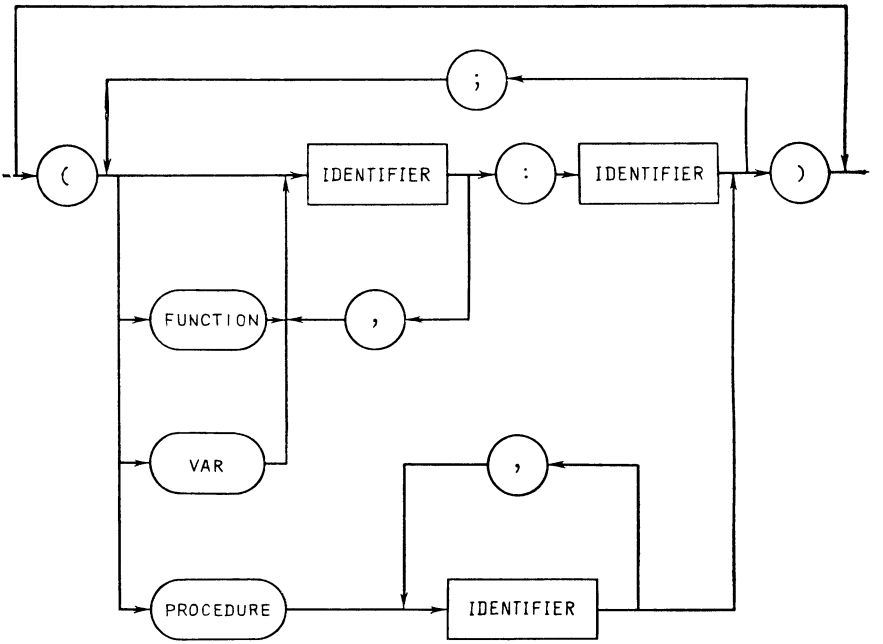


Рис. 7.2.2. Синтаксическая диаграмма для списка параметров

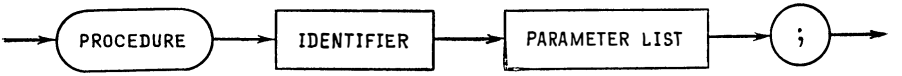


Рис. 7.2.3. Синтаксическая диаграмма для заголовка процедуры

С помощью рассуждений, аналогичных приведенным в примере 7.1.1, нетрудно показать, что взвешенные маршрутные множества взвешенных графов Майхилла допустимы и что все допустимые множества являются взвешенными маршрутными множествами для взвешенных графов Майхилла. Таким образом, взвешенные графы Майхилла являются дополнительным способом представления допустимых множеств.

Теорема 7.2.4 (теорема о графах Майхилла). Пусть X — конечное множество.

1. Если G — взвешенный граф Майхилла над X, то множество $WB(G)$ допустимо. В частности, допустимо любое маршрутное множество некоторого графа Майхилла.

2. Для каждого допустимого подмножества L моноида $F(X)$ существует взвешенный граф Майхилла G, для которого L — взвешенное маршрутное множество, т. е. такой граф G, что $L=WB(G)$. Если $\Lambda \notin L$, то граф G может быть выбран Λ-свободным.

3. Не каждое конечное подмножество моноида $F(X)$ является маршрутным множеством для некоторого графа Майхилла, так что не каждое допустимое множество является маршрутным множеством для некоторого графа Майхилла.

Доказательство. 1. Пусть $G=(E, K, X, b, S, F)$ — взвешенный граф Майхилла. Тогда, как в примере 7.1.1, может быть построен НРС-автомат, допускающий множество $WB(G)$.

Мы используем здесь несколько иной подход. Идея этого подхода может быть представлена двумя способами.

а) Пусть A_G — построенный по G в соответствии с предписанием из п.3 примера 7.2.2 автомат Мура. Тогда дополним A_G начальным состоянием, из которого будут достижимы все состояния из S, преобразуем его в автомат Мили и отбросим входы.

б) Представим себе машину M, работающую следующим образом.

Машина M имеет «указатель», который может указывать на некоторую вершину графа G или на некоторую точку P вне графа G. Машина M обрабатывает входы из множества $X \cup \Lambda$.

В начальном состоянии z_0 указатель не укызывает ни на какую-либо вершину графа G, ни на точку P.

Если M в начальном состоянии z_0 получает вход x, то указатель переходит на одну из помеченных символом x начальных вершин графа G, если таковая существует, в противном случае указатель переходит на точку P.

Если машина M указывает на точку P, то положение указателя более не меняется ни при каких входах.

Если машина M указывает на вершину e графа G и получает вход x, то указатель переходит из e по какому-либо ориентированному ребру на вершину с меткой x, если это возможно, в противном случае — на точку P.

Если указатель переходит на одну из конечных вершин, то

поступившая на вход последовательность считается допустимой.

Итак, пусть A — следующий HPC-автомат:

$A=(E\cup z_0, X, t, z_0, F)$, где $z_0\notin E$,

$(z_0, x', e)\in\tau$ тогда и только тогда, когда $e\in S$ и $b(e)=x'\in X\cup\Lambda$,

$(e, x', e')\in\tau$ тогда и только тогда, когда $(e, e')\in K$ и $b(e')=x'\in X\cup\Lambda$.

Отметим, что A — ДРС-автомат (или побуквенный автомат), если G — граф Майхилла (соответственно Λ-свободный граф). Легко проверяется, что $L(A)=WB(G)$.

2. Пусть L — допустимое подмножество моноида $F(X)$. Тогда, очевидно, существует алфавитный HPC-автомат

$A=(Z, X, t, S, F)$ с $L=L(A)$ и $S\cap F=\varnothing$.

Если Λ не принадлежит L, то в качестве A может быть выбран даже побуквенный HPC-автомат.

Допустим теперь, что $G=(Z\times(X\cup\Lambda), K, X, b, S\times(X\cup\Lambda), F')$ — взвешенный граф Майхилла, в котором $((z, x), (z', x'))\in K$ тогда и только тогда, когда $(z, x, z')\in\tau$ и $b(z, x)=x$ (для всех z и z' из Z, всех x и x' из $X\cup\Lambda$), и

$F'=\{(z, x)\in Z\times X|$ существует $z'\in F$ такое, что $(z, x, z')\in\tau\}$.

Если $\Lambda\notin L$, т. е. A — побуквенный HPC-автомат, то G — Λ-свободный граф.

Легко проверяется, что выполнено равенство $WB(G)=L(A)$.

Если методом из примера 7.1.1 построить для G HPC-автомат, то этот автомат будет эквивалентен автомату A.

3. Множество $L=\{ab, ac, bc\}$ не является маршрутным множеством какого-либо графа Майхилла, поскольку в графе Майхилла G с $W(G)=L$ элемент a должен был бы быть начальной, а элемент c — конечной вершиной и должны были бы иметься ребра (a, b) и (b, c), так что и слово abc должно было бы принадлежать $W(G)$. ■

С помощью теоремы о графах Майхилла очень легко можно выполнить п.3 упражнения 5.6. Сейчас мы рассмотрим частный случай этой теоремы, которой нам понадобится ниже.

Следствие 7.2.5. Пусть X и Y — конечные множества и $f: F(X)\to F(Y)$ — алфавитный гомоморфизм, т. е. гомоморфизм со свойством $f(X)\subseteq Y\cup\Lambda$.

Тогда $f(Rat(X))\subseteq Rat(Y)$, т. е. для любого $L\in Rat(X)$ выполняется включение $f(L)\in Rat(Y)$.

Доказательство. Пусть $L\in Rat(X)$. Тогда по теореме 7.4.2, п. 2 существует взвешенный граф Майхилла G с $L=WB(G)$. Заменяя в G множество весов X на множество Y и взвешивающее отображение b — на fb, т. е., заменяя у каждой вершины e метку $b(e)$ на $f(b(e))$, получаем, очевидно, взвешенный граф Майхилла G' с $WB(G')=f(L)$. ■

В упражнении 7.3 рассмотрено обобщение понятия взвешенного графа Майхилла, в котором в качестве весов вершин допускаются слова. С помощью этого понятия легко показать, что следствие 7.2.5 сохраняет силу и для неалфавитного гомоморфизма f.

7.3. СТАНДАРТНЫЕ МНОЖЕСТВА

Одним из особенно важных классов допустимых множеств являются стандартные множества (называемые также локальными множествами). Они встречаются во многих приложениях и служат основой для новой характеристики и описания допустимых множеств.

Определение 7.3.1. Подмножество L моноида $F(X)$ называется *стандартным множеством* над X, если существуют подмножества B и E множества X и подмножество P множества X^2 такие, что L является множеством всех слов из $F(X)$, начинающихся символом из B, оканчивающихся символом из E и не содержащих ни одной пары соседних букв из P, т. е. такие, что $L=BX^*\cap X^*E-X^*PX^*$, где $B, E\subseteq X$ и $P\subseteq X^2$.

Замечание. Стандартные множества называют также и *локальными множествами,* поскольку принадлежность некоторого слова w из $F(X)$ стандартному множеству L может быть установлена проверкой принадлежности первого и последнего символов множествам B и E соответственно и принадлежности всех пар соседних символов множеству X^2-P (см. также п.1 упражнения 5.9).

ХАРАКТЕРИЗАЦИЯ ДОПУСТИМЫХ МНОЖЕСТВ С ПОМОЩЬЮ СТАНДАРТНЫХ МНОЖЕСТВ

Лемма 7.3.2. Подмножество L моноида $F(X)$ является стандартным множеством тогда и только тогда, когда оно является маршрутным множеством некоторого графа Майхилла над множеством X.

Доказательство. а) Пусть $B, E\subseteq X$ и $P\subseteq X^2$, а $W(B, E, P)=BX^*\cap X^*E-X^*PX^*$.

Тогда, очевидно, $W(B, E, P)=\{x_1 \ldots x_n\in F(X) \mid n\in N,\ x_1\in B,\ x_n\in E$ и $x_ix_{i+1}\notin P$ при $i=1, \ldots, n-1\}$.

б) Пусть $L=W(G)$ для некоторого графа Майхилла $G=(X, K, S, F)$. Положим в этом случае $P=\{xx'\in X^2 \mid (x, x')\notin K\}$. Из определения множества $W(G)$ и п.а) вытекает равенство $L=W(S, F, P)$.

в) Пусть $L=W(B, E, P)$. Положим $K=\{(x, x')\in X\times X \mid xx'\notin P\}$. Тогда по определению графов Майхилла и из п.а) получаем, что $G=(X, K, B, E)$ — граф Майхилла с $W(G)=L$. ■

Другие свойства стандартных множеств приведены в упражнении 7.4.

Из теоремы о графах Майхилла и только что доказанной леммы получается новая характеризация для $Akz(X)$.

Теорема 7.3.3. (Хомский, Шютценбергер). Подмножество U моноида $F(X)$ допустимо тогда и только тогда, когда существуют конечное множество Y, алфавитный гомоморфизм f из $F(Y)$ на $F(X)$ [т. е. гомоморфизм такой, что $X\subseteq f(Y)\subseteq X\cup\Lambda$] и стандартное множество L над Y такие, что $U=f(L)$. Если $\Lambda\notin U$, то может быть использован Λ-свободный гомоморфизм f [т. е. такой, что $f(Y)=X$].

Доказательство. 1. Если множество U допустимо, то из п.2 теоремы 7.2.4 следует, что существует взвешенный граф Майхилла $G=(E, K, X, b, S, F)$ такой, что $WB(G)=U$, являющийся Λ-свободным, если $\Lambda \notin U$. Из замечания 3 к определению 7.2.1 следует, что $G'=(E, K, S, F)$ — граф Майхилла с $WB(G)=h_b(W(G'))$, где h_b — определенный функцией b гомоморфизм из $F(E)$ на $F(X)$. h_b является алфавитным, поскольку $h_b(E)=b(E)=X \cup \Lambda$, и даже Λ-свободным, если $\Lambda \notin U$. По лемме 7.3.2 $L=W(G')$ — стандартное множество.

2. Пусть $U=f(L)$, причем L — стандартное множество и f — некоторый алфавитный гомоморфизм из $F(Y)$ на $F(X)$. Тогда по лемме 7.3.2 существует граф Майхилла $G'=(Y, K, S, F)$, где $L=W(G')$. Далее, $G=(Y, K, X, b, S, F)$, где b — сужение f/Y отображения f на множество Y, представляет собой взвешенный граф Майхилла с $WB(G)=f(L)$, так что множество U на основании теоремы п. 2 теоремы 7.2.4 допустимо.

Замечание. Иногда к стандартным множествам причисляют и множества вида $L \cup \Lambda$, где L — стандартное множество. В таком случае в теореме 7.3.3 всегда используются Λ-свободные гомоморфизмы.

РАЦИОНАЛЬНОСТЬ СТАНДАРТНЫХ МНОЖЕСТВ

Мы дадим прямое доказательство того, что стандартные множества рациональны (аналогично п.1 упражнения 5.7). Оно вместе с теоремой 7.3.3 и прямым доказательством следствия 7.2.5 (индукцией по подвыражениям рационального выражения) составляет новое доказательство рациональности допустимых множеств.

Теорема 7.3.4 (Майхилл). Каждое стандартное множество рационально.

Доказательство. Пусть $G=(X, K, S, F)$ — граф Майхилла. Для каждой пары (x, x') из $S \times F$ положим $G(x, x')=(X, K, x, x')$. Тогда выполняется равенство $W(G)=\cup\{W(G(x, x')) \mid (x, x') \in S \times F\}$.

Отсюда следует, что достаточно при фиксированной паре x, x' полной индукцией по числу $k=|K|$ ребер графа G показать рациональность множества $W=W(G(x, x'))$. При этом следует рассмотреть только случай, когда $W \neq \varnothing$.

При $k=0$ должно быть $x=x'$, так что $W=\{x\}$, т. е. множество W рационально.

Если $k=1$, то $K=\{(x, x')\}$ и W рационально, так как

$$W=\begin{cases} xx', & \text{если } x \neq x', \\ y^*, & \text{если } x=x'. \end{cases}$$

Предположение индукции: пусть при $k=n \geqslant 1$ множество W рационально.

Итак, пусть $k=n+1$. Тогда в K должно содержаться ребро $(a, b) \neq (x, x')$ такое, что в G должно существовать по одному

пути из x в a и из b в x′ (при этом может быть, что $x=a$ или $b=x'$).

Пусть для произвольных вершин e и e′ графа G $W_i(e, e')$ — множество всех слов из $W(G(e, e'))$, соответствующих путям из e в e′, в которые ребро (a, b) входит ровно i раз. Тогда

$$W=\cup\{W_i(x, x')\mid i=0, 1, 2, \ldots\},\ W_1(x, x')=W_0(x, a)W_0(b, x'),$$

$W_2(x, x')=W_0(x, a)W_0(b, a)W_0(b, x')$ и в общем случае

$$W_{i+1}(x, x)=W_0(x, a)(W_0(b, a))^iW_0(b, x')$$

при $i=0, 1, 2, \ldots$

Это означает, что выполняется равенство

$$W=W_0(x, x')\cup W_0(x, a)(W_0(b, a))^*W_0(b, x').$$

Чтобы показать рациональность множества W, нужно, таким образом, только показать, что при любых вершинах e и e′ рационально множество $W_0(e, e')$. Но это следует из предположения индукции, поскольку $W_0(e, e')$ является маршрутным множеством графа Майхилла, получающегося из графа $G(e, e')$ при удалении ребра (a, b). ■

МНОЖЕСТВА МЕДВЕДЕВА — КОСТИЧА

Из теоремы Хомского—Шютценбергера вытекает еще одна аналогичная характеризация допустимых множеств, в которой роль стандартных множеств принимают на себя множества, вводимые следующим определением.

Определение 7.3.5. Пусть X — конечное множество. Множество $MC(X)$ *множеств Медведева — Костича* над X есть наименьшее подмножество M булеана $F(X)$, обладающее следующими свойствами:

1. X принадлежит M и при любом a из X множества X^*a и X^*aX принадлежат M.

2. Вместе с U и V множества $U\cup V$ и $U\cap V$ также принадлежат M.

3. Если U принадлежит M, то и следующее множество $Pk(U)$ принадлежит M:

$Pk(U)=\{w\in U\mid$ при всех u, $v\in F^+(X)$ таких, что $uv=w$, выполнено $u\in U\}$.

Множество $Pk(U)$ называется *префиксным ядром* множества U.

Замечание. Префиксное ядро множества слов U — это наибольшее подмножество множества U, которое вместе с каждым словом содержит все непустые префиксы этого слова. Выполняется равенство $Pk(U\cup\Lambda)=Pk(U)\cup\Lambda$ и из $U\subseteq U'$ следует $Pk(U)\subseteq Pk(U')$.

Теорема 7.3.6 (Медведев, Костич). Подмножество L моноида $F(X)$ является допустимым тогда и только тогда, когда существуют конечное множество Y, множество Медведева—Костича M над Y и алфавитный гомоморфизм f из $F(Y)$ в $F(X)$ такие, что

$L=f(M)$. Если $\Lambda\notin L$, то гомоморфизм f может быть выбран Λ-свободным.

Доказательство. 1. Чтобы показать, что образ любого множества Медведева—Костича при алфавитном гомоморфизме является допустимым множеством, нам на основании следствия 7.2.5 достаточно лишь показать, что любое множество Медведева—Костича рационально.

Поскольку множества X, X^*a и X^*aX рациональны и объединение и пересечение рациональных множеств тоже рациональны (по теореме 5.5.5), то должно быть лишь показано, что префиксное ядро рационального множества рационально.

Итак, пусть $U\in Rat(X)$. Тогда существует РС-автомат A с $L(A)=U\cup\Lambda$. Так как выполняется включение $\Lambda\in L(A)$, начальное состояние автомата A оказывается и финальным состоянием. Положим теперь $A'=(Z, X, f', s, F)$, где

$$f'(z, x)=\begin{cases}f(z, x), \text{ если } z\in F,\\ \text{не определено в противном случае.}\end{cases}$$

Промежуточное утверждение. $L(A')=Pk(U)\cup\Lambda$.

Доказательство. Очевидно, что $L(A')\subseteq L(A)$.

Так как $s\in F$, то выполнено включение $\Lambda\in L(A')$. Если wx принадлежит $L(A')$ при некотором x из X, то состояние $f'(f'^*(s, w), x)$ принадлежит F и потому определено. Из определения автомата A' следует, что в этом случае $f'^*(s, w)\in F$ и потому $w\in L(A')$. Отсюда вытекает, что $L(A')=Pk(L(A'))\subseteq Pk(L(A))$.

Пусть теперь $w=x_1x_2\ldots x_n$ — слово из $Pk(L(A))$, где $x_1, \ldots, x_n$ — символы из X. Тогда каждое слово $w_i=x_1x_2\ldots x_i$ при $i=1, \ldots, n$ принадлежит $L(A)$. Поэтому состояния $z_0=s$ и $z_i=f^*(s, w_i)$ принадлежат F и выполнены равенства $z_{i+1}=f(z_i, x_{i+1})=f'(z_i, x_{i+1})$ при $i=0, 1, \ldots, n-1$.

Отсюда следует, что w принадлежит $L(A')$ и $Pk(L(A))\subseteq L(A')$. В целом получаем

$$Pk(U)\cup\Lambda=Pk(U\cup\Lambda)=Pk(L(A))=L(A').$$

Итак, множество $Pk(U)\cup\Lambda$ допустимо. Если $\Lambda\notin Pk(U)$, то $Pk(U)=(Pk(U)\cup\Lambda)\cap F^+(X)$.

В любом случае множество $Pk(U)$ допустимо.

2. Для доказательства обратного высказывания по теореме 7.3.3 достаточно показать, что каждое стандартное множество является множеством Медведева — Костича.

Пусть $S=BX^*\cap X^*E-X^*PX^*$ — стандартное множество такое, что $B, E\subseteq X$ и $P\subseteq X^2$.

Из пп. 1 и 2 определения 7.3.5 вытекает, что следующие три множества принадлежат $MC(X)$:

$$X^*E=\cup\{X^*e\mid e\in E\},$$

$$B=\cup\{X^*b\mid b\in B\}\cap X \text{ и } C=\cup\{X^*pX\cap X^*p'\mid pp'\in X^2-P\}.$$

Если нам теперь удастся доказать следующее утверждение, то теорема будет доказана, так как тогда $S=X^*E\cap Pk(B\cup C)$ принадлежит $MC(X)$.

Промежуточное утверждение. $Pk(B\cup C)=BX^*-X^*PX^*$.

Доказательство. Выполняется равенство $C=\cup\{X^*pp'|pp'\in X^2-P\}=X^*(X^2-P)$, так что

$$Pk(B\cup C)=Pk(B\cup X^*(X^2-P)).$$

Пусть $L_i=X^i\cap Pk(B\cup C)$ при $i\in\mathbf{N}$. Тогда $L_1=B$, $L_2=BX\cap X^2-P=BX-P$ и вообще при $i\in\mathbf{N}$

$$L_{i+1}=L_iX-X^{i-1}P=BX^i-(PX^{i-1}\cup XPX^{i-2}\cup\ldots\cup X^{i-1}P).$$

Отсюда следует, что $\cup\{L_i|i\in\mathbf{N}\}=BX^*-X^*PX^*$, и потому утверждение верно. ■

Следствие 7.3.7. Каждое стандартное множество является множеством Медведева — Костича.

Дальнейшие формы представления допустимых множеств, в которых особую роль играют стандартные множества, описаны в упражнении 7.5.

7.4. ДВУСТОРОННИЕ АВТОМАТЫ

ОПРЕДЕЛЕНИЕ ДВУСТОРОННЕГО АВТОМАТА

Ниже будет приведен пример, в котором стандартные множества встретятся как «последовательности вычислений» машин. С помощью теоремы Майхилла, Хомского и Шютценбергера мы сможем при этом очень быстро установить, что автоматы описываемого ниже вида, обладающие на первый взгляд существенно большими возможностями, чем РС-автоматы, на самом деле имеют ту же самую «мощность». Мы будем исходить из описанного в разд. 5.4 представления о РС-автоматах как о читающих машинах. При этом для того, чтобы определить так называемые двусторонние автоматы, мы будем допускать, что читающая головка может передвигаться не только слева направо, но и справа налево. Точнее говоря, двусторонний автомат — это машина, состоящая из:

конечного контрольного блока, который в зависимости от входов может принимать одно из конечного множества состояний (и среди них одно начальное состояние и определенные финальные состояния);

входной ленты, разделенной на ячейки, которые занумерованы слева направо натуральными числами, начиная с 1, и могут содержать либо один из входных символов, либо быть пустыми (содержать «пустой символ»); весь (конечной длины) вход (входное слово) всегда записывается начиная слева без промежутков (пустых ячеек) на входной ленте; справа от входного слова имеются, таким образом, только пустые ячейки;

читающей головки, которая считывает символы, находящиеся в ячейках входной ленты, и передает соответствующую информа-

цию контрольному блоку; она, кроме того, по команде от контрольного блока после считывания символа перемещается на одну ячейку вправо или влево или остается на месте.

Когда автомату предлагается некоторое входное слово, то он начинает его считывание с ячейки с номером 1. Слово допускается автоматом, если он переходит в одно из финальных состояний в момент, когда читающая головка достигает правого конца этого слова.

Входное слово не допускается автоматом в следующих трех случаях:

в момент, когда читающая головка «покидает» слово справа, автомат находится в состоянии, не являющемся финальным;

читающая головка «покидает» слово слева;

читающая головка бесконечно долго читает слово (зацикливание).

Определение 7.4.1. *Двусторонний автомат* — это пятерка $A=(Z, X, f, s, F)$, где Z, X, s и F имеют то же значение, что и в случае РС-автомата, а $f: Z\times(X\cup\Lambda)\to Z\times\{-1, 0, 1\}$ — функция переходов и передвижений (читающей головки).

Равенство $f(z, x)=(z', i)$ означает, что автомат A после считывания x в состоянии z переходит в состояние z', а его читающая головка передвигается на i ячеек, а именно, влево, если $i=-1$, и вправо, если $i=1$.

Всегда выполняется равенство $f(z, \Lambda)=(z, 0)$.

Тройка (z, x, p) из $Z\times(X\cup\Lambda)\times\mathbf{N}$ называется *конфигурацией автомата* A, при этом p задает положение читающей головки автомата, находящегося в состоянии z, и x — знак, записанный в p-й ячейке входной ленты (т. е. в ячейке, обозреваемой читающей головкой).

Слово $w=x_1x_2\ldots x_n$, где $n\in\mathbf{N}$ и $x_1, x_2, \ldots, x_n$ — символы из X, *допускается* автоматом A тогда и только тогда, когда существует последовательность конфигураций (z_k, y_k, p_k), $k=1, 2, \ldots, m$, $m\in\mathbf{N}$, автомата A такая, что выполнены следующие условия:

$$f(z_k, y_k)=(z_{k+1}, i) \text{ и } p_{k+1}=p_k+i \text{ при } 1\leqslant p_k\leqslant n,$$

где $y_k=x_{p_k}$ при $k=1, 2, \ldots, m-1$, а также $z_1=s$, $p_1=1$, $z_m\in F$, $y_m=\Lambda$ и $p_m=n+1$.

Пустое слово Λ допускается тогда и только тогда, когда $s\in F$.

Реакцией $L(A)$ *автомата* A называется множество всех допускаемых автоматом A слов из моноида $F(X)$.

Замечания. 1. Если ограничить определение двустороннего автомата, задав область значений отображения f как множество $Z\times\{+1\}$, то будет получено определение одностороннего автомата, который, очевидно, соответствует приведенной в разд. 5.4 интерпретации РС-автомата. Для таких автоматов введенное в определении 7.4.1 понятие конфигурации не требуется, поскольку всегда выполняется равенство $p_k=k$. По этой причине все относящиеся к p_k условия из определения 7.4.1 могут быть опущены.

Легко понять, что в таком случае множество M всех конечных последовательностей «сокращенных» конфигураций [т. е. пар вида (z, x)], возникающих при обработке допустимых слов, является стандартным множеством. А именно M является маршрутным множеством, определяемым графом Майхилла $G'=(Z\times(X\cup\cup\Lambda), K, S\times(X\cup\Lambda), F')$ из доказательства п.2 теоремы 7.2.4 (см. также доказательство теоремы 7.3.3).

2. Любой РС-автомат работает в реальном времени, т. е. за каждый такт он обрабатывает один входной символ и после поступления на вход последнего символа слова немедленно дает ответ на вопрос о его допустимости. Напротив, для двустороннего автомата нужен буферный регистр (а именно — входная лента) для входа, причем регистр, емкость которого может по мере надобности произвольно увеличиваться, чтобы хранить входные слова произвольной длины. Кроме того, двустороннему автомату может, вообще говоря, понадобится более n тактов (шагов) для решения вопроса о допустимости входного слова длины n.

Варианты данного определения содержатся в упражнении 7.6.

ДВУСТОРОННИЙ АВТОМАТ И ЭКВИВАЛЕНТНЫЙ ЕМУ РС-АВТОМАТ

Пример 7.4.2. (См. также п.1 упражнения 7.7). Пусть $X=\{x_0, x_1, x_2, x_3\}$. Мы построим двусторонний автомат, допускающий множество U всех слов w из моноида F(X), которые начинаются символом x_0 и не содержат других вхождений x_0, но содержат по меньшей мере по одному вхождению символов x_i при $i=1, 2, 3$:

$$U=x_0X_0^*\cap X_0^*x_1X_0^*\cap X_0^*x_2X_0^*\cap X_0^*x_3X_0^*, \text{ где } X_0=\{x_1, x_2, x_3\}.$$

Способ функционирования искомого автомата очень прост. Вначале он проверяет, является ли x_0 первым символом входного слова. Если это условие выполнено, то он передвигает читающую головку вправо до тех пор, пока не будет найден символ x_1. Если этот символ найден, то автомат передвигает читающую головку на начало слова и начинает поиск символа x_2. Найдя x_2, он снова передвигает читающую головку на начало слова и начинает поиск символа x_3. Если он нашел и этот символ, то слово прочитывается до конца и допускается, если справа от первого вхождения символа x_0, в данном слове таких вхождений больше нет.

Итак, пусть двусторонний автомат A_U определяется следующим образом:

$$A_U=(\{z_0, z_1, z_2, z_3, z_0', z_1', z_2', z_3'\}, X, f, z_0, z_3'),$$

где

$$f(z_0, x_i)=\begin{cases}(z_1, +1), & \text{если } i=0\\ (z_0', +1) & \text{в противном случае;}\end{cases}$$

$$f(z_0', x_i)=(z_0', +1) \quad \text{при } i=0, 1, 2, 3;$$

$$f(z_j,\ x_f)=\begin{cases}(z_0',\ +1) & \text{при } i=0,\ j=1,\ 2,\ 3,\\ (z'_j,\ -1) & \text{при } i=j,\ j=1,\ 2,\\ (z_3',\ +1) & i=j=3,\\ (z_j,\ +1) & \text{при } i\neq j,\ j=1,\ 2,\ 3;\end{cases}$$

$$f(z'_j,\ x_l)=\begin{cases}(z_{j+1},\ +1) & \text{при } i=0,\ j=1,\ 2,\\ (z'_j,\ -1) & \text{при } i=1,\ 2,\ 3,\ j=1,\ 2,\\ (z_3',\ +1) & \text{при } i=1,\ 2,\ 3,\ j=3,\\ (z_0',\ +1) & \text{при } i=0,\ j=3.\end{cases}$$

Граф автомата A_U изображен на рис. 7.4.1.

Любой двусторонний автомат может быть представлен графом (ориентированным). На ребрах этого графа указываются входы и направление, в котором передвигается читающая головка после прочтения указанного входа.

Для того чтобы решить вопрос о допустимости слова $x_0x_3{}^nx_2x_1$ при $n\in\mathbf{N}$, автомату A_U нужно совершить ровно $(1+n+1)+(2+n)+(1+n)+1+n+2=5n+9=2(|X|-2)(n+2)+n+3-2$ шагов (передвижений читающей головки).

Нетрудно построить РС-автомат A'_U, допускающий множество U. Для решения вопроса о допустимости указанного выше слова такому автомату придется совершить только $n+3$ шагов, однако при этом он должен иметь большее число состояний. Действительно, с помощью состояний автомат должен запоминать информацию о том, какие символы он уже нашел, для чего необходимо по меньшейй мере по одному состоянию для каждого подмножества $X-\{x_0\}$, и о том, встретился ли символ x_0 в прочитанной части слова один раз или более (рис. 7.4.2).

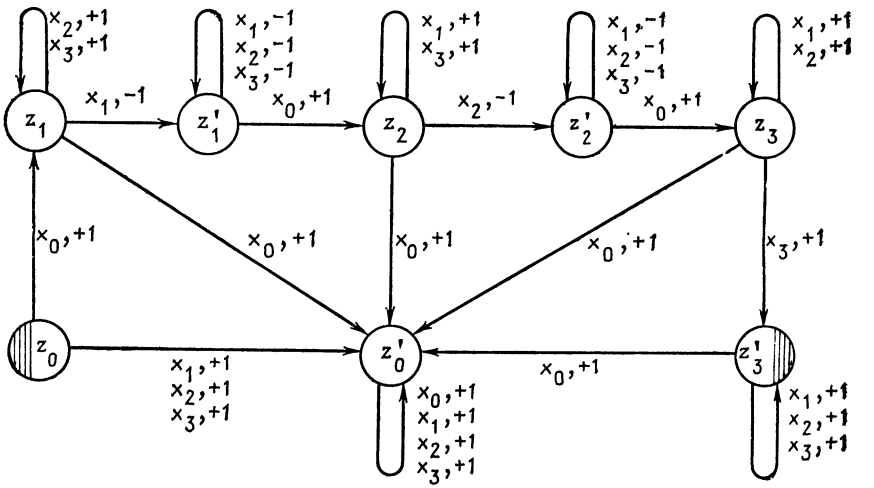


Рис. 7.4.1. Граф двустороннего автомата A_U

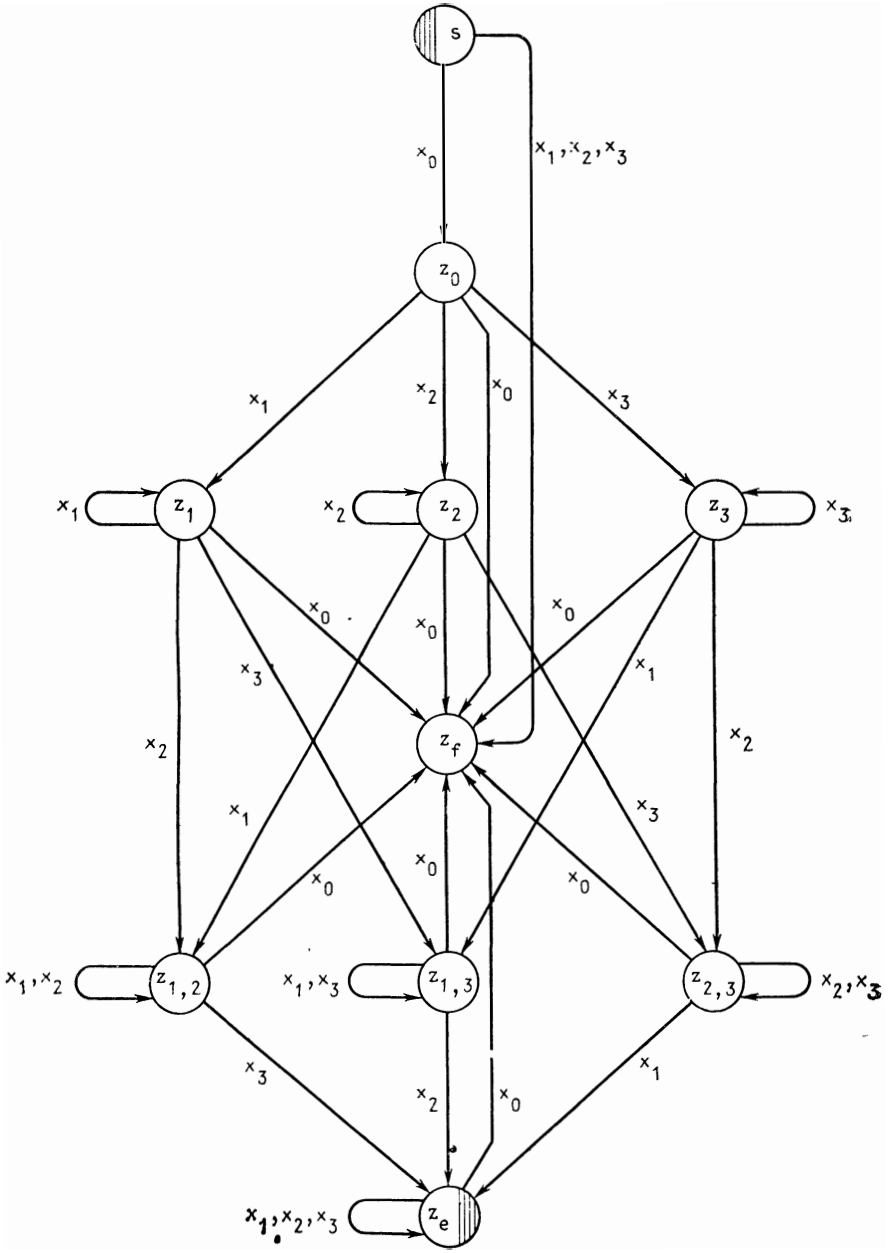


Рис. 7.4.2. Граф РС-автомата A_U'

Как показывает п.2 упражнения 7.7, различие между числом состояний двуленточного автомата и эквивалентного минимального РС-автомата может быть и существенно бо́льшим.

Замечание. Множество последовательностей конфигураций, которые возникают при обработке некоторым двусторонним автоматом допустимых слов, не является стандартным множеством, так как оно не является подмножеством никакого конечно-порожденного свободного моноида (множество конфигураций $Z \times X \times \mathbf{N}$ бесконечно). Даже и при постоянном n из **N** множество последовательностей конфигураций, возникающих при обработке слов длины n, не является стандартным множеством, поскольку для выполнения условия $y_k = x_{p_k}$ требуется, чтобы всегда имелась возможность проверки всего префикса слова (или последовательности конфигураций). Это легко понять, рассматривая пример 7.4.2: слово $x_0x_1x_2x_3$ порождает последовательность конфигураций $(z_0, x_0, 1)(z_1, x_1, 2)(z_1', x_0, 1)$

$(z_2, x_1, 2)(z_2, x_2, 3)\ (z_2', x_1, 2)(z_2', x_0, 1)$

$(z_3, x_1, 2)(z_3, x_2, 3)(z_3, x_3, 4)(z_3', \Lambda, 5)$.

Если же пренебречь условием $y_k = x_{p_k}$, то префикс $(z_0, x_0, 1)$, $(z_1, x_1, 2)(z_1', x_0, 1)$ этой последовательности можно продолжить и другим способом, скажем так: $(z_0, x_0, 1)(z_1, x_1, 2)(z_1', x_0, 1)(z_2, x_2, 2)(z_2', x_0, 1)(z_3, x_3, 2)(z_3', \Lambda, 3)$.
Данная последовательность удовлетворяет всем остальным условиям из определения, но не соответствует никакому слову из U, поскольку все слова из U имеют длину, бо́льшую чем 4.

Несмотря на сказанное, с помощью стандартных множеств (и теоремы Хомского — Шютценбергера) может быть доказана равносильность двусторонних автоматов и РС-автоматов.

РАВНОСИЛЬНОСТЬ ДВУСТОРОННИХ И РС-АВТОМАТОВ

Теорема 7.4.3. Для каждого двустороннего автомата существует РС-автомат с той же реакцией.

Доказательство. Мы будем действовать так же, как в замечании к определению 7.4.1 в частном случае одностороннего автомата. Используя замечание к примеру 7.4.2, мы можем при этом не использовать конфигурации из определения 7.4.1. Эти конфигурации имеют еще один недостаток, от которого следует избавиться: в последовательностях конфигураций, соответствующих определению 7.4.1, символы из допускаемого слова могут встречаться многократно, так что такие последовательности конфигураций, вообще говоря, оказываются более длинными, чем само слово.

Итак, будем искать модификацию понятия конфигурации. Попробуем исходить из троек вида (z, x, r), где $(z, x) \in Z \times X$, а r должно быть определено так, чтобы в последовательности конфи-

гураций, соответствующей обработке слова w, последовательность вторых компонент (символов x) представляла собой слово w и чтобы только по тройке (z, x, r) можно было определить, какая тройка может следовать непосредственно вслед за ней. С этой целью проведем следующее рассуждение.

Пусть A — двусторонний автомат в смысле определения 7.4.1. Каждое слово w из $F(X)$ задает в этом случае частичное отображение $r_w: (Z\times X)\to Z$ такое, что равенство $r_w(z, x)=z'$ выполняется тогда и только тогда, когда выполнено условие: пусть $k=|w|+1$; если слово wxv содержится на входной ленте автомата A [причем v — произвольное слово из $F(X)$], читающая головка обозревает k-ю ячейку и A находится в состоянии z, то читающая головка через конечное число тактов достигает $(k+1)$-й ячейки и z' оказывается состоянием, в котором автомат A находится в момент, когда $(k+1)$-я ячейка обозревается читающей головкой в первый раз (перед этим обозреваются только символы слова w). Формально это условие может быть выражено так: если $w=x_1x_2\ldots x_{k-1}$, где $x_j\in X$, при $j=1, .,., k-1$, то существует единственная последовательность конфигураций (z_j, y_j, p_j), $j=1,\ldots,m$ такая, что $z_1=z$, $p_1=k$, $y_1=x$, $z_m=z'$, $p_m=k+1$, $f(z_j, y_j)=(z_{j+1}, i)$, $p_{j+1}=p_j+1$, $1\leqslant p_j\leqslant k$ и $y_j=x_{p_j}$ при $j=1,\ldots,m-1$.

Значение $r_w(z, x)$ не определено тогда и только тогда, когда A «покидает» входную ленту слева или попадает в бесконечно повторяющийся цикл, начав работу в состоянии z со словом wxv на входной ленте и с читающей головкой, обозревающей k-ю ячейку.

Число всех частичных отображений конечного множества $Z\times X$ в конечное множество Z равно $(|Z|+1)^{|Z\times X|}$, поскольку путем присоединения нового элемента $u\notin Z$ можно, как известно, каждое частичное отображение g из $Z\times X$ в Z превратить в полностью определенное (тотальное) отображение g' из $Z\times X$ в $Z\cup u$ [полагая $g'(z, x)=u$ тогда и только тогда, когда значение $g(z, x)$ не определено]. Каждое такое отображение соответствует в точности одному частичному отображению из $Z\times X$ в Z.

Итак, поэтому множество $R=r_w|w\in F(X)\}$ всех определенных выше отображений r_w конечно.

Отсюда вытекает, что существует конечное подмножество W моноида $F(X)$ такое, что $R=\{r_w|w\in W\}$, причем $\Lambda\in W$ и $w\neq w'$ тогда и только тогда, когда $r_w\neq r_{w'}$.

Кроме того, существует отображение $g: W\times X\to W$ такое, что $g(w, x)=w'$, если и только если $r_{wx}=r_{w'}$.

Теперь оставшаяся часть доказательства не представляет сложности.

Пусть $M=Z\times(X\cup\Lambda)\times W$ — множество всех модифицированных конфигураций автомата A. Здесь $(z, x, w)\in M$ означает, что автомат «прочитал» слово w' такое, что $r_{w'}=r_w$, в первый раз достиг $(|w'|+1)$-й ячейки и принял при этом состояние z, а читающая головка «видит» символ x.

Пусть S — следующее стандартное множество над M:

$$S=(s\times(X\cup\Lambda)\times\Lambda)M^*\cap M^*(F\times\Lambda\times W)-M^*PM^*,$$

где $(z, x, w)(z', x', w')\in M^2-P$ тогда и только тогда, когда $x\in X$, $r_w(z, x)=z'$ и $g(w, x)=w'$.

Пусть, далее, h — следующий моноидный гомоморфизм: $h: F(M)\to F(X)$, $h(z, x, w)=x$ для каждой конфигурации (z, x, w) из M.

Тогда выполняется включение $L(A)\subseteq h(S)$. Действительно, если u принадлежит $L(A)$, то существует последовательность модифицированных конфигураций из $F(M)$, воспроизводящая последовательность ситуаций, в которых автомат A впервые прочитывает k-й символ слова u ($k=1, 2, \ldots$). Эта последовательность принадлежит, очевидно, множеству S.

Чтобы показать, что $L(A)\supseteq h(S)$, предположим, что $t=t_1t_2\ldots t_k$ — последовательность конфигураций из S. Тогда $h(t)=h(t_1\ldots t_{k-1})$, поскольку $t_k\in F\times\Lambda\times W$. Покажем теперь полной индукцией по q, что для каждого префикса $t'_q=t_1\ldots t_q$ последовательности t (при $1\leqslant q\leqslant k-1$, $t_q=(z, x, w)$ и $r_w(z, x)=z'$) может быть построена последовательность v конфигураций из $Z\times X\times \mathbf{N}$, которая в смысле определения 7.4.1 в точности является описанием того, что слово $h(t'_q)$ допускается двусторонним автоматом $A'=(Z, X, f, s, z')$, т. е. того, что автомат A за конечное число шагов целиком прочитывает слово $h(t_q')$ и переходит после этого в состояние z'.

При $k=1$ имеем $t=t_1=(s, \Lambda, \Lambda)$, так что $s\in F$ и потому $h(t)=\Lambda\in L(A)$.

Пусть теперь $k\geqslant 2$. Тогда $t_1=(s, x, \Lambda)$ при некотором x из X.

Пусть $q=1$. Тогда $t_q'=t_1=(s, x, \Lambda)$ и t_1' соответствует последовательность конфигураций $v=(s, x, 1)v_1v_2\ldots v_m(z', \Lambda, 2)$, где $v_1\ldots v_m$ — последовательность конфигураций, которая по определению отображения r_Λ отвечает соотношению $r(s, x)=z'$. Очевидно, что вторая компонента во всех v_i есть x, а третья — 1. Поэтому x допускается автоматом A'.

Предположение индукции. Утверждение выполнено при $q\geqslant 1$. Пусть тогда $k>q+1$ и $t'_{q+1}=t_q'(z', x', w')$; пусть, далее, $v(z', \Lambda, q+1)$ — последовательность конфигураций, которая по предположению индукции может быть построена для t_q'. Как и в случае $q=1$, пусть тогда $v'(z'', \Lambda, q+2)$ — последовательность конфигураций, отвечающая соотношению $r_{w'}(z', x')=z''$. Тогда, очевидно, $vv'(z'', \Lambda, q+2)$ — соответствующая t'_{q+1} последовательность конфигураций.

По предположению индукции $h(t_q')$ допускается автоматом A'. Третьи компоненты конфигураций из v' по построению все лежат между 1 и $q+1$. Если положить, что $A''=(Z, X, f, s, z'')$, то A'' допускает слово $h(t_q')x'=h(t'_{q+1})$.

Итак, выполняется равенство $L(A)=h(S)$, так что по теореме 7.3.3 множество $L(A)$ допустимо. ■

Замечание. Чтобы показать, что конструкции доказательства эффективны, следует убедиться в том, что множество R может быть определено за конечное число шагов — отсюда вытекает, что W и g также могут быть построены эффективным образом. См. по этому поводу упражнение 7.8.

7.5. АВТОМАТЫ С ПРЕДВАРИТЕЛЬНЫМ ПРОСМОТРОМ[1]

В предыдущем разделе мы видели, что (детерминированные) двусторонние автоматы могут иметь существенно меньше состояний, чем эквивалентные им РС-автоматы (см., в частности, упражнение 7.7, п.2). Теперь мы рассмотрим иную модель детерминированных автоматов, которые, вообще говоря, также могут иметь меньше состояний, чем РС-автоматы. Основная идея восходит к области синтаксического анализа контекстно-свободных языков (и соответствует рекурсивному спуску с предварительным просмотром k символов).

Мы изучим следующий вопрос: пусть задан НРС-автомат A, который будет трактоваться как читающая машина (см. замечание к определению 5.4.1); можно ли сделать процесс работы этого автомата детерминированным, разрешив автомату A (в качестве ослабленного варианта идеи двусторонних автоматов) в каждом состоянии просматривать входную ленту на k символов вперед и в зависимости от этих символов решать, какой из возможных переходов должен быть реализован? Это можно представить себе, предположив, что A обладает читающей головкой, способной одновременно считывать содержимое k соседних ячеек входной ленты и передвигающейся за такт всегда только на одну ячейку вправо. При этом следует еще предположить, что входная лента на (k—1) ячеек длиннее, чем входное слово, и что все «дополнительные» ячейки пусты, так что читающая головка, достигая конца входного слова, видит только пустые ячейки.

Пример 7.5.1. Рассмотрим НРС-автоматы, графы которых изображены на рис. 7.5.1.

Автомату A_4 для детерминированного считывания слова abba необходим предварительный просмотр четырех ячеек. Действительно, если читающая головка обозревает первое a и автомат находится в состоянии 1, то возможны как переход в состояние 2, так и переход в состояние 3. Какой из переходов должен быть реализован, нельзя решить на основе рассмотрения первых трех символов слова, поскольку для того, чтобы допустить слово abbb, автомат должен перейти в состояние 2 (из состояния 1).

Для автомата A_4 предварительный просмотр четырех символов является и достаточным, поскольку:

в состоянии 1 вход aa должен приводить к переходу в состояние 3, а вход aba — к переходу в состояние 2;

---

[1] В оригинале — Automaten mit Vorausschau. — *Прим. перев.*

в состоянии 2 входы bb и baa должны приводить к переходу в состояние 3, а вход bab — к переходу в состояние 4.

Автомат A_m «многозначен», т. е. существуют слова, которые могут допускаться этим автоматом при различных последовательностях принимаемых состояний (так что предварительный просмотр не может избавить от недетерминированности) — примерами являются слова ab и abb.

Автомат A_u не является «многозначным», поскольку любое допускаемое этим автоматом слово заканчивается либо символами ab — тогда предпоследнее состояние 2, либо символами bb — тогда предпоследнее состояние 5.

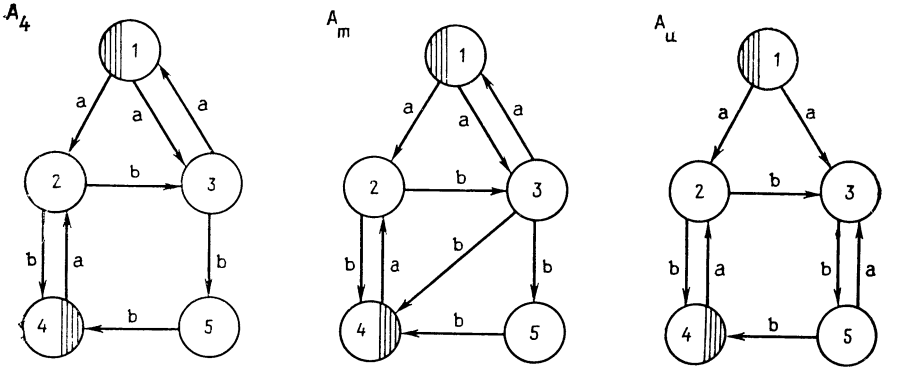


Рис. 7.5.1. НРС-автоматы A_4, A_m и A_u

Для автомата A_u необходим, однако, неограниченно большой предварительный просмотр. Действительно, при любом k предварительный просмотр 2k+2 ячеек не может помочь решить вопрос о выборе перехода из состояния 1 в 2 или из 1 в 3 при обработке допустимых слов $a(ba)^kb$ и $a(ba)^kbb$.

Итак, для того чтобы получить детерминированные автоматы, допускающие множества $L(A_u)$, $L(A_m)$ и $L(A_u)$, автоматы A_m и A_u следует преобразовать в эквивалентные ДРС-автоматы или в двусторонние автоматы. Автомат же A_4 достаточно снабдить «механизмом предварительного просмотра», который в простейшем случае представляет собой читающую головку, способную одновременно обозревать содержимое четырех ячеек, и таблицами для состояний 1 и 2, задающими при различных результатах предварительного просмотра (например, для состояния 2 — при словах bb, baa и bab) состояние, в которое должен быть совершен следующий переход (т. е. 3, 3 и 4 для состояния 2).

Пример 7.5.2. Существенное уменьшение числа необходимых состояний при использовании предварительного просмотра демонстрируют примеры 6.1.1 и 6.1.2. Определяемые графами, изображенными на рис. 6.1.1 и 6.1.3, НРС-автоматы могут допускать множества E_k и U_k детерминированным образом при предварительном просмотре (k+1) ячеек. Действительно, до тех пор пока

справа при предварительном просмотре не найден конец слова, автомат, граф которого изображен на рис. 6.1.1, должен переходить из состояния i в состояние $i+1$, а автомат, граф которого изображен на рис. 6.1.3, должен оставаться в состоянии 0. Когда же читающая головка при предварительном просмотре впервые обнаружит пустую ячейку, то при входе b первый из автоматов должен совершить переход в состояние $k+1$, а второй — в состояние 1.

Чтобы разумным образом рассматривать поставленный выше вопрос, целесообразно несколько ограничить класс изучаемых НРС-автоматов.

1. Поскольку анализируется вопрос о детерминированном способе работы, можно рассматривать только случай, когда автомат имеет только одно начальное состояние и когда нет переходов из финальных состояний. Иными словами, когда автомат, «приняв решение» о допустимости некоторого слова, т. е. перейдя в финальное состояние, больше не может его покинуть. В частности, начальное состояние в таком случае не может быть и финальным состоянием, так как иначе автомат не будет допускать ни одного слова.

2. Поскольку считывание входного слова посимвольное, изучаемые автоматы должны быть побуквенными.

3. Автоматы, конечно, должны быть неизбыточными.

Ясно, что «с точностью до пустого слова» приведенные условия не являются существенным ограничением. Действительно, если A — произвольный НРС-автомат с $\Lambda \notin L(A)$ и A' — эквивалентный автомату A D-минимальный ДРС-автомат, то можно получить эквивалентный автомату A НРС-автомат A'', удовлетворяющий приведенным выше условиям, если добавить к A' новое состояние e, добавить для каждого перехода в финальное состояние автомата A' по соответствующему переходу в состояние e и объявить e единственным финальным состоянием автомата A''.

Если НРС-автомату A из описанного класса сопоставить праволинейную грамматику (в смысле разд. 5.2) и отбросить в правилах этой грамматики знак финального состояния e, то будет получена грамматика с правилами вида $z \to xz'$ и $z \to x$ при $z, z' \in Z$ и $x \in X$ и единственным начальным символом s. Таким образом, для порождаемого грамматикой G языка будет выполняться равенство

$$L(G) = \{w \in F(X) \mid s \Rightarrow^*_G w\} = L(A).$$

Определение 7.5.3. 1. Неизбыточный побуквенный НРС-автомат $A = (Z, X, t, s, e)$ с $s \neq e$ и $t(e, X) = \varnothing$ называется *автоматом с предварительным просмотром.*

2. Автомат с предварительным просмотром A называется *многозначным,* если существуют слова u и v из $F^+(X)$ и состояния z и z' из Z такие, что $z \neq z'$, $\{z, z'\} \subseteq t^*(s, u)$ и $e \in t^*(z, v) \cap t^*(z', v)$. Автомат с предварительным просмотром, не являющийся многозначным, называется *однозначным.*

3. Для каждого k из **N** *k-префикс* $a_k(w)$ слова w из F(X) определяется отображением $a_k: F(X) \to F(X)$:

$$a_k(w) = \begin{cases} w, & \text{если } |w| \leqslant k, \\ u, & \text{если } w = uv \text{ при } |u| = k \end{cases}$$

(см. п.1 упражнения 5.9).

4. Однозначный автомат с предварительным просмотром A называется *k-детерминированным*, если существует натуральное число k такое, что при произвольных u, v и v′ из F(X), произвольном x из X и произвольных z_0, z и z′ из Z выполнено условие: из $z_0 \in t^*(s, u)$, $(z_0, x, z) \in \tau$ и $e \in t^*(z, v)$, $(z_0, x, z') \in \tau$ и $e \in t^*(z', v')$ и из равенства $a_k(xv) = a_k(xv')$ следует, что $z = z'$.

5. k-детерминированный автомат с предварительным просмотром называется автоматом с предварительным k-просмотром, если он не является (k—1)-детерминированным.

Замечания. 1. 1-детерминированный автомат с предварительным просмотром является ДРС-автоматом.

2. Построенный выше для произвольного НРС-автомата A эквивалентный автомат с предварительным просмотром A″ является однозначным и даже автоматом с предварительным 1-просмотром.

3. Если автомат с предварительным просмотром многозначен, то должны существовать z, z′ и z″ в Z такие, что $z' \neq z''$, и должен существовать вход x в X такой, что $z \in t(z', x) \cap t(z'', x)$.

4. Если автомат A является k-детерминированным, то он является и (k+1)-детерминированным.

5. Если A — автомат с предварительным k-просмотром, $k \geqslant 2$, то при произвольных z_0, z и z′ из Z, x из X и v из F(X) таких, что $z \neq z'$ и $|v| \geqslant k-1$, выполнено условие: из $\{z, z'\} \subseteq t(z_0, x)$ следует, что $t^*(z, v) = \varnothing$ либо $t^*(z', v) = \varnothing$. Действительно, вследствие неизбыточности автомата A в противном случае должны бы были существовать слова w и w′ в F(X) такие, что $e \in t^*(z_0, xvw) \cap \cap t^*(z_0, xvw')$. Но это противоречит соотношению $z \neq z'$, так как $a_k(xvw) = a_k(xvw')$.

Теорема 7.5.4. 1. Вопрос о многозначности автоматов с предварительным просмотром разрешим.

2. Разрешим вопрос: существует ли для данного автомата с предварительным просмотром A число k такое, что A является k-детерминированным автоматом?

Доказательство. Пусть A — автомат с предварительным просмотром и с (n+1) состоянием и P — множество всех неупорядоченных пар (двухэлементных множеств) нефинальных состояний автомата A: $P = \{\{z, z'\} \subseteq Z - e \mid z \neq z'\}$. Тогда $|P| \leqslant n(n-1)/2$. Пусть, далее, $P_a = \{p \in P \mid$ существуют $z \in Z$, $x \in X$ такие, что $p \subseteq t(z, x)\}$; $P_e' = \{\{z, z'\} \in P \mid t(z, X) = \varnothing$ или $t(z', X) = \varnothing\}$; $P_e = \{\{z, z'\} \in P \mid$ существует $x \in X$ такое, что $t(z, x) \cap t(z', x) \neq \varnothing\}$.

Если $P_a = \varnothing$, то автомат A — однозначный и 1-детерминированный.

Итак, мы можем в дальнейшем предполагать, что $P_a \neq \varnothing$.

Построим следующий НРС-автомат:

$$\bar{A} = (P, X, \bar{t}, P_a, P_e),$$

где $\bar{t}(\{z_1, z_2\}, x) = \{\{z_1', z_2'\} \in P \mid z_i' \in t(z_i, x) \text{ при } i = 1, 2\}$.

Переходом в автомате $\bar{A}$ является пара «параллельных» переходов в A; путь в графе автомата $\bar{A}$ — это пара «параллельных» путей в графе автомата A (они не имеют общей части и не перекрещиваются). Эти пути заканчиваются в элементах из P_e и P_e' (в P_e за счет слияния путей, а в P_e' — за счет того, что один из путей заканчивается).

Доказательство утверждения 1. Очевидно, что эквивалентны следующие высказывания:

P_e содержит некоторое достижимое в $\bar{A}$ состояние;

существуют $p \in P_a$, $p' \in P_e$ и $w \in F(X)$ такие, что $p' \in \bar{t}^*(p, w)$;

существуют u, v, $w \in F(X)$, $p \in P_a$ и $p' \in P_e$ такие, что $p \subseteq t^*(s, u)$, $p' \in \bar{t}^*(p, w)$ и $e \in t^*(p', v)$;

существует слово uwv, допускаемое автоматом A двумя способами, т. е. A многозначен.

Поскольку разрешим вопрос о выполнении равенства $P_a = \varnothing$, то утверждение 1 вытекает из вышесказанного (см. метод 6.2.3).

Доказательство утверждения 2. Поскольку, очевидно, разрешим вопрос о том, является ли данный автомат с предварительным просмотром 1-детерминированным, на основании утверждения 1 можно предположить, что рассматриваемый автомат A однозначен и не 1-детерминирован.

Пусть теперь $\bar{A}'$—НРС-автомат, полученный из автомата $\bar{A}$ изменением множества финальных состояний:

$$\bar{A}' = (P, X, \bar{t}, P_a, P - P_e').$$

Если A — автомат с предварительным k-просмотром при $k \geqslant 2$, то из п.5 замечаний к определению 7.5.3 следует, что ни одно слово v из моноида F(X) длины, большей либо равной (k—1), не принадлежит $L(\bar{A}')$, т. е. множество $L(\bar{A}')$ конечно.

Если, с другой стороны, A ни при одном $k \geqslant 2$ не является автоматом с предварительным k-просмотром, то для каждого $k \geqslant 2$ существуют слово v с $|v| \geqslant k-1$, состояния z_0, z и z′ из Z, вход x из X и слова w и w′ из F(X) такие, что $z \neq z'$, $\{z, z'\} \subseteq t(z_0, x)$, $e \in t^*(z_0, xvw) \cap t^*(z_0, xvw')$, т. е. такие, что $(P - P_e') \cap t^*(P_a, v) \neq \varnothing$. Итак, в этом случае множество $L(\bar{A}')$ бесконечно. Таким образом, автомат A является автоматом с предварительным k-просмотром при некотором $k \geqslant 2$ тогда и только тогда, когда множество $L(\bar{A}')$ конечно, а вопрос о конечности этого множества разрешим (см. п. 3 теоремы 5.5.9). ■

Для более глубокого ознакомления с вопросом читателю рекомендуется выполнить пп. 1 и 2 упражнения 7.9.

Следствие 7.5.5. Пусть A — однозначный автомат с предварительным просмотром, имеющий (n+1) состояние $n \geqslant 1$. Если A яв-

ляется k-детерминированным при некотором $k \geqslant 1$, то A является также и $((n(n-1)/2)+1)$-детерминированным.

Доказательство. Пусть A—k-детерминированный автомат. Из доказательства п.2 теоремы 7.5.4 следует, что множество $L(\bar{A}')$ конечно, откуда на базе доказательства п.3 теоремы 5.5.9 получаем, что наибольшая длина слов из $L(\bar{A}')$ не превышает $h=(n(n-1)/2)-1$. Отсюда вытекает, что A является $(h+2)$-детерминированным. ■

Тот факт, что полученная в следствии 7.5.5 граница точна, показан в п. 3 упражнения 7.9. ■

Высказывания теоремы и следствия могут быть сформулированы и для праволинейных грамматик, соответствующих автоматам с предварительным просмотром. Отметим, однако, что для грамматик более общего вида (например, для контекстно-свободных грамматик, соответствующих нормальной форме Бэкуса — Наура) оба высказывания теоремы теряют силу.

7.6. МАТРИЧНЫЕ ПРЕДСТАВЛЕНИЯ

Пусть A — побуквенный НРС-автомат с n состояниями. Каждый элемент t_w моноида переходов автомата A (см. теорему 5.2.3) является соответствием из множества состояний Z в себя. Его график может быть описан $n \times n$-матрицей (матрицей смежности). Отсюда получается новая характеризация рациональных множеств с помощью матричных представлений.

Определение 7.6.1. Пусть n — произвольное натуральное число и X — произвольное конечное множество.

1. Пусть $\mathcal{M}_n$ — моноид всех $n \times n$-матриц с элементами из $\mathbf{N}_0$ и обычным умножением матриц в качестве моноидной операции (и с единичной матрицей в качестве единичного элемента).

Матричным гомоморфизмом порядка n над X называется гомоморфизм μ из $F(X)$ в $\mathcal{M}_n$, для которого выполнено условие: для каждого x из X каждый элемент матрицы $\mu(x)$ равен либо 0, либо 1.

2. Подмножество L моноида $F(X)$ обладает *матричным представлением порядка n,* если существует матричный гомоморфизм μ порядка n над X и существуют n-компонентная вектор-строка ζ и n-компонентный вектор-столбец σ такие, что их компоненты равны 0, либо 1, и $L=\{w \in F(X) \mid \zeta\mu(w)\sigma \neq 0\}$.

Замечание. Пусть μ — матричный гомоморфизм порядка n над X. Пусть, далее, $Z=\{z_1, \ldots, z_n\}$. Каждому x из X может быть тогда сопоставлено соответствие t_x из Z в себя следующим образом [так, что $\mu(x)$ окажется матрицей смежности для t_x]: $z_j \in t_x(z_i)$ тогда и только тогда, когда $\mu(x)_{i,j}=1$.

Сразу видно, что матрица смежности для суперпозиции $t_y t_x$ двух таких соответствий является матрицей, которая получается из матрицы $\mu(x)\mu(y)$ при замене всех отличных от нуля элементов на 1.

Теорема 7.6.2 (Шютценбергер). Подмножество L моноида $F(X)$ рационально тогда и только тогда, когда L обладает матричным представлением.

Доказательство. Если L обладает матричным представлением $M=(\zeta, \mu, \sigma)$ порядка n и если Z и t_x (при каждом x из X) определены как в вышеприведенном замечании, то положим, что A — следующий НРС-автомат: $A_M=(Z, X, t, S, F)$, где $t(z, x)=t_x(z)$ при каждом $z\in Z$ и каждом $x\in X$, а S (соответственно F) — множество всех z_i, для которых $i=e$ компоненты $\zeta_i(\sigma_i)$ вектора $\zeta(\sigma)$ отличны от нуля.

Если, наоборот, A — допускающий множество L побуквенный НРС-автомат с n состояниями, то сопоставим ему матричное представление $M_A=(\zeta, \mu, \sigma)$ порядка n следующим образом.

Пусть $Z=\{z_1, ..., z_n\}$. Тогда положим, что i-я компонента вектора $\zeta(\sigma)$ при $i=1, ..., n$ равна 1 тогда и только тогда, когда $z_i\in S$ ($z_i\in F$). Положим, далее, что при каждом x из X $\mu(x)$ — матрица смежности для t_x, т. е. что $\mu(x)_{i,j}=1$ тогда и только тогда, когда $z_j\in t_x(z_i)=t(z_i, x)$, т. е. когда в графе автомата A существует ребро с меткой x, ведущее из z_i в z_j.

Сразу видно, что описанные конструкции «взаимно обратны»: если применить второй метод к A_M, то будет получена тройка $M=(\zeta, \mu, \sigma)$, по которой строился автомат A_M; если применить к тройке $M_A=(\zeta, \mu, \sigma)$, построенной для автомата A, первый метод, то снова будет получен A.

Итак, остается показать, что L(A) имеет матричное представление M_A.

Пусть $w\in F(X)$. Тогда, очевидно, $\mu(w)_{i,j}$ — число различных путей в графе автомата A, ведущих из z_i в z_j, таких, что последовательности меток на ребрах составляют слово w, так что из $\mu(w)$ можно получить матрицу смежности для t^*_w, если все отличные от нуля элементы заменить на 1. При этом j-я компонента $\zeta\mu(w)$ отлична от нуля тогда и только тогда, когда $z_j\in t^*(S, w)$. Так что $\zeta\mu(w)\neq 0$ тогда и только тогда, когда $t^*(S, w)\cap F\neq \varnothing$, т. е. L(A) обладает матричным представлением M_A. ■

Замечания. 1. Для $x\in X$ матрицу $\mu(x)$ можно получить из матрицы сопоставленной автомату A (в смысле п.2 определения 5.6.3) системы равенств, если положить, что $\mu(x)_{1,j}=1$ тогда и только тогда, когда $x\in L_{1j}$.

2. Если предположить, что A — автомат с предварительным просмотром (см. определение 7.5.3), то для L(A) получится матричное представление, в котором ζ и σ будут иметь по единственному отличному от нуля элементу. Соответствующим выбором нумерации состояний ($s=z_1$, $e=z_n$) можно тогда добиться того, что $w\in L(A)$ в точности тогда, когда элемент $\mu(w)_{1,n}$ в верхнем правом углу матрицы $\mu(w)$ отличен от нуля. Автомат A оказывается многозначным тогда и только тогда, когда существует слово w такое, что $\mu(w)_{1,n}>1$. Поскольку для каждого рационального множества L с $\Lambda\notin L$ существует автомат с предварительным 1-просмотром и реакцией L, то каждое рациональное

подмножество полугруппы $F^*(X)$ обладает матричным представлением, в котором элементами матрицы $\mu(w)$ являются только 0 и 1 и для которого $w \in L(A)$ тогда и только тогда, когда $\mu(w)_{1,n} = 1$.

3. Если A — ДРС-автомат, то ζ имеет только один отличный от нуля элемент и все $\mu(w)$ состоят только из нулей и единиц.

4. Вместо матриц над $\mathbf{N}_0$ достаточно рассматривать булевы матрицы (с элементом 0 и 1)и определить матричное умножение, заменив в обычном определении операции $+$ и $\cdot$ на булевы операции $\bigvee$ и $\bigwedge$.

5. Поскольку, вообще говоря, элементами $\mu(w)$ могут быть произвольные натуральные числа, можно допустить, чтобы и элементами $\mu(w)$ при x из X также могли быть произвольные натуральные числа. В графе (см. замечания к определению 7.6.1), соответствующем такому «кратному» матричному гомоморфизму, могут в том случае появиться кратные ребра: если $\mu(x)_{i,j} = k$, то в графе имеется k ребер с меткой x, ведущих из z_i в z_j (или одно ребро с меткой $k \cdot x$).

Для более глубокого знакомства с вопросом читателю рекомендуется выполнить упражнение 7.10.

7.7. НРС-АВТОМАТЫ С ОДНОЭЛЕМЕНТНЫМ ВХОДНЫМ АЛФАВИТОМ

В данном разделе рассматриваются НРС-автоматы с входным алфавитом $\{a\}$.

Отображение унарного представления, которое натуральному числу n сопоставляет слово a^n, является изоморфизмом аддитивного моноида $(\mathbf{N}_0, +)$ (с обычным сложением в качестве моноидной операции и единичным элементом 0) на $F(\{a\})$. Таким образом, рациональные подмножества моноида $F(\{a\})$ могут быть охарактеризованы с помощью подмножеств множества $\mathbf{N}_0$.

Теорема 7.7.1. L является рациональным подмножеством моноида $F(\{a\})$ тогда и только тогда, когда существуют конечные подмножества F_1 и F_2 моноида $F(\{a\})$ и число p такие, что $L = F_1 \cup F_2\{a^p\}^*$.

Доказательство. Пусть A — минимальный РС-автомат с реакцией L. Тогда граф автомата A имеет вид, показанный на рис. 7.7.1.

Пусть $Z = \{z_1, \ldots, z_n\}$, $s = z_1$, $f(z_i, a) = z_{i+1}$ при $i = 1, \ldots, n-1$, $f(z_n, a) = z_q$, $p = n + 1 - q$ и $F = \{z_{i_1}, z_{i_2}, \ldots, z_{i_m}\}$, где $i_j < i_k$ при $j < k$.

Тогда

$L(A) = \{a^i \mid$ существует j такое, что $i = i_j < q\} \cup \{a^i \mid$ существует j такое, что $i = i_j \geqslant q\}\{a^p\}^*$ ■

Определение 7.7.2. 1. Подмножество P множества $\mathbf{N}_0$ вида $P = \{q + ip \mid i \in \mathbf{N}_0\}$ при $q \in \mathbf{N}_0$, $p \in \mathbf{N}_0$ называется *арифметической прогрессией* периода p.

2. Подмножество L множества $\mathbf{N}_0$ называется *конечно-периодическим,* если оно является объединением конечного множества и конечного числа арифметических прогрессий одинакового периода.

Замечание. В п. 1 и 2 упражнения 7.11 и в следствии 7.7.5 содержатся равносильные определения понятия конечно-периодического числового множества.

Следствие 7.7.3. Подмножество L моноида $F(\{a\})$ рационально тогда и только тогда, когда множество $L'=\{i \mid a^i \in L\}$ длин элементов из L является конечно-периодическим.

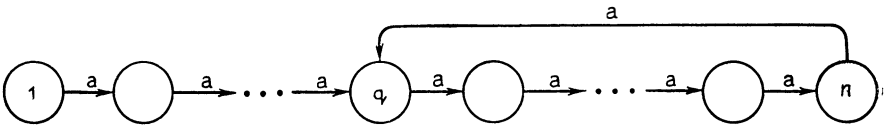


Рис. 7.7.1. Граф РС-автомата с входом a

Теперь мы имеем возможность очень легко доказать п.2 следствия 5.4.7 и аналогичные высказывания. В качестве примера в дополнение к следствию 5.5.8 покажем, что множество всех унарных представлений квадратов натуральных чисел не является рациональным (см. упражнение 5.15, п. 2).

Следствие 7.7.4. $\{a^{n^2} \mid n \in \mathbf{N}_0\}$ не рационально.

Доказательство. Если бы множество $Q=\{n^2 \mid n \in \mathbf{N}_0\}$ было конечно-периодическим, то должно бы было существовать $p \in N$ такое, что при достаточно больших n вместе с n^2 и n^2+p принадлежало бы Q. Но при $n>p$ имеем $(n+1)^2=n^2+2n+1>n^2+p>n^2$, так что число n^2+p не может быть квадратом целого числа, следовательно, предположение ложно. ■

Из следствия 7.7.3 немедленно вытекает, что в п.2 определения 7.7.2 можно отказаться от требования равенства периодов.

Следствие 7.7.5. Подмножество Q множества $\mathbf{N}_0$ является конечно-периодическим тогда и только тогда, когда оно является объединением конечного множества и конечного числа (произвольных) арифметических прогрессий.

Доказательство. Для каждой арифметической прогрессии P множество $\{a^p \mid p \in P\}$ по следствию 7.7.3 является рациональным множеством. Если Q — объединение конечного множества и конечного числа арифметических прогрессий, то и множество $\{a^n \mid n \in Q\}$ рационально. Отсюда по следствию 7.7.3 получаем, что множество Q — конечно-периодическое. ■

Пусть X — произвольное конечное множество. Тогда существует естественный алфавитный гомоморфизм h_1 из $F(X)$ на $F(\{a\})$, определенный равенством $h_1(w)=a^{|w|}$. С его помощью из сказанного выше получаем следующую теорему.

Теорема 7.7.6. Пусть X — произвольное конечное множество. Если $L \in \mathrm{Rat}(X)$, то $\{|w| \mid w \in L\}$ — конечно-периодическое множество.

Доказательство. Пусть h_1 — определенное выше отображение, которое в силу $h_1(\Lambda)=0$ и $h_1(x)=a$ при любом x из X и $|uv|=|u|+|v|$ является алфавитным гомоморфизмом.

Тогда вместе с L по следствию 7.2.5 оказывается рациональным и $h_1(L)$, и потому множество $\{|w| \mid w\in L\}=\{i \mid a^i\in h_1(L)\}$ — конечно-периодическое. ■

УПРАЖНЕНИЯ

7.1. 1. (Манна.) Докажите, что описанные ниже в обозначениях алгольного типа схемы Янова S_1 и S_2 эквивалентны:

```
(S1)   BEGIN(x); y: = x;
       if p1(y) then go to M1;
       if p2(y) then FALSE;
       if p1(y) then go to M2;
       y: = f5(y); z:=y; END;
M2:    y: = f4(y); z: = y; END;
M1:    if p2(y) then go to M3;
       y: = f2(y);
       if p1(y) then go to M4;
       y: = f3(y);
M5:    if p2(y) then go to M6;
       z: = y; END;
M6:    y: = f3(y); go to M5;
M4:    y: = f3(y);
       if p2(y) then go to M4;
       z: = y; END;
M3:    if p1(y) tnen go to M3;
       y: = f1(y); z: = y; END.
(S2)   BEGIN(x); y: = x;
       if p2(y) then FALSE;
       if p1(y) then go to M1;
       y: = f5(y); z: = y; END;
M1:    y: = f2(y);
M2:    y: = f3(y);
       if p2(y) then go to M2;
       z: = y; END.
```

2. (Гарленд, Лакем.) Рассмотрите следующую описанную в обозначениях алгольного типа рекурсивную схему:

```
BEGIN (x);
F(x):=if p(x) then x else G(x);
G(x):=if q(x) then f(F(f(x))) else g(F(g(x))),
```

где p и q — заданные предикатные, f и g — заданные функциональные константы.

По аналогии с примером 7.1.1 определите для этой схемы множество последовательностей вычислений и докажите после этого, что не может быть определена схема Янова, обладающая таким множеством последовательностей вычислений.

7.2. 1. Исследуйте связь между схемами Янова и схемами программ, удовлетворяющими приведенным в примере 5.1.2 условиям. В частности, определите понятие языка значений схем Янова, постройте гомоморфизм, отображающий множество последовательностей вычислений на язык значений и докажите, что множество всех языков значений схем Янова равно множеству Rat всех рациональных множеств.

2. (Гарленд, Лакем.) Покажите, что ни одна схема Янова не эквивалентна следующей схеме программ (в частности, не обладает таким же языком значений):

BEGIN(x); (w, y, z) := (x, x, x);
M_1: x := f(x);
if p(w) **then go to** M_2;
w := f(w);
go to M_1;
M_2: **if** p(y) **then** END(x);
y := f(y);
w := z;
go to M_1.

7.3. Обобщите понятие взвешенного графа Майхилла следующим образом: обобщенным взвешенным графом Майхилла называется шестерка G=(E, K, X, h, S, F) такая, что G′=(E, K, S, F) — граф Майхилла и h : F(E)→F(X) — произвольный сюръективный гомоморфизм. Взвешенное маршрутное множество определим как h(W(G′)).

1. Распространите теорему о графах Майхилла на случай обобщенных взвешенных графов Майхилла.

2. Докажите следствие 7 2 5 для неалфавитного f.

7.4. (Майхилл, Боднарчук.) Для стандартных множеств S_i над X_i (i=1, 2) покажите следующее.

1. $S_1 \cup S_2$ и $S_1 S_2$ — стандартные множества над $X_1 \cup X_2$ при предположении о дизъюнктности X_1 и X_2; предположение о дизъюнктности необходимо.

2. $S_1 \cap S_2$ — стандартное множество над $X_1 \cup X_2$ в любом случае.

3. $S_1^+ = S_1^* - \Lambda$ — стандартное множество над X_1.

7.5.* (Миркин.) Пусть X — конечное множество. Определим над F(X) новую частичную операцию ∘ следующим образом: $\Lambda \circ \Lambda = \Lambda$ и

$$u \circ v = \begin{cases} u'xv', & \text{если } u = u'x \text{ и } v = xv' \text{ при } x \in X, \\ \text{не определено в противном случае.} \end{cases}$$

Пусть, далее, для подмножеств U и V моноида F(X)

$U \circ V = \{u \circ v \mid u \in U, v \in V, u \circ v \text{ определено}\}$,

$U^{\circ\circ} = \{\Lambda\} \cup X \cup U \cup U \circ U \cup U \circ U \circ U \cup \ldots$

Пусть, наконец, PRat(X) (множество так называемых псевдорациональных множеств) — наименьшее подмножество булеана $\mathscr{P}(F(X))$, содержащее множества $\varnothing$, $\{\Lambda\}$, $\{x\}$ и xX при каждом x из X и содержащее вместе с любыми двумя множествами U и V также и множества $U \circ V$, $U \cup V$ и $U^{\circ\circ}$.

Покажите теперь, что:

1) $PRat(X) = Rat(X)$;

2) каждое стандартное множество над X может быть записано как псевдорациональное множество вида $B \circ U^{\circ\circ} \circ E$, где $U \subseteq X^2$.

7.6. 1. Покажите, что двусторонний автомат, у которого начало и конец любого входного слова маркируются специальными знаками (a и o) (т. е. его читающая головка без труда может установить, находится ли она в начале или в конце слова), также может допускать только рациональные множества слов (без начальной и конечной маркировки). Это означает, что если $A = (Z, X, f, s, F)$ с $X = \{a, o\} \cup X'$, где $a, o \notin X'$ — двусторонний автомат, то множество $L'(A) = \{w \in F(X) \mid awo \in L(A)\}$ рационально.

Покажите, далее, что при использовании начальной и конечной маркировки можно не применять остановку читающей головки.

2. (Патерсон.) Покажите, что при каждом $k \geqslant 2$ множество U_k из примера 6.1.2 может допускаться двусторонним автоматом описанного в п.1 вида, имеющим $k+5$ состояний, причем для обработки слова длины n ему понадобятся $n+2k+2$ тактов. [Указание. Используйте рис. 6.1.4.] Какое число состояний понадобится для «нормального» двустороннего автомата без начальной и конечной маркировки?

7.7. 1. (Барнес.) В качестве обобщения примера 7.4.2 задайте для $X = \{x_0, x_1, \ldots, x_n\}$, $n \in \mathbf{N}$, двусторонний автомат с $2n+2$ состояниями, допускающий множество U всех слов из $F(X)$, начинающихся символом x_0 и не содержащих других вхождений этого символа, в которых каждое x_i, $i = 1, \ldots, n$, встречается по меньшей мере один раз.

Покажите, далее, что РС-автомат с реакцией U должен иметь не менее 2^n+2 состояний. [Указание. Используйте следствие 6.6.3.]

2. (Мейер, Фишер.) Покажите, что при каждом n из $\mathbf{N}$ следующее конечное множество F_n может допускаться некоторым двусторонним автоматом с $5n+6$ состояниями, и докажите, что минимальный РС-автомат, допускающий F_n, должен иметь по меньшей мере n^n состояний:

$$F_n = \{0^{i_1}10^{i_2}1 \ldots 10^{i_n}2^k0^{i_k} \mid 1 \leqslant k \leqslant n$$

и $1 \leqslant i_j \leqslant n$ при $j = 1, \ldots, n\}$.

Сколько состояний должен иметь (по меньшей мере) допускающий F_n НРС-автомат?

7.8. Докажите, что конструкции доказательства теоремы 7.4.3 эффективны. В частности, докажите, что множества R и W и отображение g могут быть построены эффективным образом.

7.9. (Острэнд, Полл, Уэйкер.) 1. Предложите алгоритм, устанавливающий для данного автомата с предварительным просмотром, является ли этот автомат однозначным, и если это так, то является ли он k-детерминированным при некотором k из $\mathbf{N}$.

2. Предложите метод, управляющий процессом обработки входных слов автоматом с предварительным k-просмотром, не используя при этом таблицы

соответствия результатов предварительного просмотра и «следующих» состояний (поскольку они могут занимать слишком много места). Этот метод работает, конечно, медленнее, чем приведенный в примере 7.5.2.

3. Докажите, что следующий НРС-автомат является автоматом с предварительным $((n(n-1)/2)+1)$-просмотром:

$A=(\{z_1, \ldots, z_n, e\}, \{x_0, x_1, \ldots, x_m\}, t, z_1, e)$, $n=2m$ или $n=2m-1$,

$t(z_1, x_0)=\{z_1, z_2\}$, $t(z_2, x_2)=t(z_{n-1}, x_1)=\{e\}$,

$t(z_i, x_1)=\{z_{i+1}\}$ при $i=1, 2, \ldots, n-1$, $t(z_n, x_j)=\{z_1\}$ при $j=2, 3, \ldots, m$,

$t(z_{n-i}, x_{1+i})=\{z_{2+i}\}$,

$t(z_{1+i}, x_{1+i})=\{z_{n+1-i}\}$ при $i=1, 2, \ldots, m-1$.

7.10. 1. Постройте матричное представление множества, допускаемого НРС-автоматом из примера 5.1.2 (см. также пример 5.2.4).

2. Докажите, не используя ранее доказанных теорем (т. е. только с помощью рассуждений о матричных гомоморфизмах и т. п.), что $Rat(X)$ содержится в множестве всех подмножеств моноида $F(X)$, обладающих матричными представлениями конечного порядка. Иными словами, покажите, что множества $\varnothing$ и $\{x\}$ обладают таким представлением, что вместе с U и V также и $U \cup V$, UV и U^* обладают теми же представлениями.

3. (Берстел.) Пусть $X=\{0, 1\}$, $Z=\{z_1, z_2\}$ $\zeta=(1, 0)$, $\sigma=\begin{pmatrix}0\\1\end{pmatrix}$,

$$\mu(0)=\begin{Vmatrix}1 & 0\\ 0 & 2\end{Vmatrix}, \quad \mu(1)=\begin{Vmatrix}1 & 1\\ 0 & 2\end{Vmatrix}.$$

Докажите, что для $u \in F(X)$ равенство $\zeta\mu(u)\sigma=k$ выполняется тогда и только тогда, когда u является двоичным представлением (возможно, с дополнительными нулями) числа k.

Для наглядности представьте μ (как упоминалось в п.5 замечаний к теореме 7.6.2) как граф с кратными одинаково помеченными ребрами между двумя вершинами.

7.11. 1. (Майхилл.) Докажите, что подмножество Q множества $\mathbf{N}_0$ в точности тогда является конечно-периодическим, когда Q конечно или когда существуют p и q такие, что при каждом $n \geqslant q$ выполнено условие: $n \in Q$ тогда и только тогда, когда $n+p \in Q$.

2. (Майхилл.) Бесконечная последовательность $y_1, y_2, \ldots, y_n, \ldots$ натуральных чисел называется конечно-периодической, если существуют $r \geqslant 0$ и $s \geqslant 1$ такие, что при всех $n \geqslant r$ выполнено равенство $y_{n+s}=y_n$.

Пусть Q — бесконечное подмножество множества N_0. Пусть тогда S_Q — бесконечная последовательность $k_1, k_2, \ldots$ элементов множества Q в порядке возрастания $(k_1<k_{i+1})$ и пусть D_Q — бесконечная последовательность разностей $k_1, k_2-k_1, k_3-k_2, \ldots, k_{i+1}-k_i, \ldots$

Докажите, что подмножество Q множества $\mathbf{N}_0$ является конечно-периодическим тогда и только тогда, когда либо множество Q конечно, либо последовательность D_Q является конечно-периодической.

3 Докажите, что следующие множества не рациональны: $\{a^{2^{2^k}} \mid k \in \mathbf{N}\}$, $\{a^{2^k} \mid k \in \mathbf{N}\}$, $\{a^{n!} \mid n \in \mathbf{N}\}$, $\{a^p \mid p$ — простое число$\}$ (см. п.3 упражнения 5.15).

Схема Янова, изображенная на рис. 7.1.1, основана на одной программе Кнута; по этому поводу, а также по поводу теории схем Янова и упражнений 7.1 и 7.2 см. [30] из списка литературы к гл. 5. Схемы Янова были введены и подробно исследованы в [8].

Графы Майхилла (см. определение 7.2.1) и стандартные множества (см. определение 7.3.1) рассматривались уже в [37] из списка литературы к гл. 5. Там же были в основном доказаны теоремы 7.2.4, 7.3.3, 7.3.4, 7.7.1 и 7.7.6, лемма 7.3.2, следствия 7.2.5 и 7.7.3 и высказывания из упражнений 7.4 и 7 11, пп. 1, 2.

Понятие стандартного множества было независимо введено в [10] из списка литературы к гл. 5. Там же была снова доказана теорема 7.3.3. Эта же теорема была почти одновременно доказана в [3] (см. также [11] из списка литературы к гл. 5). Поскольку Хомский и Шютценбергер сделали теорему 7.3.3 центральной теоремой теории рациональных множеств, то она обычно и называется теоремой Хомского — Шютценбергера.

Понятие локального множества было введено в [3] из списка литературы к гл. 2.

Синтаксические диаграммы для языка Паскаль (пример 7.2.3) можно найти в любом описании этого языка, например в [26] из списка литературы к гл. 5.

Теорема 7.3.6 — это доказанная в [4] модификация (с использованием меньшего числа исходных множеств и основных операций) результата Медведева (см. гл. 5). По поводу теоремы 7.3.6 см. также [5].

Определение 7.4.1 и теорема 7.4.3 взяты из [41] из списка литературы к гл. 5. Там же и в [12] можно найти иное доказательство этой теоремы. Пример 7.4.2 взят из [1].

Содержание разд. 7.5 восходит к работе [10].

Матричные представления для рациональных множеств были введены в [11]. Там же приведены пп. 2—5 замечаний к теореме 7.6.2. Представление из определения 7.6.1 в обобщенной форме, указанной в п.5 замечаний к теореме 7.6.2, взято из [6]. По поводу раздела 7.6 см. также [2].

Упражнения 7.6, п.7 и 7.7, п 2 основаны на [16] из списка литературы к гл. 6.

ГЛАВА 8.

ПРЕОБРАЗОВАТЕЛИ И ДВУЛЕНТОЧНЫЕ АВТОМАТЫ

8.1. РЕТРОСПЕКЦИЯ

До сих пор мы рассматривали два типа автоматов:

автоматы, перерабатывающие входные последовательности в выходные; реакции таких автоматов описывались конечными множествами отображений;

автоматы, классифицирующие входные последовательности на допустимые и недопустимые; их реакции описывались с помощью подмножеств множества всех входных последовательностей.

Для обоих типов автоматов выполнялись следующие общие предположения:

каждый автомат мог принимать только состояния из некоторого конечного множества;

входами были дискретные полностью различимые между собой неделимые объекты, независимые друг от друга и вводимые в автомат один за другим (в произвольном порядке); то же относилось и к выходам.

Автоматы первого типа (автоматы Мили и Мура и частичные автоматы Мили) были введены как модели детерминированных последовательностных машин, процессов или алгоритмов, причем допускалось, что их функционирование определено не полностью. Такие автоматы при получении допустимого входа (состоящего из одного объекта) сразу (до получения следующего входа) порождают определенную реакцию — переход в новое состояние и (возможно, неопределенный) выход.

Автоматы второго типа (РС-автоматы, ДРС-автоматы, НРС-автоматы) были введены как средство представления (не обязательно детерминированных) методов анализа и классификации последовательностей символов. Для таких автоматов допускалось, что их реакции (переходы из одного состояния в другое) спонтанны (не обусловлены получением входа) или соответствуют получению на вход сразу нескольких символов. Здесь также допускалась частичная определенность. Полностью определенные и детерминированные автоматы этого типа (РС автоматы) интерпретировались очевидным образом как автоматы Мура. В то же время поведение автоматов Мура и Мили очень точно может быть описано с помощью РС-автоматов.

Очень важен тот факт, что НРС-автоматы, ДРС-автоматы и РС-автоматы обладают одинаковыми возможностями как автоматы, допускающие входные последовательности. Поэтому имеется большое число возможностей простого построения таких автоматов, преобразования их в эквивалентные и простого описания множеств, допускаемых РС-автоматами.

Аналогичные факты не будут верны для рассматриваемых ниже автоматов. Однако с некоторыми предосторожностями большое число полученных выше высказываний может быть распространено и на рассматриваемый ниже случай. Мы проанализируем с этой точки зрения некоторые важные результаты.

Автоматы всех упомянутых выше типов могут быть представлены взвешенными ориентированными графами. Такие графы представляют собой (статические) описания структур автоматов. Для того чтобы представить себе функционирование (динамическое поведение) некоторого РС-автомата, мы интерпретировали его как «читающую» («допускающую») машину или же как «пишущую» («порождающую») машину (см. разд. 5.4). Такая интерпретация может быть распространена и на случай автоматов Мили, т. е. автомат Мили можно представлять себе как машину (рис. 8.1.1), обладающую:

конечным контрольным блоком (который может принимать конечное число состояний);

входной лентой (разделенной на конечное число ячеек и бесконечно продолжаемой вправо; в каждой ячейке этой ленты может находиться один входной символ; входные слова записываются на этой ленте слева направо без пропусков);

читающей головкой (обозревающей содержимое ячеек и «информирующей» контрольный блок; после считывания очередного символа она передвигается на одну ячейку вправо; это продолжается до тех пор, пока она не выходит за пределы входного слова);

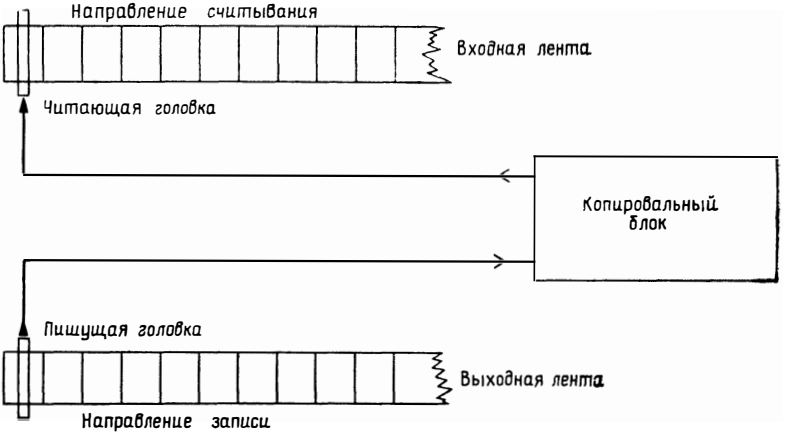


Рис. 8.1.1. Автомат Мили как читающая и пишущая машина

пишущей головкой (которая может записывать передаваемые контрольным блоком символы на выходной ленте; после записи каждого символа она сдвигается на одну ячейку вправо).

Машина начинает работу с входной лентой, на которой записано рассматриваемое входное слово, и пустой выходной лентой. При этом обе головки машины находятся над самыми левыми ячейками соответствующих лент.

Находясь в любом состоянии, контрольный блок «приказывает» читающей головке считать содержимое очередной ячейки и, в зависимости от результата считывания, «приказывает» пишущей головке записать на выходной ленте тот или иной символ, после чего переходит в новое состояние.

Эта новая интерпретация автоматов Мили показывает, что «читающая часть» этих автоматов может рассматриваться как читающий РС-автомат, а «пишущая часть» — как пишущий НРС-автомат. Автомат Мили в целом может рассматриваться, таким образом, как совокупность двух НРС-автоматов очень сходной структуры (если, скажем, каждое состояние считать и начальным, и финальным одновременно). Из графа автомата Мили можно получить граф «читающей части», если опустить все выходные

символы, и граф «пишущей части», если опустить все входные символы.

Эта интерпретация приводит к мысли о возможности обобщения понятия автомата Мили.

В данной главе мы будем использовать следующее *общее предположение:* X, X′, Y, Y′, Z и Z′ будут считаться произвольными непустыми конечными множествами (если специально не оговорено противное).

8.2. а-ПРЕОБРАЗОВАТЕЛИ

ПОСЛЕДОВАТЕЛЬНОСТНЫЕ МАШИНЫ ГИНЗБУРГА

Автоматы Мили могут вычислять только «сохраняющие длину» отображения (см. упражнение 2.7), т. е. входное и соответствующее выходное слова имеют одинаковую длину. Первое обобщение состоит в допущении того, что пищущая головка между поступлением двух последовательных входов либо записывает на выходной ленте несколько знаков, либо вообще ничего не записывает. Как и в случае РС-автоматов, одно из состояний выбирается в качестве начального. Реакцией полученного таким образом автомата оказывается реакция его начального состояния, причем она не должна, вообще говоря, быть сохраняющим длину отображением.

Автоматы только что описанного вида называются *конечными преобразователями* или *последовательностными машинами Гинзбурга.*

Легко видеть, что любой гомоморфизм h из $F(X)$ в $F(Y)$ порождается некоторым конечным преобразователем, т. е. может быть представлен как реакция последовательностной машины Гинзбурга. Такому конечному преобразователю достаточно иметь только одно состояние — при поступлении на его вход x на выход подается $h(x)$.

Итак, такой конечный преобразователь может быть определен как $M=(Z, X, Y, f, g, s)$, где $Z=\{s\}$, $f(s, x)=s$ и $g(s, x) = h(x)$ при каждом x из X. Соответствующий граф изображен на рис. 8.2.1.

По поводу дальнейших свойств конечных преобразователей см. упражнение 8.1.

Второй шаг обобщения состоит в выделении множества финальных состояний. При этом входное слово рассматривается как допустимое, если оно приводит к переходу из начального состояния в одно из финальных состояний, т. е. если оно допускается «читающей частью» автомата. Такой автомат называется *конечным преобразователем (последовательностной машиной Гинзбурга) с допускающими состояниями.*

Итак, конечный преобразователь с допускающими состояниями реализует, вообще говоря, частичное отображение, областью определения которого является рациональное множество. Очевидно, и область значений такого отображения оказывается рацио-

нальным множеством, поскольку «пишущая часть» конечного преобразователя с допускающими состояниями может рассматриваться как пишущий НРС-автомат.

Пример 8.2.1. На рис. 8.2.2 изображен граф конечного преобразователя с допускающими состояниями, реализующего отображение множества $0^*(10^*10^*)^*$ на множество $F(\{0, 1\})$:

$M_0 = (\{s, z\}, \{0, 1\}, \{0, 1\}, f, g, s, s)$,

$gr\, f = \{(s, 0, s), (s, 1, z), (z, 0, z), (z, 1, s)\}$,

$gr\, g = \{(s, 0, 0), (s, 1, 1), (z, 0, \Lambda), (z, 1, \Lambda)\}$.

По поводу дальнейших свойств конечных преобразователей с допускающими состояниями см. упражнения 8.2 и 8.3.

Рис. 8.2.1. Конечный преобразователь M_h, порождающий гомоморфизм h

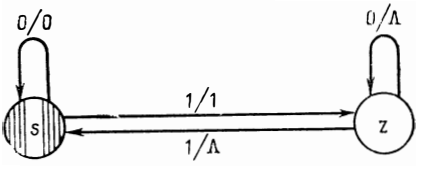


Рис. 8.2.2. Конечный преобразователь с допускающими состояниями M_0

По аналогии со случаем НРС-автоматов можно допустить и недетерминированность и частичную определенность функционирования конечных преобразователей, которые будут реализовывать в результате не только отображения, но и соответствия. Первый шаг в этом направлении можно сделать, если определить «читающую часть» рассматриваемых машин как алфавитный НРС-автомат с единственным начальным состоянием. Это приводит к понятию *недетерминированного конечного преобразователя с допускающими состояниями.* Недетерминированный конечный преобразователь с допускающими состояниями, все состояния которого являются финальными, называется *недетерминированным конечным преобразователем (недетерминированной последовательностной машиной Гинзбурга).*

ОПРЕДЕЛЕНИЕ a-ПРЕОБРАЗОВАТЕЛЯ

Если в дополнение к сказанному отказаться от требования посимвольного считывания, то мы придем к понятию a-преобразователя, играющему очень важную роль в теории формальных языков.

Определение 8.2.2. *a-преобразователем* M называется шестерка $M = (Z, X, Y, t, s, F)$, где Z, X и Y — *множество состояний, входной алфавит* и *выходной алфавит* соответственно, $s \in Z$ — *начальное состояние,* $F \subseteq Z$ — *множество допускающих (финальных) состояний* и $t = (Z \times F(X), F(X) \times Z, \tau)$ — соответствие с конечным графиком τ — *соответствие функционирования.*

M называется *алфавитным, если* $\tau \subseteq Z \times (X \cup \Lambda) \times (Y \cup \Lambda) \times Z$.

M называется *Λ-свободным, если* $\tau \subseteq Z \times F(X) \times F^+(Y) \times Z$.

Соответствие t (как и в случае НРС-автоматов) может быть продолжено до *последовательностного соответствия* $t^* = (Z \times F(X), F(Y) \times Z, \tau^*)$ следующим образом:

$\tau^0 = \{(z, \Lambda, \Lambda, z) \mid z \in Z\}$, $\tau^1 = \tau$ и при каждом n из **N**

$\tau^{n+1} = \{(z, uu', vv', z') \mid$ существует состояние $z'' \in Z$ такое, что $(z, u, v, z'') \in \tau^n$ и $(z'', u', v', z') \in \tau\}$;

$\tau^* = \bigcup \{\tau^i \mid i \in \mathbf{N}_0\}$.

a-преобразователь M порождает соответствие T_M из F(X) в F(Y), называемое *порожденным M преобразованием:*

$T_M(w) = \{v \in F(Y) \mid$ существует $z \in F$ такое, что $(v, z) \in t^*(s, w)\}$ — для каждого w из F(X).

Соответствие T_M обычным образом может рассматриваться как отображение булеана моноида F(X) в булеан моноида F(Y). Это отображение часто также обозначается символом M и называется *порожденным M a-преобразовательным отображением:* $M(L) = \bigcup \{T_M(w) \mid w \in L\}$ для любого подмножества L моноида F(X).

Порожденным M *обратным (или инверсным) a-преобразовательным отображением* M^{-1} называется отображение, определяемое равенством

$M^{-1}(L') = \bigcup \{T_M^{-1}(v) \mid v \in L'\} = \{w \in F(X) \mid$ существует $v \in L'$ такое, что $v \in T_M(w)\}$ для каждого подмножества L′ моноида F(Y).

Соответствие из F(X) в F(Y) называется *рациональным преобразованием,* если существует порождающий это соответствие a-преобразователь.

Замечания. 1. Очевидно, что каждый конечный преобразователь, каждый недетерминированный конечный преобразователь, каждый конечный преобразователь с допускающими состояниями и каждый недетерминированный конечный преобразователь с допускающими состояниями являются частными случаями a-преобразователей.

2. Не только каждый гомоморфизм h из F(X) в F(Y), но и каждое обратное к гомоморфизму отображение h^{-1} являются a-преобразовательными отображениями (см. рис. 8.2.1).

3. Вследствие равенства $M(\{w\}) = T_M(w)$ [при каждом w из F(X)] при любом подмножестве L′ моноида F(Y) выполнено равенство $M^{-1}(L') = \{w \in F(X) \mid M(\{w\}) \cap L' \neq \varnothing\}$.

Отметим, в частности, что, вообще говоря, $M^{-1}(M(\{w\})) \neq \{w\} \neq M(M^{-1}(\{w\}))$. Примером, приводящим к этому выводу, является определяемое равенствами $h(a) = h(b) = b$ рациональное преобразование h моноида $F(\{a, b\})$ в себя. Действительно, в этом случае $h^{-1}(h(a)) = \{a, b\} \neq \{a\}$ и $h(h^{-1}(a)) = \varnothing \neq \{a\}$.

4. Для рационального преобразования r из F(X) на F(Y) соответствующее a-преобразовательное отображение из $\mathscr{P}(F(X))$ на $\mathscr{P}(F(Y))$ будет часто также обозначаться символом r.

5. Как и в случае HPC-автоматов, для каждого a-преобразователя M может быть построен алфавитный a-преобразователь M′, порождающий то же преобразование: если в τ содержится переход (z, ux, vy, z′) с $u \neq \Lambda$, $v \neq \Lambda$, $x \in X$ и $y \in Y$, то введем в Z новое состояние z″ и заменим рассматриваемый переход на пару переходов: (z, u, v, z″) и (z″, x, y, z′). Аналогичным образом можно поступать и в случае, когда вместо ux или vy встречается Λ (см. п.1 упражнения 8.4).

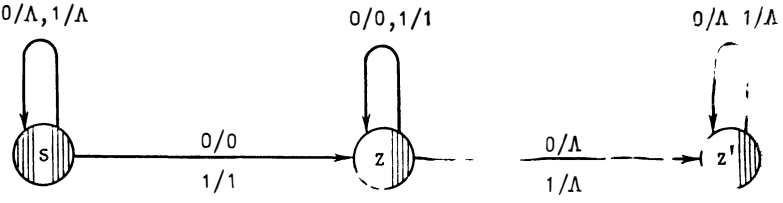


Рис. 8.2.3. a-преобразователь M_1

Пример 8.2.3. a-преобразователь, порождающий для данного слова все его подслова.

Пусть $X=Y=\{0, 1\}$, $M_1=(\{s, z, z'\}, X, Y, t, s, \{s, z, z'\})$;

$t(s, x)=\{(\Lambda, s), (x, z)\}$ — для всех x из X;

$t(z, x)=\{(x, z), (\Lambda, z')\}$ — для всех x из X;

$t(z', x)=\{(\Lambda, z')\}$ — для всех x из X.

Тогда M_1 имеет граф, изображенный на рис. 8.2.3.

Легко показать, что для каждого слова w из F(X) выполнено равенство

$T_{M_1}(w)=\{w' \in F(X) \mid$ существуют слова u и v в F(X) такие, что $w=uw'v\}$.

a-преобразователь M_1 является, очевидно, недетерминированным конечным преобразователем с допускающими состояниями.

Далее, если $L=\{0^n1^n \mid n \in N\}$, то $M_1(L)=0^*1^*$. Последнее равенство показывает, что образом не рационального множества (см. теорему 5.4.12) при a-преобразовательном отображении может быть рациональное множество. Мы скоро увидим, однако, что a-преобразователи переводят рациональные множества всегда в рациональные же.

ХАРАКТЕРИЗАЦИЯ a-ПРЕОБРАЗОВАТЕЛЬНЫХ ОТОБРАЖЕНИЙ

Прежде всего мы на основе тесной связи между a-преобразователями и HPC-автоматами получим некоторую характеризацию для a-преобразовательных отображений. Дальнейшие их свойства можно найти в упражнении 8.4.

Теорема 8.2.4. (Нивat). 1. Пусть M — a-преобразователь. Тогда эффективным образом можно задать конечное множество P, рациональное подмножество R моноида $F(P)$ и гомоморфизмы h_1 из $F(P)$ в $F(X)$ и h_2 из $F(P)$ в $F(Y)$ так, что для любого подмножества L моноида $F(X)$ будет выполняться равенство $M(L)=h_2(h_1^{-1}(L)\cap R)$.

2. Пусть P' — конечное множество, R' — рациональное подмножество моноида $F(P')$, h_1' — гомоморфизм из $F(P')$ в $F(X)$ и h_2' — гомоморфизм из $F(P')$ в $F(Y)$. Тогда эффективным образом можно определить a-преобразователь M' такой, что при любом подмножестве L моноида $F(X)$ будет выполняться равенство $M'(L)=h_2'(h_1'^{-1}(L)\cap R')$.

Доказательство. 1. Пусть $P=pr_{2,3}\tau$. Тогда M можно рассматривать как НРС-автомат A с входным алфавитом P: $A=(Z, P, \bar{t}, s, F)$ с $\bar{\tau}=\{(z, p, z')\mid p=(u, v)$ и $(z, u, v, z')\in\tau\}$.

Итак, мы рассматриваем каждую пару, состоящую из входного слова и выходного слова a-преобразователя M, как отдельный вход автомата A. В терминах приведенной выше интерпретации это означает, что мы объединяем входную и выходную ленты, пишущую и читающую головки и считаем, что выходная лента уже перед началом работы заполнена соответствующим образом, т. е. может рассматриваться как входная лента. Пара слов (w, w'), записанных на обеих лентах, допускается автоматом A тогда и только тогда, когда существуют конечная последовательность $p_1=(u_1, v_1)$, ..., $p_n=(u_n, v_n)$ элементов множества P и последовательность состояний $z_0=s$, z_1, ..., z_n с z_n из F такие, что $u_1u_2 \ldots u_n=w$, $v_1v_2 \ldots v_n=w'$ и $(z_{i-1}, (u_i, v_i), z_i)\in\tau$ при $i=1, \ldots, n$.

Последнее условие равнозначно тому, что НРС-автомат A допускает входную последовательность $p_1, p_2 \ldots p_n=(u_1, v_1)(u_2, v_2) \ldots (u_n, v_n)$, рассматриваемую как элемент моноида $F(P)$. В то же время оно же равнозначно тому, что $(z_{i-1}, u_i, v_i, z_i)\in\tau$ при $i=1, \ldots, n$, так что M при входе $w=u_1u_2 \ldots u_n$ порождает выход $w'=v_1v_2 \ldots v_n$, т. е. w' принадлежит $T_M(w)=M(\{w\})$.

Пусть теперь h_i — гомоморфизмы $(i=1, 2)$, определяемые ограничением на множество P проекций pr_i произведения $F(X)\times F(Y)$, т. е. пусть $h_1: F(P)\to F(X)$, где $h_1(p_1p_2 \ldots p_n)=h_1((u_1, v_1)(u_2, v_2) \ldots (u_n, v_n))=u_1u_2 \ldots u_n$ и $h_2: F(P)\to F(Y)$, где $h_2(p_1, p_2 \ldots p_n)=h_2((u_1, v_1)(u_2, v_2) \ldots (u_n, v_n))=v_1v_2 \ldots v_n$.

Пусть, далее, $R=L(A)$ — допускаемое автоматом A подмножество моноида $F(P)$. Мы показали, что для пары слов (w, w') из $F(X)F(Y)$ слово w' принадлежит $T_M(w)=M(\{w\})$ тогда и только тогда, когда существует элемент q множества $F(P)$, принадлежащий R, такой, что $h_1(q)=w$ и $h_2(q)=w'$.

Множество всех слов w' из $F(Y)$, принадлежащих $M(\{w\})$, получаем, таким образом, как множество всех $h_2(q)$ таких, что $q\in R$ и $h_1(q)=w$.

2. Теперь мы поступаем наоборот. Пусть A — ДРС-автомат над P', допускающий множество R'. Мы можем рассматривать

его как а-преобразователь M', считая, что входная лента и читающая головка разделены на две части каждая и что каждый входной символ p преобразован в пару $h_1'(p)$ и $h_2'(p)$, причем $h_1'(p)$ рассматривается как вход, а $h_2'(p)$ — как выход. Граф автомата A становится, таким образом, графом преобразователя M' при замене p на $h_1'(p)/h_2'(p)$. Остальные рассуждения проводятся так же, как в доказательстве п.1. ■

Замечания. 1. Легко видеть, что в п.1 теоремы 8.2.4 h_2 оказывается Λ-свободным [т. е. $h_2(p)\neq\Lambda$ при всех p из P] тогда и только тогда, когда преобразователь M Λ-свободен.

2. Поскольку суперпозиция гомоморфизмов снова является гомоморфизмом, то, используя теорему 7.3.3 (теорему Хомского — Шютценбергера), в п.1 теоремы 8.2.4 можно требовать, чтобы R было стандартным множеством (или по теореме 7.3.6 — множеством Медведева — Костича).

3. Поскольку для дизъюнктных множеств X и Y соотношениями $x\to(x, \Lambda)$ для всех x из X и $y\to(y, \Lambda)$ для всех y из Y определяется гомоморфизм из $F(X\cup Y)$ на $Q=F(X\times\Lambda\cup\Lambda\times Y)$ и поскольку для множества P из доказательства п.1 теоремы 8.2.4 моноид F(P) может рассматриваться и как рациональное подмножество моноида Q, то, используя теорему 7.3.3, в п.1 теоремы 8.2.4 множество P можно заменить на $X\cup Y$, если X и Y дизъюнктны.

4. С учетом п.5 замечаний к определению 8.2.2 в п.1 теоремы 8.2.4 можно требовать, чтобы h_1 и h_2 были алфавитными (см. п.1 упражнения 8.4).

Пример 8.2.5. Применим к а-преобразователю M из примера 8.2.3 теорему 8.2.4, п.1. Из доказательства этой теоремы получаем:

$$P=pr_{2,3}\tau=\{(0, \Lambda), (1, \Lambda), (0, 0), (1, 1)\};$$

$$h_1: F(P)\to F(X),\ h_1((0, \Lambda))=h_1((0, 0))=0;\ h_1((1, \Lambda))=$$

$$=h_1((1, 1))=1,$$

$$h_2: F(P)\to F(Y);\ h_2((0, \Lambda))=h_2((1, \Lambda))=\Lambda,\ h_2((0, 0))=$$

$$=0,\ h_2((1, 1))=1;$$

$$R=\{(0, \Lambda), (1, \Lambda)\}^*\cdot\{(0, 0), (1, 1)\}^*\cdot\{(0, \Lambda), (1, \Lambda)\}^*.$$

Отметим, что здесь слово $(0, \Lambda)(1, 1)(1, \Lambda)$ как элемент моноида F(P) отлично от $(0, \Lambda)(1, \Lambda)(1, 1)$.

Поскольку у M_1 множества входов и выходов равны, то нельзя выбрать $P=X\cup Y$. Заменим поэтому Y на множество {2, 3}, т. е. положим

$$P'=\{0, 1, 2, 3\};$$

$$h_1': F(P')\to F(X),\ h_1'(0)=0,\ h_1'(1)=1;\ h_1'(2)=h_1'(3)=\Lambda,$$

$$h_2': F(P')\to F(Y),\ h_2'(0)=h_2'(1)=\Lambda;\ h_2'(2)=0,\ h_2'(3)=1.$$

Тогда, например, имеем

$h_1'(0131)=h_1'(0113)=011=h_1((0,\Lambda)(1,1)(1,\Lambda))=$

$=h_1((0,\Lambda)(1,\Lambda)(1,1))$;

$h_2'(0131)=h_2'(0113)=1=h_2((0,\Lambda)(1,1)(1,\Lambda))=$

$=h_2((0,\Lambda)(1,\Lambda)(1,1))$.

В качестве R' выберем множество, которое при гомоморфизме из $F(P')$ в $F(\{0,1,\Lambda\}\times\{0,1,\Lambda\})$, определяемом соотношениями $0\to(0,\Lambda)$, $1\to(1,\Lambda)$, $2\to(\Lambda,0)$ и $3\to(\Lambda,1)$, отображается на множество R, причем в R пара $(0,0)$ заменяется на $(0,\Lambda)(\Lambda,0)$ и пара $(1,1)$ — на $(1,\Lambda)(\Lambda,1)$:

$R'=\{0,1\}^*\cdot\{02,13\}^*\cdot\{0,1\}^*$.

Тогда для каждого слова w из $F(X)$ выполняются равенства $M_1(\{w\})=h_2(h_1^{-1}(w)\cap R)=h_2'(h_1'^{-1}(w)\cap R')$.

Например, для $w=0^n1^n$ при n из $\mathbf{N}$ имеем:

$h_1^{-1}(0^n1^n)=\{(0,\Lambda),(0,0)\}^n\cdot\{(1,\Lambda),(1,1)\}^n$;

$h_1^{-1}(0^n1^n)\cap R=\{(0,\Lambda)^n(1,\Lambda)^n\}\cup$

$\cup\{(0,\Lambda)^n(1,\Lambda)^i(1,1)^j(1,\Lambda)^k\mid i+j+k=n,\ i\geqslant0,\ j\geqslant1,$

$k\geqslant0\}\cup\{(0,\Lambda)^i(0,0)^j(1,1)^k(1,\Lambda)^m\mid i+j=n,\ i\geqslant0,\ j\geqslant1,$

$k+m=n,\ k\geqslant1,\ m\geqslant0\}\cup\{(0,\Lambda)^i(0,0)^j(0,\Lambda)^k(1,\Lambda)^n\mid i+$

$+j+k=n,\ i\geqslant0,\ j\geqslant1,\ k\geqslant0\}$;

$h_2(h_1^{-1}(0^n1^n)\cap R)=\Lambda\cup\{1^j\mid1\leqslant j\leqslant n\}\cup$

$\cup\{0^j1^k\mid1\leqslant j\leqslant n,\ 1\leqslant k\leqslant n\}\cup\{0^j\mid1\leqslant j\leqslant n\}=$

$=\{0^i1^j\mid0\leqslant i,\ j\leqslant n\}$.

Аналогично проверяется и равенство

$h_2'(h_1'^{-1}(0^n1^n)\cap R')=\{0^i1^j\mid0\leqslant i,\ j\leqslant n\}$.

ПРИМЕНЕНИЯ ХАРАКТЕРИЗАЦИОННОЙ ТЕОРЕМЫ

Следствие 8.2.6. Пусть M — а-преобразователь. Тогда:

1. Обратное а-преобразовательное отображение M^{-1} снова является а-преобразовательным отображением, т. е. может быть построен а-преобразователь M' такой, что для любого подмножества L' моноида $F(Y)$ будут справедливы равенства $M'(L')=M^{-1}(L')=\{w\in F(X)\mid M(\{w\})\cap L'=\varnothing\}$.

2. Для любого рационального подмножества L моноида $F(X)$ множество $M(L)$ рационально. По представлению L в виде рационального или различимого множества может быть эффективным образом построено соответствующее представление для множества $M(L)$.

Доказательство. Пусть h_1, h_2 и R построены для M также, как в п.1 теоремы 8.2.4.

1. Очевидно, что для w из $F(X)$ и v из $F(Y)$ следующие три высказывания равносильны:

а) $v \in h_2(h_1^{-1}(w) \cap R)$;

б) в R существует r такое, что $h_1(r)=w$ и $h_2(r)=v$;

в) $w \in h_1(h_2^{-1}(v) \cap R)$.

Если теперь $w \in M^{-1}(L')$, то из п.1 теоремы 8.2.4 и из п.3 замечаний к определению 8.2.2 следует, что в L' существует слово v, удовлетворяющее условию а), так что из условия в) в этом случае вытекает $w \in h_1(h_2^{-1}(L') \cap R)$.

В то же время из последнего включения вытекает существование в L' слова v, удовлетворяющего условию в), а потому и условию а). Отсюда следует, что $M(\{w\}) \cap L' \neq \varnothing$, так что $w \in M^{-1}(L')$.

Поэтому для любого подмножества L' моноида $F(Y)$ выполняется равенство $M^{-1}(L')=h_1(h_2^{-1}(L') \cap R)$. Итак, полагая в п.2 теоремы 8.2.4 $P'=P$, $h_1'=h_2$, $h_2'=h_1$ и $R'=R$, получаем искомый а-преобразователь M'.

2. Если множество L рационально (различимо), то по лемме 5.4.3 и множество $h_1^{-1}(L)$ различимо. По теореме 5.5.7 в этом случае множество $h_1^{-1}(L) \cap R$ рационально, а из следствия 7.2.5 и п.4 замечаний к теореме 8.2.4 следует, что и множество $M(L)$ рационально. Поскольку гомоморфизмы h_1 и h_2 и множество R могут быть заданы эффективным образом, а построения из доказательств теоремы 5.5.7, леммы 5.4.3 и следствия 7.2.5 могут быть проведены эффективно, то представление множества $M(L)$ может быть получено из соответствующего представления множества L эффективным образом. ■

Несмотря на то, что нетрудно привести примеры множеств, отображаемых друг на друга а-преобразователями (см. упражнение 8.5), оказывается, вообще говоря, довольно затруднительно привести обратные примеры. Такой пример содержится в следствии 8.7.2 (в качестве дополнения см. также упражнение 8.6). Доказательство этого следствия, довольно простое само по себе, призвано дать исходное представление о доказательствах подобных утверждений. Кроме того, с помощью данного примера можно найти простое отображение, не являющееся а-преобразовательным, хотя при нем рациональные множества и отображаются на рациональные же.

Следствие 8.2.7 (Берстел). *Не существует* а-преобразователя, переводящего одно из двух множеств $U=\{a^n b^m \mid 0 \leqslant m \leqslant n\}$ и $V=\{a^n b^m \mid 0 \leqslant n \leqslant m\}$ на другое (сюръективно).

Доказательство. а) Вследствие симметрии достаточно показать, что не существует а-преобразователя M такого, что $M(U)=V$. Пусть множество $Y=\{c, d\}$ не пересекается с множеством $X=\{a, b\}$ и $T=\{c^n d^m \mid 0 \leqslant n \leqslant m\}$. Ясно, что любой а-преобразователь M такой, что $M(U)=T$, при замене c на a и d на b превращается в а-преобразователь M' такой, что $M'(U)=V$. Поэтому мы предположим, что существует а-преобразователь M та-

кой, что $M(U)=T$, и докажем, что это предположение приводит к противоречию.

Из п.1 теоремы 8.2.4 и замечаний к ней следует, что при выполнении нашего предположения существуют гомоморфизмы h_1 из $F(X \cup Y)$ в $F(X)$ и h_2 из $F(X \cup Y)$ в $F(Y)$ и рациональное подмножество R моноида $F(X \cup Y)$ такие, что $T=M(U)=h_2(h_1^{-1}(U) \cap R)$.

б) Теперь мы докажем следующее.

Промежуточное утверждение. Для каждого натурального числа i существует натуральное число k, $k \geqslant i$ такое, что для любого слова w из $h_1^{-1}(U) \cap R \cap h_2^{-1}(c^k d^k)$ выполнено равенство $h_1(w)=a^n b^m$, где $i \leqslant m \leqslant n$.

Это означает, что в T существуют «длинные» слова, которые могут быть образами только «длинных» слов из U.

Доказательство. Если бы промежуточное утверждение было ложно, то существовало бы натуральное число i такое, что для любого $k \geqslant i$ в $h_1^{-1}(U) \cap R \cap h_2^{-1}(c^k d^k)$ можно было бы найти слово w, для которого выполнялось бы равенство $h_1(w)=a^j b^l$ при $0 \leqslant l \leqslant i$ и $1 \leqslant j$.

Пусть $L=\{a^j b^l \mid l \leqslant j,\ 0 \leqslant l < i\}$.

Тогда $L \subseteq U$ и $L=a^* \cdot \{a^l b^l \mid 0 \leqslant l < i\}$.

Итак, в этом случае множество L рационально, а потому рационально и множество $M(L)$ п.2 следствия 8.2.6.

Таким образом, при нашем предположении должны были бы выполняться соотношения $\{c^k d^k \mid k \geqslant i\} \subseteq M(L) \subseteq (U)=T$.

По uvw-теореме (см. следствие 5.4.10) в этом случае [$M(L)$ — рационально!] существовало бы $k \geqslant i$ такое, что $c^k d^k = uvu'$ при $v \neq \Lambda$ и $|uv| \leqslant k$, так что выполнялось бы равенство $v=c^p$ при $p \neq 0$, а поэтому слово $c^k c^p d^k$ принадлежало бы $M(L)$ и T, что противоречит определению T. Итак, промежуточное утверждение истинно.

в) Пусть r — число состояний минимального ДРС-автомата, допускающего множество R. Положим в промежуточном утверждении $i=r$ и выберем некоторое постоянное $k \geqslant 1$. Пусть, далее, w — слово минимальной длины из непустого, как следует из равенства $M(U)=T$, множества $h_1^{-1}(U) \cap R \cap h_2^{-1}(c^k d^k)$. Для $h_1(w)=a^j b^l$ из промежуточного утверждения имеем $r \leqslant l \leqslant j$.

Слово w можно разложить на подслова двумя способами:

$$w=w_1 w_2=w_1' w_2', \text{ где } h_1(w_1)=a^j,\ h_1(w_2)=b^l,\ h_2(w_1')=c^k,$$

$$h_2(w_2')=d^k.$$

Пусть v — кратчайшее из слов w_2 и w_2', и v' — слово, определяемое условием $w=v'v$. Тогда $|v| \geqslant r$.

Так как $R \subseteq w$, то v допускается ДРС-автоматом A', получающимся из автомата A заменой начального состояния s состоянием $f^*(s, v')$. Автомат A' также имеет r состояний. По uvw-теоре-

ме в этом случае v может быть разложено следующим образом:

$v=xuy$, $0<|u|\leqslant r$ и $v'xy\in R$.

Из условия выбора слова v следует, что $h_1(v)$, а потому и $h_1(u)$ принадлежат b^*. Поэтому выполняется включение $h_1(v'xy)\in U$. Далее, $h_2(v'xy)=c^kd^{k-q}$ при $q=|h_2(u)|$.

Так как $v'xy\in h_1^{-1}(U)\cap R$, то по теореме 8.2.4 п.1 $h_2(v'xy)$ принадлежит T. Отсюда следует, что $q=0$. Из этого равенства вытекает, что $v'xy\in h_1^{-1}(U)\cap R\cap h_2^{-1}(c^kd^k)$, что вследствие $|v'xy|<|w|$ противоречит минимальности w. Итак, a-преобразователя M не существует. ■

Следствие 8.2.8. Отображение $F(\{a, b\})$ в себя, переводящее каждое слово в зеркальное для него, не является рациональным преобразованием.

Доказательство. Если бы зеркальное отображение s было рациональным преобразованием, то и отображение s′, которое сначала переводит слово в зеркальное для него, а потом меняет a на b и обратно, было бы рациональным преобразованием.

Действительно, a-преобразователь, реализующий s, можно было бы получить из a-преобразователя, реализующего s′, заменив выход a на b и обратно. Для множеств U и V из следствия 8.2.7 в этом случае вытекало бы равенство $s'(U)=V$. Но это противоречит следствию 8.2.7. ■

8.3. НЕРАЗРЕШИМОСТЬ ПРОБЛЕМЫ ЭКВИВАЛЕНТНОСТИ a-ПРЕОБРАЗОВАТЕЛЕЙ

Определение 8.3.1. Два a-преобразователя M и M′ с одинаковыми входными и выходными алфавитами называются *эквивалентными,* если $T_M=T_{M'}$.

Хотя разрешимость проблемы эквивалентности для конечных преобразователей может быть показана так же просто, как в случае автоматов Мили (см. упражнение 8.3), проблема эквивалентности для Λ-свободных недетерминированных конечных преобразователей оказывается неразрешимой — уточнение этого высказывания содержится в упражнении 8.7.

Теорема 8.3.2. 1. Проблема эквивалентности конечных преобразователей разрешима.

2. (Гриффитс.) Не существует алгоритма, позволяющего решить, являются ли два данных Λ-свободных недетерминированных конечных преобразователя эквивалентными.

Доказательство. 1. Пусть $M=(Z, X, Y, f, g, s)$ и $M'=(Z', X', Y', f', g', s')$ — два конечных преобразователя (как обычно, считается, что Y и Y′ не содержат «лишних» элементов). Они могут быть эквивалентны только в том случае, когда $X=X'$ и $Y=Y'$, так что будем считать, что эти равенства выполнены. Мы будем предполагать далее, что каждое состояние преобразователя M(M′) достижимо из начального состояния s (из

s′), поскольку для любого состояния конечного преобразователя вопрос о том, достижимо ли оно из начального состояния, разрешим (как и в случае РС-автоматов).

Чтобы M и M′ были эквивалентны, должно, в частности, при любом слове w из F(X) и любом входе x из X выполняться равенство

$$g^*(s, w)\,g(f^*(s, w), x) = g'^*(s', w)\,g'(f'^*(s', w), x).$$

(Здесь f^* и g^* понимаются как в определении 2.3.1.)

Отсюда следует, что $g(f^*(s, w), x) = g'(f'^*(s', w), x)$, т. е. для каждого z из Z в Z′ существует z′ такое, что $g(z, x) = g'(z', x)$, и наоборот, так что множества W и W′ «элементарных» выходных слов преобразователей M и M′ должны совпадать:

$$W = \{g(z, x) \mid z \in Z, x \in X\} = W' = \{g'(z', x) \mid z' \in$$

$$\in Z', x \in X\}.$$

Поскольку вопрос о равенстве множеств W и W′ разрешим, мы будем в дальнейшем предполагать, что W = W′.

Преобразователи M и M′ можно теперь рассматривать как автоматы Мили $\bar{M}$ и $\bar{M}'$ соответственно с общим входным алфавитом W, считая элементы множества W «буквами». Очевидно, что M и M′ эквивалентны тогда и только тогда, когда состояния s и s′ автоматов $\bar{M}$ и $\bar{M}'$ соответственно имеют равные реакции. Но этот вопрос по следствию 2.3.4 разрешим.

2. Любой Λ-свободный недетерминированный конечный преобразователь M является a-преобразователем $M = (Z, X, Y, t, s, Z)$, где $\tau \subseteq Z \times X \times F^+(Y) \times Z$. В случае недетерминированных конечных преобразователей мы опускаем описание множества финальных (допускающих) состояний.

Для доказательства мы используем следующую теорему о неразрешимости (см. лемму 8.3.5): «Не существует алгоритма, позволяющего решить вопрос, существует ли для данных двух гомоморфизмов g и h из F(X) в F(Y) таких, что $h(X) \cup g(X) \subseteq Y^2Y^*$, слово w в $F^+(X)$ такое, что $g(w) = h(w)$».

Пусть теперь заданы два указанных гомоморфизма g и h. Положим $m = \max\{|g(x)|, |h(x)| \mid x \in X\}$.

Пусть, далее, M — следующий Λ-свободный недетерминированный конечный преобразователь

$$M = (\{s_m\}, X, Y, t_m, s_m),$$

где $t_m(s_m, x) = \{(u, s_m) \mid u \in F^+(Y), |u| \leqslant m\}$ —

для всех x из X.

Тогда для всех w из $F^+(X)$ выполнено равенство

$$T_M(w) = \{v \in F^+(Y) \mid |w| \leqslant |v| \leqslant m|w|\}.$$

Построим, наконец (в лемме 8.3.3), два Λ-свободных недетерминированных конечных преобразователя

$$G = (Z_g, X, Y, t_g, s_g) \text{ и } H = (Z_h, X, Y, t_h, s_h)$$

так, что для каждого w из $F^+(X)$ будут верны равенства

$$T_G(w)=T_M(w)-g(w) \text{ и } T_H(w)=T_M(w)-h(w).$$

Мы можем предполагать, что Z_g и Z_h дизъюнктны. Построим тогда следующий Λ-свободный недетерминированный конечный преобразователь:

$N=(Z_g \cup Z_h \cup S, X, Y, t, s)$, где $s \notin Z_g \cup Z_h$ и

$$t(z, x)=\begin{cases} t_g(s_g, x) \cup t_h(s_h, x), & \text{если } z=s, \\ t_g(z, x), & \text{если } z \in Z_g, \\ t_h(z, x), & \text{если } z \in Z_h, \end{cases}$$

для всех z из $Z_g \cup Z_h \cup s$ и всех x из X.

Очевидно, что для всякого w из $F^+(X)$

$$T_N(w)=T_G(w) \cup T_H(w)=(T_M(w)-g(w)) \cup (T_M(w)-h(w)).$$

Отсюда следует, что для любого w из $F^+(X)$ соотношение $T_N(w) \neq T_M(w)$ выполняется тогда и только тогда, когда $g(w)=h(w)$.

Итак, вопрос об эквивалентности Λ-свободных недетерминированных конечных преобразователей M и N разрешим в том и только в том случае, если разрешим вопрос о существовании слова $w \neq \Lambda$ такого, что $g(w)=h(w)$, а это, как следует из приведенной выше теоремы о неразрешимости, неверно.

Для доказательства утверждения 2 нам осталось только доказать леммы 8.3.3 и 8.3.5. ■

Лемма 8.3.3. Использованные в доказательстве п.2. теоремы 8.3.2 Λ-свободные недетерминированные конечные преобразователи G и H могут быть заданы эффективным образом.

Доказательство. Мы построим только G, поскольку H задается аналогично.

Будем считать, что множество $\{s_g, -, 0, +\}$ не пересекается с Y. Положим тогда $Z_g=Y \cup \{s_g, -, 0, +\}$.

Пусть x — произвольный элемент множества X и $g(x)=y_1y_2 \ldots y_n$, где $y_i \in Y$. Так как $g(x) \in Y^2Y^*$, то $n \geqslant 2$. Пусть, далее, z — произвольный элемент из Y.

Положим

$$t_g(s_g, x)=\{(y_1y_2 \ldots y_{n-1}, y_n)\} \cup \{(u, -) \mid u \in F^+(Y),$$
$$|u|<n\} \cup \{(v, 0) \mid v \in F^+(Y),\ v \neq g(x),\ |v|=n\} \cup$$
$$\cup \{(w, +) \mid w \in F^+(Y),\ n<|w| \leqslant m\};$$
$$t_g(y, x)=\{yv, z') \mid (v, z') \in t_g(s_g, x)\} \text{ — для каждого y из Y;}$$
$$t_g(-, x)=\{(y, -) \mid y \in Y\};$$
$$t_g(0, x)=\{(u, -) \mid u \in F^*(Y),\ |u|<n\} \cup \{(v, 0) \mid v \in F^+(Y),$$
$$|v|=n\} \cup \{(w, +) \mid w \in F^+(Y),\ n<|w| \leqslant m\};$$
$$t_g(+, x)=\{(v, +) \mid F^+(Y),\ |v|=m\}.$$

G является в этом случае Λ-свободным недетерминированным конечным преобразователем, и нам остается только доказать следующее промежуточное утверждение.

Промежуточное утверждение. Пусть w — произвольное слово из $F^+(X)$ и $g(w)=y_1'y_2'\dots y_k'$ при $y_1'\in Y$.
(Так как $g(X)\subseteq Y^2Y^*$, то $k\geqslant 2|w|$.) Тогда

$$t_g^*(s_g, w)=\{(y_1'y_2'\dots y_{k-1}', y_k')\}\cup\{(u, -)\,|\,u\in F^+(Y),\ |w|\leqslant$$
$$\leqslant|u|<k\}\cup\{(u, 0)\,|\,u\in F^+(Y),\ u\neq g(w),\ |u|=k\}\cup\{(u, +)\,|\,u\in$$
$$\in F^+(Y),\ k<|u|\leqslant m|w|\}.$$

Действительно, из промежуточного утверждения следует, что каждое слово v из $F^+(Y)$ при $|w|\leqslant|v|\leqslant m|w|$ и $v\neq g(w)$ принадлежит $T_G(w)$, т. е. $T_M(w)-g(w)\subseteq T_G(w)$;

$T_G(w)$ не содержит иных элементов, так как $|w|\leqslant 2|w|-1\leqslant$ $\leqslant|y_1'y_2'\dots y_{k-1}'|<m|w|$ и $y_1'y_2'\dots y_{k-1}'\neq g(w)$.

Доказательство промежуточного утверждения. Промежуточное утверждение мы докажем полной индукцией по длине слова w.

При $|w|=1$ утверждение вытекает из определения t_g.

Предположим теперь, что утверждение выполнено для всех слов w таких, что $|w|=r>1$.

Пусть, далее, x — произвольный вход из X и $g(x)=y_1y_2\dots y_n$ с $y_1\in Y$. Тогда по предположению о g имеем $n\geqslant 2$ и $g(wx)=$ $=y_1'y_2'\dots y_k'y_1y_2\dots y_n$.

Из определений t_g и t_g^* получаем

$t_g^*(s_g, wx)=\{(uv, z')\,|$ существует $z\in Z_g$ такое, что $(u, z)\in$ $\in t_g^*(s_g, w)$ и $(v, z')\in t_g(z, x)\}$.

В зависимости от того, каким именно элементом множества Z_g оказывается «промежуточное» состояние z, приходится использовать один из четырех случаев определения t_g (так как $w\neq\Lambda$, выполнено неравенство $z\neq s_g$).

1) $z=-$. Пусть тогда

$$K_-=\{(uv, z')\,|\,(u, -)\in t_g^*(s_g, w),\ (v, z')\in t_g(-, x)\}=$$
$$=\{(u, v, z')\,||w|\leqslant|u|<k,\ v\in Y,\ z'=-\}=$$
$$=\{(w', -)\,|\,w'\in F^+(Y),\ |wx|\leqslant|w'|<k+1\}.$$

2) $z=0$. Пусть тогда

$$K_0=\{(uv, z')\,|\,(u, 0)\in t_g^*(s_g, w),\ (v, z')\in t_g(0, x)\}=$$
$$=\{(uv, z')\,|\,u\neq g(w),\ |u|=k,\ 1\leqslant|v|<n,\ z'=-\}\cup$$
$$\cup\{(uv, z')\,|\,u\neq g(w),\ |u|=k,\ |v|=n,\ z'=0\}\cup$$
$$\cup\{(uv, z')\,|\neq g(w),\ |u|=k,\ n<|v|\leqslant m,\ z'=+\};$$
$$K_0'=\{(w', -)\,|\,w'\in F^+(Y),\ k+1\leqslant|w'|<k+n\}\cup$$
$$\cup\{(w', 0)\,|\,w'\in F^+(Y),\ w'\neq g(wx),\ |w'|=k+n\}\cup$$
$$\cup\{(w', +)\,|\,w'\in F^+(Y),\ k+n<|w'|\leqslant k+m\}.$$

3) $z=+$. Пусть тогда

$K_+=\{(uv, z')\,|\,k<|u|\leqslant m|w|,\ |v|=m,\ z'=+\}=$
$=\{(w', +)\,|\,w'\in F^+(Y),\ k+m<|w'|\leqslant m|wx|\}.$

4) $z\in Y$. Пусть тогда

$K_Y=\{(uv, z')\,|\,(u, y)\in t^*(s_g, w),\ y\in Y,\ (v, z')\in$
$\in t_g(y, x)\}=\{(uv, z')\,|\,(y_1'\ldots y_{k-1}', y_k')\in$
$\in t^*(s_g, w),\ v=y_k'v',\ (v', z')\in t_g(s_g, x)\}=$
$=\{(y_1'\ldots y_k'y_1\ldots y_{n-1}, y_n)\}\cup\{(y_1'\ldots y_k'v', -)\,|\,v'\in F^+(X),$
$|v'|<n\}\cup\{(y_1'\ldots y_k'v', 0)\,|\,v'\in F^+(X),\ v'\neq g(x),$
$|v'|=n\}\cup\{(y_1'\ldots y_k'v', +)\,|\,v'\in F^+(X),\ n<|v'|\leqslant m\}.$

При $K_Y'=\{(y_1'\ldots y_k'y_1\ldots y_{n-1}, y_n)\}$ имеем $K_Y=K_Y'\cup(K_0'-K_0)$. Отсюда сразу видно, что $t_g^*(s_g, wx)=K_Y'\cup K_-\cup K_0'\cup K_+$ и что утверждение остается верным при замене w на wx (и соответственно k на k+n). ■

ПРОБЛЕМА СООТВЕТСТВИЙ ПОСТА

Использованная в доказательстве п.2 теоремы 8.3.2 теорема о неразрешимости является модификацией часто используемой теоремы о неразрешимости так называемой проблемы соответствий Поста.

Определение 8.3.4. Пусть n — натуральное число, а $u=(u_1, u_2, \ldots, u_n)$ и $v=(v_1, v_2, \ldots, v_n)$ — n-ки слов u_1, v_1 из $F^+(X)$. Четверка $Q=(X, n, u, v)$ называется тогда *случаем проблемы соответствий Поста над X. Решением* Q называется конечная непустая последовательность $i_1, i_2, \ldots, i_k$ натуральных чисел i_j $(1\leqslant i_j\leqslant n)$ такая, что $u_{i_1}u_{i_2}\ldots u_{i_k}=v_{i_1}v_{i_2}\ldots v_{i_k}$.

Общей проблемой соответствий Поста над X называется задача построения алгоритма, определяющего для каждого случая проблемы соответствий Поста над X, имеет ли он решение или нет.

Частной проблемой соответствий Поста над X ранга r (при r из **N**) называется задача построения алгоритма, определяющего для каждого случая $Q=(X, r, u, v)$ проблемы соответствий Поста над X, имеет ли Q решение или нет.

Лемма 8.3.5. (Пост). 1. Общая проблема соответствий Поста над любым по меньшей мере двухэлементным множеством X неразрешима, т. е. не существует алгоритма, который для любого случая проблемы соответствий Поста над X определяет, имеет ли он решение или нет.

2. Для любого $r\geqslant 9$ и любого X с по меньшей мере двумя элементами частная проблема соответствий Поста ранга r над X неразрешима.

3. Общая проблема соответствий Поста над одноэлементным множеством X разрешима.

4. Общая проблема соответствий Поста над X разрешима если и только если существует алгоритм, который для каждого конеч-

ного множества Y и любых двух гомоморфизмов g и h из $F^+(Y)$ в $F^+(X)$ таких, что $h(Y) \cup g(Y) \subseteq X^2X^*$, может решить, существует ли в $F^+(Y)$ слово w такое, что $g(w)=h(w)$.

Доказательство. 1. Неразрешимость общей проблемы соответствий Поста над X выводится, среди прочего, из неразрешимости проблемы остановки для машин Тьюринга. Поэтому мы ограничимся ссылкой на учебники по теории машин Тьюринга, теории вычислимости, теории алгоритмов или теории формальных языков (на последние — в первую очередь).

2. Данное утверждение вытекает из стандартного доказательства п.1 с учетом того факта, что существуют универсальные машины Тьюринга.

3. Пусть $Q=(\{x\}, n, u, v)$ — случай проблемы соответствий Поста над $\{x\}$, где $p_i=|u_i|$, $q_i=|v_i|$ и $p_i \neq q_i$ (иначе всегда существует решение i) при $i=1, \ldots, n$. Q имеет решение тогда и только тогда, когда существуют k_i в $\mathbf{N}_0$ [1] такие, что $k_1(p_1-q_1)+k_2(p_2-q_2)+\ldots+k_n(p_n-q_n)=0$.

Если все разности p_i-q_i имеют один знак, то решения не существует. В противном случае имеется решение

$$k_{r_1}=\ldots=k_{r_a}=(q_{s_1}-p_{s_1})+\ldots+(q_{s_c}-p_{s_c}) \text{ и}$$

$$k_{s_1}=\ldots=k_{s_c}=(p_{r_1}-q_{r_1})+\ldots+(p_{r_a}-q_{r_a}),$$

где $r_1, \ldots, r_a$ (соответственно $s_1, \ldots, s_c$) — все индексы r (s) из $\{1, \ldots, n\}$ такие, что $p_r-q_r>0$ (соответственно $p_s-q_s<0$).

4. Прежде всего мы определим для каждого случая Q проблемы соответствий Поста над X конечное множество Y и гомоморфизмы g и h из $F^+(Y)$ в $F^+(X)$ так, что Q будет иметь решение в том и только в том случае, когда $F^+(Y)$ будет содержать слово w такое, что $g(w)=h(w)$.

Пусть $Q=(X, n, u, v)$. Пусть тогда $Y=\{y_1, y_2, \ldots, y_n\}$, $g(y_i)=u_i$ и $h(y_i)=v_i$ при $i=1, \ldots, n$.

Если, наоборот, заданы конечное множество $Y=\{y_1, \ldots, y_n\}$ и два гомоморфизма g и h из $F^+(Y)$ в $F^+(X)$, то $Q=(X, n, u, v)$, где $u_i=g(y_i)$ и $v_i=h(y_i)$ при $i=1, \ldots, n$ — случай проблемы соответствий Поста над X, имеющий решение в точности тогда, когда в $F^+(Y)$ существует слово w такое, что $g(w)=h(w)$.

Зададим, наконец, для каждого множества Y и для любых двух гомоморфизмов g и h из $F^+(Y)$ в $F^+(X)$ два гомоморфизма g' и h' из $F^+(Y)$ в $F^+(X)$ со свойством $h'(Y) \cup g'(Y) \subseteq X^2X^*$ так, что при каждом слове w из $F^+(Y)$ равенство $g(w)=h(w)$ будет выполняться тогда и только тогда, когда $g'(w)=h'(w)$.

Пусть при этом d — гомоморфизм из $F^+(X)$ в себя, определенный условием: $d(x)=xx$ при любом x из X.

Очевидно, что равенство $d(u)=d(v)$ при u и v из $F^+(X)$ выполняется тогда и только тогда, когда $u=v$.

---

[1] Не все равные нулю. — *Прим. перев.*

Поэтому $g'=dg$ и $h'=dh$ обладают требуемыми свойствами, и утверждение 4 доказано. ■

Дальнейшие сведения о проблеме соответствий Поста можно найти в упражнении 8.8.

8.4. ДВУЛЕНТОЧНЫЕ АВТОМАТЫ ЭЛГО—МЕЗЕЯ

Не изменяя формального описания а-преобразователя, мы можем (аналогично тому, как было сделано в доказательстве теоремы Нивата) при содержательной интерпретации рассматривать обе ленты преобразователя как входные. При этом мы получаем автомат, синхронно считывающий символы с двух лент и допускающий пары слов [элементы произведения $F(X)\times F(Y)$]. Реакцией такого автомата оказывается, таким образом, не соответствие, а подмножество декартова произведения двух конечно-порожденных моноидов. Такой автомат функционирует вполне аналогично НРС-автомату: если в него введена некоторая пара слов, то он ищет какую-либо последовательность шагов, которые состоят в считывании или в изменении состояния, приводящую при обработке рассматриваемых слов к переходу из начального в какое-либо финальное состояние. Если такая последовательность существует, то пара слов допускается, в противном случае — нет. В данном случае по аналогии с НРС-автоматами мы будем допускать, что рассматриваемый автомат имеет более одного начального состояния.

Определение 8.4.1. (*Недетерминированным*) *двуленточным автоматом Элго — Мезея над (X, Y)* (сокращенно: 2-ЭМ-автоматом) называется шестерка $A=(Z, X, Y, t, S, F)$, где Z — *множество состояний,* X и Y — *входные алфавиты,* $S\subseteq Z$ (соответственно $F\subseteq Z$) — множество *начальный* (*финальных*) состояний автомата A и $t=(Z\times F(X)\times F(Y), Z, \tau)$ — конечное соответствие (*соответствие переходов* автомата A).

Соответствие t может быть продолжено до последовательностного соответствия $t^*=(Z\times F(X)\times F(Y), Z, \tau^*)$ автомата A, где τ^* понимается так же, как в определении 8.2.2.

Реакцией автомата A (или *допускаемым* автоматом A *множеством*) называется множество

$$L(A)=\{(w, v)\in F(X)\times F(Y) \mid t^*(S, (w, v))\cap F\neq\varnothing\}.$$

Два 2-ЭМ-автомата называются *эквивалентными,* если они имеют одинаковые реакции.

Замечания. 1. 2-ЭМ-автомат может быть представлен, как и НРС-автомат, взвешенным ориентированным графом, только в случае 2-ЭМ-автомата метками на ребрах будут пары слов.

2. Пусть A — 2-ЭМ-автомат. Каждая пара слов (w, v) из $pr_{2,3}\tau$ порождает, как и в случае НРС-автоматов, соответствие $t_{w,v}=(Z, Z, pr_{1,4}(\tau\cap Z\times\{w, v\})\times Z))$ из Z в себя. График этого соответствия отвечает множеству всех ребер (и принадлежащих им вершин) с меткой (w, v) в графе автомата A.

3. Пусть A — 2-ЭМ-автомат. Пара слов (w, v) допускается автоматом A, т. е. $t^*(S, (w, v)) \cap F \neq \varnothing$ тогда и только тогда, когда существуют последовательность $z_0, z_1, \ldots, z_n$ состояний автомата A и последовательность $(u_1, u_1'), (u_2, u_2'), \ldots, (u_n, u_n')$ элементов произведения $F(X) \times F(Y)$ такие, что $z_0 \in S$, $z_n \in F$ и $(z_{i-1}, u_i, u_i', z_i) \in \tau$ при $i=1, \ldots, n$, а $w=u_1u_2 \ldots u_n$ и $v=u_1'u_2' \ldots u_n'$. Пара (Λ, Λ) допускается, если $S \cap F \neq \varnothing$.

4. В дальнейшем мы везде вместо $t^*(z, (w, v))$ будем, избегая употребления лишних скобок, писать $t^*(z, w, v)$.

Пример 8.4.2. Граф, изображенный на рис. 8.2.3, можно рассматривать как граф некоторого 2-ЭМ-автомата A_1 — достаточно везде заменить метки w/v на (w, v). Реакцию автомата A_1 получаем из приведенного в примере 8.2.5 множества R, производя покомпонентное перемножение.

Пусть $X=\{0, 1\}$. Тогда

$L(A_1)=\{(w, v) \in F(X) \times F(X) \mid$ существуют u, u′, $v \in F(X)$ такие, что $w=uvu'\}$.

РАВНОСИЛЬНОСТЬ 2-ЭМ-АВТОМАТОВ И а-ПРЕОБРАЗОВАТЕЛЕЙ

Очевидно, что график каждого преобразования, порождаемого некоторым а-преобразователем, допускается этим а-преобразователем, рассматриваемым как 2-ЭМ-автомат. Верно даже и обратное, т. е. 2-ЭМ-автоматы и а-преобразователи в определенном смысле равносильны.

Теоремы 8.4.3. Для любого подмножества L произведения $F(X) \times F(Y)$ следующие высказывания эквивалентны:

1) L является реакцией некоторого 2-ЭМ-автомата над (X, Y);

2) L является графиком рационального преобразования из F(X) в F(Y).

Доказательство. Нам нужно только показать, что из утверждения 1) следует 2). Поскольку каждый 2-ЭМ-автомат A с единственным начальным состоянием может рассматриваться как а-преобразователь, у которого отвечающее ему преобразование имеет график, в точности совпадающий с реакцией автомата A, то теорема будет доказана, если нам удастся показать, что для любого 2-ЭМ-автомата A может быть построен 2-ЭМ-автомат A′ с единственным начальным состоянием и такой же реакцией. Но это сделать просто: пусть A — 2-ЭМ-автомат. Присоединим к множеству состояний автомата A новое состояние s, соединенное спонтанными переходами [вход (Λ, Λ)] со всеми начальными состояниями автомата A, и сделаем s единственным начальным состоянием автомата A′:

$A'=(Z \cup s, X, Y, t', s, F)$, где $s \notin Z$ и $\tau'=\tau \cup \{(s, \Lambda, \Lambda, z) \mid z \in S\}$,

$t'=((Z \cup s) \times F(X) \times F(Y), Z \cup s, \tau')$.

Очевидно, что в этом случае $L(A')=L(A)$. ■

Теперь мы можем все полученные для а-преобразователей

результаты перенести непосредственно на 2-ЭМ-автоматы (см. также упражнения 8.1—8.6). Таким образом мы получаем, в частности, характеризационную теорему для реакций 2-ЭМ-автоматов, два в сравнении с теоремой 5.5.9 удивительных (надо надеяться) результата о неразрешимости и необходимый критерий допустимости множества 2-ЭМ-автоматом.

Следствие 8.4.4. 1. Подмножество L произведения $F(X)\times F(Y)$ является реакцией некоторого 2-ЭМ-автомата над (X, Y) тогда и только тогда, когда существуют конечное множество P, рациональное подмножество R моноида F(P) и гомоморфизмы h_1 и h_2 из F(P) соответственно в F(X) и в F(Y), такие, что

$$L=\{(h_1(w), h_2(w)) \mid w\in R\}.$$

В качестве P может быть выбрано подмножество произведения $F(X)\times F(Y)$, а в качестве h_1 и h_2 — определяемые ниже гомоморфизмы π_X из F(P) в F(X) и π_Y из F(P) в F(Y) (они называются проектированиями): $\pi_X(u, v)=u$ и $\pi_Y(u, v)=v$ для всех (u, v) из P.

2. Для 2-ЭМ-автоматов A и A′ неразрешимы следующие проблемы:

Являются ли A и A′ эквивалентными?

Являются ли множества L(A) и L(A′) дизъюнктными?

Является ли пересечение $L(A) \cap L(A')$ бесконечным множеством?

3. Пусть $L\subseteq F(X)\times F(Y)$. Если L — реакция некоторого 2-ЭМ-автомата A [т. е. L=L(A)], то множества $pr_1(L)$ и $pr_2(L)$ рациональны. Из рациональности множеств $pr_i(L)$, где i=1, 2, не следует, однако, с необходимостью, что L является реакцией некоторого 2-ЭМ-автомата.

Доказательство. 1. Утверждение вытекает из теоремы Нивата и ее доказательства.

2. Неразрешимость проблемы эквивалентности вытекает из теоремы Гриффитса.

Пусть $|X|\geqslant 2$ и Q=(X, n, u, v) — случай проблемы соответствий Поста над X (см. определение 8.3.4). Пусть, далее, A — 2-ЭМ-автомат, допускающий множество $\{(w, w) \mid w\in F^+(X)\}$:

$A=(\{z_1, z_2\}, X, X, t, z_1, z_2)$, где

$$\tau=\{(z_1, x, x, z_2) \mid x\in X\}\cup\{(z_2, x, x, z_2) \mid x\in X\}.$$

Пусть, наконец, A′ — 2-ЭМ-автомат, допускающий множество всех пар слов $(u_{i_1}u_{i_2}\ldots u_{i_n},\ v_{i_1}v_{i_2}\ldots v_{i_n})$:

$$A'=(z', X, X, t', z', z'), \text{ где } \tau'=\{(z', u_i, v_i, z') \mid i=1, \ldots, n\}.$$

Очевидно, что при этом пересечение $L(A)\cap L(A')$ пусто в том и только в том случае, когда Q не имеет решения, а $L(A)\cap L(A')$ бесконечно тогда и только тогда, когда оно не пусто (см. п.1 упражнения 8.8), поскольку вместе с парой (w, w) данному пересечению принадлежат и все пары вида (w^k, w^k). Остальные высказывания п.2 следствия вытекают теперь из п.1 леммы 8.3.5.

3. Пусть $L=L(A)$, $i=1$ или $i=2$. Изменим граф автомата A, оставив в качестве меток на ребрах только i-е компоненты исходных пар. Таким образом, будет получен граф НРС-автомата с реакцией $pr_i(L(A))$.

Контрпримером, необходимым для доказательства последнего утверждения п.3 теоремы, является множеством $M=\{(w, \tilde{w}) \mid w\in \in F(X)\}$, обе проекции которого равны $F(X)$ и потому рациональны. Действительно, если бы это множество было реакцией некоторого 2-ЭМ-автомата, то по теореме 8.4.3 отображение, переводящее каждое слово в зеркальное для него, было бы рациональным преобразованием, чего не может быть по следствию 8.2.8.

Иной контрпример дается в п.1 упражнения 8.9. Другие доказательства того, что множество M не является реакцией никакого 2-ЭМ-автомата, получаются с помощью упражнения 8.9, пп. 3 и 4. ■

Замечание. Из п.1 следствия 8.4.4 вытекает, однако, что вопрос о пустоте реакции $L(A)$ или о бесконечности этого множества разрешим — см. упражнение 8.9, п.4.

2-ЭМ-АВТОМАТЫ И НРС-АВТОМАТЫ, ПРЕДСТАВЛЕНИЕ РЕАКЦИИ 2-ЭМ-АВТОМАТОВ

Если P — множество встречающихся в переходах некоторого 2-ЭМ-автомата A пар слов, то A можно рассматривать как НРС-автомат с входным алфавитом P, допускающий некоторое подмножество моноида $F(P)$. В то же время любой НРС-автомат с конечным подмножеством P произведения $F(X)\times F(Y)$ в качестве входного алфавита можно рассматривать как 2-ЭМ-автомат над (X, Y). Допускаемые НРС-автоматами множества удобно описывать рациональными выражениями. Это обстоятельство порождает вопрос: можно ли допускаемые 2-ЭМ-автоматами множества представлять с помощью множеств, допускаемых соответствующими НРС-автоматами? Для получения ответа мы должны исследовать связи между $F(P)$ и $F(X)\times F(Y)$ в случае, когда P является конечным подмножеством произведения $F(X)\times F(Y)$.

Над множеством $F(X)\times F(Y)$ можно очень простым образом определить операцию (умножение), превращающую это множество в моноид: умножение производим покомпонентно, т. е. полагаем $(u, v)\cdot(u', v)=(uu', vv')$. При этом пара (Λ, Λ) оказывается единичным элементом.

Полученный указанным способом моноид называется *прямым произведением* моноидов $F(X)$ и $F(Y)$. Этот моноид обозначают просто $F(X)\times F(Y)$ и часто опускают полное указание операции произведения. Мы, однако, так делать не будем, чтобы не смешивать эту операцию с операцией в $F(P)$, состоящей в непосредственном приписывании слов друг к другу. Мы зафиксируем эту конструкцию в несколько обобщенном виде в форме леммы.

Лемма 8.4.5. Пусть $(M_i, \circ_i)$, $i=1, \ldots, n$, — моноиды, e_i — единичный элемент моноида M_i. Пусть, далее, $M=M_1\times M_2\times \ldots \times M_n$ — декартово произведение множеств M_i. Пусть на множестве M оп-

ределена следующая операция $\circ$:

$(u_1, u_2, \ldots, u_n) \circ (v_1, v_2 \ldots, v_n) = (u_1 \circ_1 v_1, u_2 \circ_2 v_2, \ldots, u_n \circ_n v_n)$.

Тогда $(M, \circ)$ оказывается моноидом с единичным элементом $(e_1, e_2, \ldots, e_n)$. Он называется *прямым произведением* моноидов M_i и обозначается $M_1 \times \ldots \times M_n$.

Доказательство тривиально, так как нужно только проверить, что «$\circ$» является отображением из $M \times M$ в M, удовлетворяющим закону ассоциативности. То, что $(e_1, \ldots, e_n)$ — единичный элемент, очевидно. ■

Теперь легко установить искомую связь (и даже в общем случае из леммы) между $F(P)$ и $(F(X) \times F(Y), \cdot)$.

Следствие 8.4.6. Пусть $(M_i, \circ_i)$ при $i=1, \ldots, n$ — моноиды и P — конечное подмножество произведения $M = M_1 \times \ldots \times M_n$. Тогда существует однозначно определенный гомоморфизм ν_P из $F(P)$ в M (так называемый *естественный гомоморфизм*), который совпадает на P с тождественным отображением, т. е. такой, что $\nu_P(p) = p$ при всех $p \in P$.

Доказательство. Любой гомоморфизм из $F(P)$ в любой моноид однозначно определяется образами порождающих элементов моноида $F(P)$, т. е. образами элементов множества P. ■

Замечание. Образ при ν_P произведения двух элементов из P получаем, производя покомпонентное перемножение:

$\nu_P((u_1, \ldots, u_n)(v_1, \ldots, v_n)) = (u_1 \circ_1 v_1, \ldots, u_n \circ_n v_n)$.

Из сказанного выше получаем теорему о представлении реакции 2-ЭМ-автоматов, в основном эквивалентную теореме Нивата.

Теорема 8.4.7. Множество L в точности тогда является реакцией некоторого 2-ЭМ-автомата над (X, Y), когда существуют конечное подмножество P произведения $F(X) \times F(Y)$ и рациональное подмножество R моноида $F(P)$ такие, что для естественного гомоморфизма ν_P выполнено равенство $L = \nu_P(R)$.

Доказательство. 1. Пусть A — 2-ЭМ-автомат и, как в доказательстве п.1 теоремы 8.2.4, $P = pr_{2,3}\tau$. Тогда $A' = (Z, P, t', S, F)$, где $t' = (Z \times P, Z, \tau')$ и $\tau' = \tau$ — НРС-автомат, выполняется равенство $L(A) = \nu_P(L(A'))$ и $L(A')$ — рациональное подмножество моноида $F(P)$.

2. Если P — конечное подмножество произведения $F(X) \times F(Y)$ и R — рациональное подмножество моноида $F(P)$, то по теореме Клини существует РС-автомат $A' = (Z, P, t', s, F)$, где $L(A') = R$. Тогда $A = (Z, X, Y, t, s, F)$, где $t = (Z \times F(X) \times F(Y), Z, \tau)$ и $\tau = \tau'$ — 2-ЭМ-автомат и $L(A) = \nu_P(L(A'))$. ■

Замечание. НРС-автомат A', построенный в п. 1 доказательства для данного 2-ЭМ-автомата, мы будем называть *фундаментальным* для A НРС-автоматом.

Пример 8.4.8. Мы рассмотрим конечный преобразователь с допускающими состояниями M_0 из примера 8.2.1 как 2-ЭМ-автомат и с помощью теоремы 8.4.7, п.1 получим для допускаемого этим автоматом множества представление через рациональное множество.

С этой целью введем новое представление для элементов прямого произведения $(F(X)\times F(Y), \cdot)$ *в виде столбцов*: элемент (u, v) будем записывать как $\begin{pmatrix} u \\ v \end{pmatrix}$.

Элементы, представленные в виде столбцов, перемножаются путем их «построчного» приписывания друг к другу.

Пусть теперь $A' = (\{s, z\}, P, t, s, s)$,

где $P = \left\{\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ \Lambda \end{pmatrix}, \begin{pmatrix} 1 \\ \Lambda \end{pmatrix}\right\}$ и $\tau = \left\{\left(s, \begin{pmatrix} 0 \\ 0 \end{pmatrix}, s\right), \left(s, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, z\right), \left(z, \begin{pmatrix} 0 \\ \Lambda \end{pmatrix}, z\right), \left(z, \begin{pmatrix} 1 \\ \Lambda \end{pmatrix} s\right)\right\}$ — НРС-автомат, возникающий при рассмотрении представленного на рис. 8.2.2 конечного преобразователя с допускающими состояниями M_0 как НРС-автомата.

Допускаемое автоматом A' подмножество моноида $F(P)$ имеет вид

$$L(A') = \begin{pmatrix} 0 \\ 0 \end{pmatrix}^* \left[\begin{pmatrix} 1 \\ 1 \end{pmatrix}\begin{pmatrix} 0 \\ \Lambda \end{pmatrix}^*\begin{pmatrix} 1 \\ \Lambda \end{pmatrix}\begin{pmatrix} 0 \\ 0 \end{pmatrix}^*\right]^*.$$

Если рассмотреть M_0 или A' как 2-ЭМ-автомат, то получим $L(A) = \nu_P(L(A'))$. Итак, получены все элементы из $L(A)$, причем в каждом элементе из $L(A')$ произведено покомпонентное перемножение:

$$L(A) = \left\{\begin{pmatrix} 0^a u_1 u_2 \dots u_k \\ 0^a v_1 v_2 \dots v_k \end{pmatrix} \middle| \begin{array}{l} a,\ k \in \mathbf{N}_0,\ u_i = 10^{b_i}10^{c_i}, \\ v_i = 10^{c_i},\ b_i,\ c_i \in \mathbf{N}_0, \\ i = 1, \dots, k. \end{array} \right\}.$$

РАЦИОНАЛЬНЫЕ ПОДМНОЖЕСТВА ПРОИЗВЕДЕНИЯ F(X)×F(Y)

Теорема 8.4.7 приводит к мысли о том, что можно перенести понятие рационального подмножества конечно-порожденного свободного моноида на прямые произведения таких моноидов и соответственно обобщить теорему Клини (теорему 5.3.7).

Определение 8.4.9. Множество $\mathrm{Rat}(X, Y)$ *рациональных подмножеств* произведения $F(X)\times F(Y)$ есть наименьшее подмножество $\mathscr{R}$ булеана $\mathscr{R}(F(X)\times F(Y))$, обладающее следующими свойствами:

1) $\varnothing \in \mathscr{R}$, $\{(x, \Lambda)\} \in \mathscr{R}$ и $\{(\Lambda, y)\} \in \mathscr{R}$ для всех $x \in X$ и $y \in Y$;

2) Если U и V — множества из $\mathscr{R}$, то множества $U \cup V$ и $U \cdot V = \{u \cdot v \mid u \in U,\ v \in V\}$ (произведение) также принадлежат $\mathscr{R}$;

3) Если $U \in \mathscr{R}$, то $\mathscr{R}$ содержит также и порожденный множеством U подмоноид U^* моноида $(F(X)\times F(Y), \cdot)$, т. е. множество $U^* = U^0 \cup U^1 \cup U^2 \cup = \dots = \{u_1 \cdot u_2 \cdot \dots \cdot u_n \mid n \in \mathbf{N}_0,\ u_i \in U\}$, где $U^0 = \{(\Lambda, \Lambda\}$ и $U^{i+1} = U^i \cdot U$.

Теорема 8.4.10. (Элго, Мезей, Розенберг). Подмножество произведения $F(X)\times F(Y)$ рационально тогда и только тогда, когда оно является реакцией некоторого 2-ЭМ-автомата над (X, Y).

Доказательство. Пусть $P=(X\cup\Lambda)\times(Y\cup\Lambda)$ и ν_P — естественный гомоморфизм из $F(P)$ на $F(X)\times F(Y)$ (см. следствие 8.4.6). Тогда, как нетрудно проверить, выполняется равенство $\nu_P(\mathrm{Rat}(P))=\mathrm{Rat}(X, Y)$. Отсюда и из теоремы 8.4.7 немедленно вытекает доказываемое утверждение. ■

Замечания. 1. Рациональные преобразования оказываются, таким образом, в точности теми соответствиями, графики которых являются рациональными множествами. Поскольку графики соответствий часто рассматриваются как отношения, то рациональные подмножества произведения $F(X)\times F(Y)$ называют часто *рациональными отношениями.*

2. Рациональные подмножества произведения $F(X)\times F(Y)$ можно (как в примере 8.4.8) описывать рациональными выражениями при записи элементов в виде столбцов.

Очевидно, что теперь можно перенести на случай 2-ЭМ-автоматов и рациональных преобразований ряд результатов из гл. 5—7. (см. также упражнение 8.9, пп. 3, 4 и 6). Поскольку, однако, $(F(X)\times F(Y), \cdot)$ не является свободным моноидом, т. е. поскольку некоторые пары слов (u, v) могут быть различным образом представлены в виде произведения множителей вида (x, Λ) и (Λ, y), то на данный случай могут быть распространены не все высказывания (см. также п. 2 следствия 8.4.4).

Теорема 8.4.11. Множество $\mathrm{Rat}(X, Y)$ при $|X|+|Y|\geqslant 3$ не замкнуто относительно операций пересечения и дополнения.

Доказательство. Очевидно, что множества

$$U=\{(0^m1^n,\ 0^{m+2n})\mid n,m\in\mathbf{N}_0\}=\nu_P\left(\begin{pmatrix}0\\0\end{pmatrix}^*\begin{pmatrix}1\\0\,0\end{pmatrix}^*\right)\cap P=$$

$$=\left\{\begin{pmatrix}0\\0\end{pmatrix},\begin{pmatrix}1\\0\,0\end{pmatrix}\right\}\ \text{и}$$

$$V=\{(0^m1^n,\ 0^{2m+n})\mid n,m\in\mathbf{N}_0\}=\nu_P\left(\begin{pmatrix}0\\0\,0\end{pmatrix}^*\begin{pmatrix}1\\0\end{pmatrix}^*\right)\cap P=$$

$$=\left\{\begin{pmatrix}0\\0\,0\end{pmatrix},\begin{pmatrix}1\\0\end{pmatrix}\right\}$$

являются реакциями 2-ЭМ-автоматов над $(\{0, 1\}, \{0\})$. Однако выполняется равенство $U\cap V=\{(0^m1^m,\ 0^{3m})\mid m\in\mathbf{N}_0\}$, так что по теореме 5.4.12 $\mathrm{pr}_1(U\cap V)$ не является рациональным множеством, а потому $U\cap V$ по следствию 8.4.4, п.2 не может быть реакцией никакого 2-ЭМ-автомата. Поэтому пересечение реакций двух 2-ЭМ-автоматов не обязательно оказывается реакцией некоторого 2-ЭМ-автомата.

Из замкнутости относительно операции объединения и закона Моргана вытекает также незамкнутость относительно операции дополнения. ■

2-ЭМ-автомат A над (X, X) можно использовать для обработки слов из F(X) многими способами:

1. Слово w допускается, если (w, w) допускается автоматом A в обычном смысле.

2. Слово w допускается, если оно может быть разложено на два подслова u, v ($uv=w$) так, что пара (u, v) допускается автоматом A.

3. Слово $w=uv$ допускается, если пара (u, $\tilde{v}$) допускается автоматом A.

В первом случае 2-ЭМ-автомат можно интерпретировать как автомат с единственной входной лентой и двумя читающими головками, которые в начале работы располагаются в начале ленты и синхронно передвигаются слева направо, считывая содержимое одной и той же ячейки в каждый момент.

Во втором случае можно считать, что входные ленты 2-ЭМ-автомата считываются последовательно, одна за другой, причем специальный символ отмечает конец первой (и начало второй) ленты.

В третьем случае можно считать, что обе ленты объединены в одну, на которой записано одно слово, и что одна головка начинает работу, находясь на левом конце этой ленты, а вторая — на правом. Кроме того, головки двигаются навстречу друг другу до встречи в середине ленты.

Если рассматривать 2-ЭМ-автомат в третьей интерпретации как порождающую систему, то ему можно (как и в случае HPC-автоматов — см. разд. 5.2) сопоставить так называемую *линейную грамматику* $G=(Z, X, R, S)$ с правилами вида $z\to uz'v$ или $z\to w$ при z и z′ из Z и u, v и w из F(X).

Принятие вывода определяется так же, как в разд. 5.2: $w_1zw_2\Rightarrow_G w_3$ (для $w_i\in F(X)$) тогда и только тогда, когда в G существует правило $z\to w'$ такое, что $w_3=w_1w'w_2$.

Очевидно, что такими грамматиками могут порождаться и не рациональные подмножества моноида F(X), скажем множество $\{0^n1^n \mid n\in\mathbf{N}\}$ (соответственно такие подмножества могут допускаться 2-ЭМ-автоматами при каждой из трех приведенных выше интерпретаций). При первой интерпретации возьмем 2-ЭМ-автомат, допускающий множество $\{(0^k1^m, 0^n1^k \mid k, m, n\in\mathbf{N}\}$, во втором и в третьем случаях — 2-ЭМ-автомат с реакцией $\{(0^n, 1^n \mid n\in\mathbf{N}\}$.

8.5. ДВУЛЕНТОЧНЫЕ АВТОМАТЫ ЭЛГО — ЭЙЛЕНБЕРГА — ШЕФЕРДСОНА

2-ЭМ-автоматы недетерминированы в двух отношениях: недетерминированными, вообще говоря, являются фундаментальные HPC-автоматы и, кроме того, недетерминированным образом выбирается лента, с которой производится считывание, причем даже в том случае, когда фундаментальный HPC-ав-

томат оказывается ДРС-автоматом. Так, например, для 2-ЭМ-автомата, который соответствует изображенному на рис. 8.2.3 а-преобразователю (см. пример 8.4.2), в состоянии s при подаче на вход пары слов (00, 0) нельзя установить, должен ли быть считан на ленте 1 вход (0, Λ) или же на обеих лентах должен быть считан вход (0, 0). Это приводит к мысли о введении дополнительного правила выбора лент при считывании.

В этом разделе мы введем ограничение, состоящее в том, что автомат (пока это возможно) считывает посимвольно обе ленты, достигнув же конца слова на одной из лент, он продолжает считывание слова, записанного на другой ленте. Другой способ фиксации правила выбора лент при считывании будет исследован в разд. 8.7.

Определение 8.5.1. 2-ЭМ-автомат $A=(Z, X, Y, t\ S, F)$, где $Z=Z_0 \cup Z_1 \cup Z_2$, $Z_0 \cap (Z_1 \cup Z_2)=\varnothing$, $Z_1 \cap Z_2=\{z \in Z_1 \cap Z_2 \mid t(z, X \cup \Lambda, Y \cup \Lambda)=\varnothing\}$ и $\tau \subseteq Z_0 \times X \times Y \times Z \cup (Z_1 \cup Z_0) \times X \times \Lambda \times Z_1 \cup (Z_2 \cup Z_0) \times \Lambda \times Y \times Z_2$, называется *двуленточным автоматом Элго — Эйленберга — Шефердсона (коротко*: 2-ЭЭШ-автоматом).

Пример 8.5.2. 1. Множество $\{(0^k 1^m 1^k) \mid k, m \in \mathbf{N}\}$ является реакцией 2-ЭЭШ-автомата

$A_1=(\{s, z, z'\}, \{0, 1\}, \{0, 1\}, t, s, z')$, где

$\tau=\{(s, 0, 1, z), (z, 0, 1, z), (z, 1, \Lambda, z')\ (z', 1, \Lambda, z')\}$.

2. Множество $\{(w, w) \mid w \in F^+(\{0, 1\})\}$ является реакцией 2-ЭЭШ автомата $A_2=(\{s, z\}, \{0, 1\}, \{0, 1\}, t, s, z)$, где $\tau=\{(s, 0, 0, z), (s, 1, 1, z), (z, 0, 0, z), (z, 1, 1, z)\}$.

Описываемая теоремой 8.4.7 и ее доказательством связь между 2-ЭМ-автоматами и НРС-автоматами может быть более подробно проанализирована в случае 2-ЭЭШ-автоматов. Она приводит к очень полезной характеризации реакций 2-ЭЭШ-автоматов. Основная идея возникает при этом из наблюдения, что пара слов (u, v) из $F(X) \times F(Y)$ допускает единственное разложение в произведение следующим образом (соответствующим способу считывания 2-ЭЭШ-автоматов):

$$(u, v)=(x_1, y_1) \cdot (x_2, y_2) \cdot \ldots \cdot (x_k, y_k) \cdot (u', v')$$

при k из $\mathbf{N}_0$, $(x_1, y_1), \ldots, (x_k, y_k)$ из $X \times Y$, (u', v') из $F(X) \times F(Y)$ и $u'=\Lambda$ тогда и только тогда, когда $|u| \leqslant |v|$, и $v'=\Lambda$ тогда и только тогда, когда $|u| \geqslant |v|$.

Теорема 8.5.3 (Эйленберг, Элго, Шефердсон). Пусть

$P_0=X \times Y$, $P_1=X \times \Lambda$, $P_2=\Lambda \times Y$ и $P=P_0 \cup P_1 \cup P_2$.

Для рационального подмножества $V=P_0^*(P_1^* \cup P_2^*)$ моноида $F(P)$ и естественного гомоморфизма ν_P из $F(P)$ на $F(X) \times F(Y)$ в этом случае:

1. $\nu_P(V)=F(X) \times F(Y)$.

Ограничение ν_P/V гомоморфизма ν_P на V является инъективным и сюръективным отображением, так что обратное для него отображение β оказывается биекцией из $F(X) \times F(Y)$ на V.

2. Если A — 2-ЭЭШ-автомат над (X, Y) и A′ — НРС-автомат, получающийся при интерпретации A как НРС-автомата над P, то $L(A') = \beta(L(A)) \subseteq V$.

3. Если A′ — D-минимальный ДРС-автомат над P такой, что $L(A') \subseteq V$, и A — 2-ЭМ-автомат, получающийся при интерпретации A′ как 2-ЭМ-автомата над (X, Y), то A является 2-ЭЭШ-автоматом с $L(A) = \nu_P(L(A'))$.

4. Подмножество L произведения $F(X) \times F(Y)$ является реакцией некоторого 2-ЭЭШ-автомата над (X, Y) тогда и только тогда, когда $\beta(L)$ является рациональным подмножеством моноида $\Gamma(P)$.

Доказательство. 1. Утверждение 1 непосредственно вытекает из приведенного выше разложения элементов из $F(X) \times F(Y)$ в произведение элементов из P_0, сопровождаемых элементами только из P_1 или только из P_2 в зависимости от того, которая из компонент (слов) длиннее. Отметим, что β не является гомоморфизмом, поскольку V — не моноид, и что отображение β не «мультипликативно»: например $\beta(0, \Lambda)\beta(\Lambda, 0) \notin V$.

2. Утверждение 2 вытекает непосредственно из доказательства теоремы 8.4.7 и определения 8.5.1.

3. D-минимальный ДРС-автомат $A' = (Z, P, t, s, F)$ над P не имеет «лишних» состояний: каждое состояние A достижимо и из каждого состояния возможен переход в некоторое финальное состояние.

Пусть $Z_0' = t^*(s, P_0^*)$, $Z_1 = t^*(Z_0', P_1^+)$, $Z_2 = t^*(Z_0', P_2^+)$ и $Z_0 = Z_0' - (Z_1 \cup Z_2)$. (Отметим, что если $\Lambda \notin E$, то $E^+ = E^+ - \Lambda = EE^*$.)

Чтобы показать, что A′, рассматриваемый как 2-ЭМ-автомат, оказывается 2-ЭЭШ-автоматом, нам нужно доказать следующее:

а) $\tau \cap Z_i \times P \times Z \subseteq Z_i \times P_i \times Z_i$ при $i = 1, 2$;

б) $Z = Z_0 \cup Z_1 \cup Z_2$ и $Z_1 \cap Z_2 = \{z \in Z_1 \cap Z_2 \mid t(z, P) = \varnothing\}$.

Докажем п.а). Пусть $z \in Z_i$, $z' \in Z$, $p \in P$, причем $(z, p, z') \in \tau$, и $i = 1$ или $i = 2$. Тогда по предположению существуют u, v и w в F(P) такие, что $u \in P_0^*$, $v \in P_i^+$, $t^*(s, uv) = z$ и $uvpw \in L(A')$. Из включения $L(A') \subseteq V$ при этом вытекает, что $uvpw \in P_0^* P_i^+$, так что $p \in P_i$. Так как $z' = t^*(s, uvp) = t^*(t^*(s, u), vp)$ и $t^*(s, u) \in Z_0'$, то выполняется включение $z' \in Z_i$, чем и доказывается п.а).

Докажем п.б). Пусть $z \in Z$. Тогда в F(X) существуют слова u и v такие, что $uv \in L(A') \subseteq V$ и $z = t^*(s, u)$. Если $u \in P_0^*$, то $z \in Z_0'$ или $z \in Z_1 \cup Z_2$, т. е. $Z = Z_0 \cup Z_1 \cup Z_2$.

Если бы для некоторого z из $Z_1 \cap Z_2$ существовало $p \in P$ такое, что $t(z, p) \neq \varnothing$, то из п.а) следовало бы включение $p \in P_1 \cap P_2$, чего не может быть. Так что должно выполняться равенство $Z_1 \cap Z_2 = \{z \in Z_1 \cap Z_2 \mid t(z, P) \neq \varnothing\}$, чем и доказывается п.б).

4. Если L — реакция некоторого 2-ЭЭШ-автомата A над (X, Y), т. е $L = L(A)$, то из п.2 вытекает также $\beta(L) = \beta(L(A)) = L(A')$, т. е. $\beta(L)$ оказывается рациональным подмножеством моноида F(P).

Если же для $L \subseteq F(X) \times F(Y)$ множество $\beta(L)$ рационально, то существует D-минимальный ДРС-автомат A′ над P, допускающий

$\beta(L)$. Из п.3 в этом случае получаем $L=\nu_P(\beta(L))=\nu_P(L(A'))=$ $=L(A)$.

Итак, L является реакцией 2-ЭЭШ-автомата A над (X, Y). ▪

Замечания. 1. Из высказываний 3 и 4 теоремы 8.5.3 вытекает, что для каждого 2-ЭЭШ-автомата существует эквивалентный 2-ЭЭШ-автомат, функционирующий вполне детерминированным образом, т. е. такой, что фундаментальный для него НРС-автомат оказывается ДРС-автоматом.

2. Легко видеть, что высказывания 2—4 теоремы 8.5.3 могут быть обобщены на произвольные множества P, для которых ν_P удовлетворяет высказыванию 1 теоремы, и на соответствующие типы автоматов. В частности, множество P_0 в теореме можно заменить на множество

$P_0'=\{(x, \Lambda)(\Lambda, y) \mid (x, y)\in P_0\}$ (см. упражнение 8.10).

Следствие 8.5.4. Множество реакций 2-ЭЭШ-автоматов над (X, Y):

замкнуто относительно булевых операций (объединения, пересечения, дополнения);

содержит все множества вида $R_1\times R_2$, где $R_1\in Rat(X)$ и $R_2\in$ $\in Rat(Y)$;

содержит все конечные подмножества произведения $F(X)\times$ $\times F(Y)$;

не замкнуто относительно операции образования произведения.

Доказательство. 1. Пусть L и L′ — реакции 2-ЭЭШ-автоматов над $F(X)\times F(Y)$. По теореме 8.5.3, п. 4 в этом случае множества $\beta(L)$ и $\beta(L')$ оказываются рациональными подмножествами моноида F(P). Поскольку по теореме 5.5.5 множество Rat(P) замкнуто относительно булевых операций, поскольку V принадлежит Rat(P) и β по теореме 8.5.3, п. 1 инъективно, то и множества $\beta(L\cup L')=\beta(L)\cup\beta(L')$, $\beta(L\cap L')=\beta(L)\cap\beta(L')$ и $\beta(F(X)\times F(Y)-$ $-L)=V-\beta(L)$ рациональны. По теореме 8.5.3, п. 4 поэтому и множества $L\cup L'$, $L\cap L'$, $F(X)\times F(Y)-L$ являются реакциями некоторых 2-ЭЭШ-автоматов.

2. Пусть $R\in Rat(X)$ и A — D-минимальный ДРС-автомат, допускающий множество R. Тогда множество $R\times F(Y)$ допускается следующим 2-ЭЭШ-автоматом A′:

$A'=(Z\times z_1\cup Z\cup z_2, P, t', (s, z_1), F\times z_1\cup F\cup z_2)$, где

$\tau'=\{((z, z_1), x, y, (z', z_1)) \mid f(z, x)=z', y\in Y\}\cup$

$\cup\{((z, z_1), x, \Lambda, z') \mid f(z, x)=z'\}\cup$

$\cup\{(z, x, \Lambda, z') \mid f(z, x)=z'\}\cup\{((z, z_1), \Lambda, y, z_2) \mid z\in F, y\in$

$\in Y\}\cup\{(z_2, \Lambda, y, z_2) \mid y\in Y\}$.

В состояниях из $F\times z_1$ «допускаются» пары (w, v) с $|w|=|v|$ и $w\in R$, в состояниях из F — пары (w, v) с $|w|>|v|$ и $w\in R$, в состоянии z_2 — пары (w, v) с $|w|<|v|$ и $w\in R$.

Аналогично показывается, что $F(X)\times R'$ при $R'\in Rat(Y)$ является реакцией некоторого 2-ЭЭШ-автомата. Из п.1 поэтому сле-

дует, что и множество $R \times R' = R \times F(Y) \cap F(X) \times R'$ оказывается реакцией некоторого 2-ЭЭШ-автомата.

3. Так как $\{(u, v)\} = \{u\} \times \{v\}$, из пп.1 и 2 вытекает, что все конечные множества являются реакциями соответствующих 2-ЭЭШ-автоматов.

4. Пусть $W = (\Lambda \times 0^+) \cdot \{(0^k 1^m, 1^k) \mid k, m \in \mathbf{N}\} = \{(0^k 1^m, 0^n 1^k) \mid k, m, n \in \mathbf{N}\}$. Из п.1 примера 8.5.2 и из п.2 данного доказательства вытекает, что оба сомножителя в W являются реакциями 2-ЭЭШ-автоматов. Далее, из п.2 примера 8.5.2 следует, что множество $D = \{(w, w) \mid w \in F^+(\{0, 1\})\}$ также является реакцией некоторого 2-ЭЭШ-автомата. Если бы теперь W было реакцией некоторого 2-ЭЭШ-автомата, то на основании 1 и множество $W \cap D = \{0^k 1^k, 0^k 1^k) \mid k \in \mathbf{N}\}$ должно было бы быть реакцией соответствующего 2-ЭЭШ-автомата, чего не может быть, как вытекает из п.3 следствия 8.4.4 и теоремы 5.4.12. Итак, произведение W реакций двух 2-ЭЭШ-автоматов не является реакцией никакого 2-ЭЭШ-автомата. ■

Замечание. Из данного следствия получаем, что не для каждого 2-ЭМ-автомата существует эквивалентный 2-ЭЭШ-автомат.

8.6. ДЕТЕРМИНИРОВАННЫЕ ДВУЛЕНТОЧНЫЕ АВТОМАТЫ

ДЕТЕРМИНИРОВАННЫЕ 2-ЭМ-АВТОМАТЫ

Пусть A_1 — представленный на рис. 8.2.3 2-ЭМ-автомат (см. п.1 примера 8.4.2). Этот 2-ЭМ-автомат обладает свойством, которое не встречается у НРС-автоматов: соответствие переходов t_1 автомата A_1 является частичным отображением, однако последовательностное соответствие t_1^* автомата A_1 не является отображением, поскольку, например $t_1^*(s, 00, 0) = \{z, z'\}$, так как $(0, \Lambda) \cdot (0, 0) = (0, 0) \cdot (0, \Lambda)$.

Итак, для того чтобы определить общее понятие детерминированного 2-ЭМ-автомата, мы должны требовать большего, чем в случае НРС-автоматов.

Определение 8.6.1. Пусть A — 2-ЭМ-автомат в обозначениях определения 8.4.1.

Автомат A называется *локально детерминированным*, если t является частичным отображением.

Автомат A называется *детерминированным*, если $|S| = 1$ и t^* является частичным отображением.

Замечания. 1. 2-ЭМ-автомат A является, очевидно, локально детерминированным, если его фундаментальный НРС-автомат A′ детерминирован. Из доказательства теоремы 8.4.7 и утверждения теоремы 6.2.8 следует, что для каждого 2-ЭМ-автомата может быть построен эквивалентный локально детерминированный 2-ЭМ-автомат.

2. По теореме 8.5.3 (см. замечание к ней) для каждого 2-ЭЭШ-автомата может быть построен эквивалентный детерминирован-

ный 2-ЭМ-автомат, являющийся одновременно и 2-ЭЭШ-автоматом. Обратное, однако, неверно. Действительно, множество W из п.4 доказательства следствия 8.5.4, хотя и допускается некоторым детерминированным 2-ЭМ-автоматом, но не допускается никаким 2-ЭЭШ-автоматом.

Пример 8.6.2. 1. 2-ЭМ-автомат из примера 8.4.2, хотя и локально детерминирован, но не детерминирован (как показано выше).

2. Построенные в доказательстве п.2 следствия 8.4.4 2-ЭМ-автоматы A и A′, очевидно, детерминированы. Таким образом, вопрос о непустоте пересечения реакций неразрешим даже для детерминированных 2-ЭМ-автоматов.

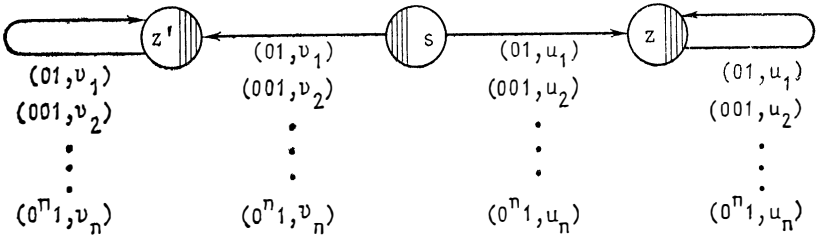


Рис. 8.6.1. 2-ЭМ-автомат A_Q

3. Каждый конечный преобразователь с допускающими состояниями, рассматриваемый как 2-ЭМ-автомат, оказывается детерминированным 2-ЭМ-автоматом, поскольку его «читающая часть» функционирует детерминированным образом (таковы и конечные преобразователи, приведенные на рис. 8.2.1 и в примере 8.2.1).

4. Множество U и V из доказательства следствия 8.4.11 допускаются, очевидно, некоторыми детерминированными 2-ЭМ-автоматами. Поэтому пересечение реакций детерминированных 2-ЭМ-автоматов не допускается, вообще говоря, детерминированным 2-ЭМ-автоматом.

Поскольку для 2-ЭМ-автомата локальной проверкой, т. е. изучением значений соответствия переходов на отдельных состояниях, нельзя установить, является ли этот 2-ЭМ-автомат детерминированным, то проверка детерминированности оказывается в общем случае очень сложной.

Теорема 8.6.3. Для 2-ЭМ-автоматов (с по меньшей мере двухэлементным входным алфавитом) неразрешим вопрос о том, являются ли они детерминированными.

Доказательство. Используем для доказательства неразрешимость общей проблемы соответствий Поста (см. лемму 8.3.5). С этой целью мы сопоставим каждому случаю Q проблемы соответствий Поста над $X=\{0, 1\}$ (заданному, как в определении 8.3.4) 2-ЭМ-автомат A_Q, определяемый графом, изображенным на рис. 8.6.1.

Итак, пусть $A_Q=(\{s, z, z'\}, X, X, t, s, \{z, z'\})$, где $\tau=\{(z'', 0^i1, u_i, z) \mid i=1, 2, \ldots, n, z''=s$ или $z''=z\}\cup\{(z'', 0^i1, v_i, z') \mid i=1, 2, \ldots, n, z''=s$ или $z''=z'\}$.

Сразу видно следующее.

1. Если автомат A_Q не локально детерминирован, то по меньшей мере для одного $i \in \{1, \ldots, n\}$ должно выполняться равенство $u_i = v_i$. Тогда Q имеет решение i.

2. Если автомат A_Q локально детерминирован, то A не является детерминированным 2-ЭМ-автоматом тогда и только тогда, когда существуют натуральные числа $i_1, i_2, \ldots, i_k$ такие, что

$$u_{i_1} u_{i_2} \ldots u_{i_k} = v_{i_1} v_{i_2} \ldots v_{i_k}.$$

Действительно, именно в этом случае выполняется равенство

$$t^*(s, 0^{i_1}10^{i_2}1 \ldots 0^{i_k}1, u_{i_1}u_{i_2}\ldots u_{i_k}) = t^*(s, 0^{i_1}10^{i_2}1 \ldots 0^{i_k}1,$$

$$v_{i_1}v_{i_2}\ldots v_{i_k}) = \{z, z'\}.$$

Итак, если автомат A_Q локально детерминирован, то A_Q является детерминированным 2-ЭМ-автоматом тогда и только тогда, когда случай Q проблемы соответствий Поста над X не имеет решения.

3. Из пп. 1 и 2 следует, что с помощью метода, определяющего, является ли данный 2-ЭМ-автомат над (X, X) детерминированным, можно также определить, разрешима ли общая проблема соответствий Поста над X, что по лемме 8.3.5 невозможно. ■

Замечания. 1. Отметим, что для а-преобразователя можно очень просто установить, является ли он детерминированным, т. е. является ли он конечным преобразователем с допускающими состояниями, поскольку для этого достаточно лишь проверить, является ли его «читающая часть» ДРС-автоматом.

2. Детерминированный 2-ЭМ-автомат, рассматриваемый как а-преобразователь, не обязательно должен быть конечным преобразователем с допускающими состояниями. Контрпримером является детерминированный 2-ЭМ-автомат $A = (\{1, 2, 3\}, \{0\}, \{0, 1\}, t, 1, \{2, 3\})$, где $\tau = \{(1, 0, 0, 2), (1, 1, 1, 2), (1, 0, 1, 3), (2, 0, 0, 2), (2, 1, 1, 2), (3, 0, 1, 3), (3, 1, 0, 2)\}$.

АЛФАВИТНЫЕ ДЕТЕРМИНИРОВАННЫЕ 2-ЭМ-АВТОМАТЫ

Путем добавления состояний (как и в случае НРС-автоматов в доказательстве п.1 теоремы 6.2.7) для любого 2-ЭМ-автомата можно построить эквивалентный алфавитный 2-ЭМ-автомат, т. е. автомат, считывающий по одному символу за такт, причем только с одной ленты. В отличие от случая НРС-автоматов, в данном случае такой переход не детерминирован.

Определение 8.6.4. 2-ЭМ-автомат называется *алфавитным*, если $\tau \subseteq Z \times (X \cup \Lambda) \times \Lambda \times Z \cup Z \times \Lambda \times (Y \cup \Lambda) \times Z$.

Пример 8.6.5. Детерминированный 2-ЭМ-автомат, граф которого изображен на рис. 8.6.2, является алфавитным и допускает множество W из п.4 доказательства следствия 8.5.4.

Из доказательства теоремы 8.6.3 вытекает, что и для алфавитных 2-ЭМ-автоматов неразрешим вопрос о том, являются ли они детерминированными (см. п.1 упражнения 8.11).

Теорема 8.6.6. Множество $M=\{(0^k, 0^m1^n) \mid k, m, n\in\mathbf{N}, k=m$ или $k=n\}$, хотя и допускается некоторым алфавитным 2-ЭМ-автоматом, но не допускается никаким алфавитным детерминированным 2-ЭМ-автоматом. В то же время M является объединением реакций двух алфавитных детерминированных 2-ЭМ-автоматов.

Доказательство. 1. Граф алфавитного 2-ЭМ-автомата, допускающего множество M, изображен на рис. 8.6.3.

Обе части рис. 8.6.3 представляют собой графы детерминированных 2-ЭМ-автоматов. Объединением их реакций является множество M.

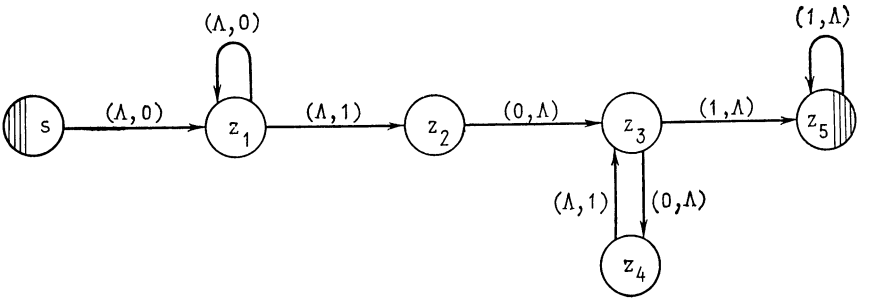


Рис. 8.6.2. Детерминированный 2-ЭМ-автомат с реакцией W

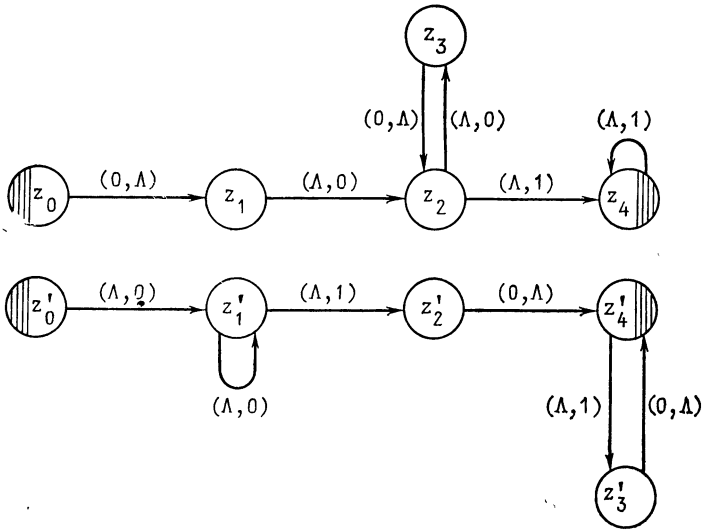


Рис. 8.6.3. Алфавитный 2-ЭМ-автомат с реакцией M

Используя построения из приведенного ниже доказательства, можно без особого труда получить неалфавитный детерминированный 2-ЭМ-автомат, допускающий множество M (см. п.2 упражнения 8.11).

2. Пусть $X=\{0, 1\}$. Предположим, что существует детерминированный 2-ЭМ-автомат $A=(Z, X, X, t, s, F)$, где $\tau\subseteq Z\times X\times\Lambda\times Z\cup Z\times\Lambda\times X\times Z$ и $L(A)=M$.

Пусть $p\in\mathbf{N}$, причем $p>|Z|$ и $L_{0,p}=\{(0^k, 0^k1^n)\,|\,k, n\in\mathbf{N}, n, k>p\}$, $L_{1,p}=\{(0^k, 0^m1^k)\,|\,k, m\in\mathbf{N}, m, k\geqslant p\}$, $(u, v)\in L_{0,p}\cup L_{1,p}$.

I. Поскольку пара слов (u, v) должна допускаться автоматом A, то должны существовать состояние z в Z, число $i\geqslant 1$ и слово w в F(X) такие, что $t^*(z, 0^i, w)=z$.

Для этой тройки z, i, w имеем:

1) $w\in 0^*$ или $w\in 1^*$. Действительно, если бы выполнялось равенство $w=a01b$, то при подходящих $q\in\mathbf{N}$ и c, $d\in F(X)$ пара $(0^{q+2i}, ca01ba01bd)$ допускалась бы автоматом A, чего быть не может.

2) $|w|=i$. Действительно, если бы, скажем, выполнялось равенство $w=0^q$ при $q\neq i$, то вместе с парой $(u, v)=(0^k, 0^m1^n)$ при каждом j из **N** допускалась бы автоматом A и пара $(0^{k+j\cdot i}, 0^{m+j\,q}1^n)$, чего быть не должно. В случае $w=1^q$ рассуждения аналогичны.

3) Существует по меньшей мере одна тройка z_0, i, w_0 с $w_0=0^i$, т. е. $t^*(z_0, 0^i, 0^i)=z_0$, и по меньшей мере одна тройка z_1, j, w_1 с $w_1=1^j$, т. е. $t^*(z_1, 0^j, 1^j)=z_1$. Действительно, если бы, например, всегда выполнялось включение $w\in 0^*$, то должны бы были существовать состояние z'' и число r такие, что $t^*(z'', \Lambda, 1^r)=z''$ [пара $(0^p, 0^{p-1}, 1^p)$ допустима]. Отсюда бы вытекало, что автомат A допускает пару $(0^p, 0^{p-1}, 1^{p+r})$. Аналогичным образом предположение, что всегда выполняется включение $w\in 1^*$, приводит к противоречию.

Состояния типа z_0 и z_1 из п.3, будем в дальнейшем называть *(0, 0)*- и соответственно *(0, 1)-цикловыми состояниями.*

II. На *допускающем пути*, т. е. на пути из начального в некоторое финальное состояние, в графе автомата A не могут одновременно встречаться (0, 0)- и (0, 1)-цикловые состояния, поскольку в противном случае автоматом A допускались бы при произвольных q и r из **N** пары $(0^{p+qi+rj}, 0^{p+qi}1^{p+rj})$.

Чтобы автомат мог допускать пары вида $(0^p, 0^p1^{2p})$, он должен иметь еще *(Λ, 1)-цикловое состояние*, т. е. состояние z_2 такое, что $t^*(z_2, \Lambda, 1^k)=z_2$ при подходящем k из **N**. Такое состояние может, конечно, встречаться в одном допускающем пути с (0, 0)-цикловым состоянием, но не с (0, 1)-цикловым состоянием.

Аналогичным образом показывается, что должно иметься и *(Λ, 0)-цикловое состояние.*

У автомата A не может быть иных цикловых состояний, поскольку вследствие I из равенства $t^*(z, w, w')=z$ вытекает, что z является (0, 0)-, (0, 1)-, (Λ, 0)- или (Λ, 1)-цикловым состоянием. Кроме того, из вышесказанного следует, что любое цикловое со-

стояние является цикловым состоянием в точности одного из этих типов.

Итак, имеются три вида допускающих путей:

1′) 0-пути. На таких путях сначала встречаются (0, 0)-цикловые состояния и только после последнего из них встречаются (Λ, 1)-цикловые состояния, причем имеется по меньшей мере по одному состоянию каждого типа. С помощью таких путей допускается бесконечно много слов из $L_{0,p}$.

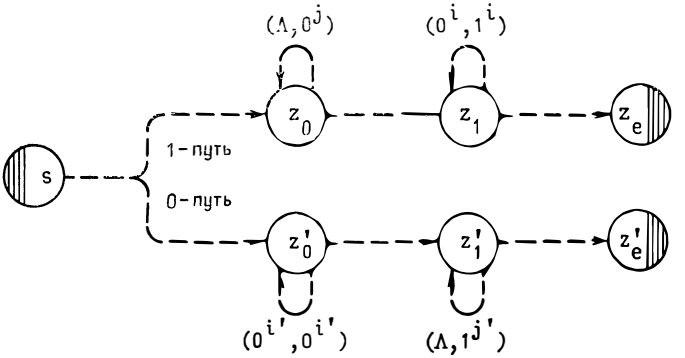


Рис. 8.6.4. Возможные допускающие пути

2′) 1-пути. На таких путях сначала встречаются (Λ, 0)-цикловые состояния и после них — (0, 1)-цикловые состояния, причем имеется по меньшей мере по одному состоянию каждого вида. С помощью таких путей допускается бесконечно много слов из $L_{1,p}$.

3′) Пути, на которых нет цикловых состояний либо есть цикловые состояния только одного вида.

III. Рассмотрим теперь вопрос о том, как происходит обработка элементов пересечения $L_{0,p} \cap L_{1,p}$. Эта обработка осуществляется только с помощью 0- или 1-путей.

Предположим, что пара $(0^{3p}, 0^{3p}1^{3p})$ допускается с помощью некоторого 1-пути из s в финальное состояние z_e. Пусть z_1 — первое (0, 1)-цикловое состояние на этом пути. Из z_1 в z_e ведет некоторый путь, на котором со второй ленты считываются только единицы.

Пара $(0^{3p}, 0^{3p}1^{4p})$ может допускаться только с помощью 0-пути с некоторым финальным состоянием z_e'. Пусть z_1' — первое (Λ, 1)-цикловое состояние на этом пути. Из z_1' в z_e' ведет тогда некоторый путь, на котором со второй ленты считываются только единицы. Итак, имеется ситуация, показанная на рис. 8.6.4.

Поскольку $p > |z|$, то должен существовать путь из s в z_1', на котором считывается пара слов $(0^k, 0^{3p}1^q)$, где $2p < k \leqslant 3p$ и $0 \leqslant q < p$.

Так как автомат A алфавитный, то в цикле у вершины z_1 или на пути из z_1 в z_e существует состояние z такое, что $t^*(s, 0^k,$

$0^{3p}1^n)=z$ и $n\geqslant p$. Отсюда же (так как $q<n$) следует, что в цикле у вершины z_1' существует состояние z' такое, что $t^*(s, 0^k, 0^{3p}1^n)=z'$.

Поскольку автомат А детерминированный, то должно выполняться равенство $z'=z$. Поэтому либо состояние z должно одновременно быть и (0, 1)- и (Λ, 1)-цикловым состоянием, либо (Λ, 1)-цикловое состояние z' должно лежать на 1-пути из z_1 в z_e, чего не может быть.

Итак, пара слов $(0^{3p}, 0^{3p}1^{3p})$ не может допускаться с помощью 1-пути.

Предположим теперь, что пара слов $(0^{3p}, 0^{3p}1^{3p})$ допускается с помощью некоторого 0-пути, имеющего вид, изображенный на рис. 8.6.4, т. е. будем считать, что первое (Λ, 1)-цикловое состояние на этом пути есть z_1'.

Пара слов $(0^{4p}, 0^{3p}1^{4p})$ допускается с помощью некоторого 1-пути, имеющего вид, представленный на рис. 8.6.4. Итак, будем считать, что первое (0,1)-цикловое состояние на этом пути есть z_1.

Теперь будем действовать совершенно аналогично тому, как это делалось выше.

На некотором пути из s в z_1' может быть считана пара слов $(0^k, 0^{3p}1^m)$, где $2p<k\leqslant 3p$ и $m\leqslant p$. Поскольку автомат А алфавитный, то в цикле у состояния z_1 или после него существует состояние z такое, что $t^*(s, 0^k, 0^{3p}1^n)=z$ и $n\geqslant p$. По той же причине, а также вследствие неравенства $m\leqslant n$ в этом случае в цикле у z_1' существует состояние z' такое, что $t^*(s, 0^k, 0^{3p}1^n)=z'$.

Так как автомат А детерминирован, то должно быть $z=z'$, но это невозможно.

Итак, пара слов $(0^{3p}, 0^{3p}1^{3p})$ вообще не допускается, т. е. не существует допускающего множества М алфавитного детерминированного 2-ЭМ-автомата. ■

Замечания. 1. Из п.2 замечаний к теореме 8.5.3, п.2 и замечаний к определению 8.6.1 вытекает, что для каждого 2-ЭЭШ-автомата существует эквивалентный алфавитный детерминированный 2-ЭМ-автомат. Из примера 8.6.5 и из сказанного выше следует, что множество реакций 2-ЭЭШ-автоматов оказывается собственным подмножеством множества реакций алфавитных детерминированных 2-ЭМ-автоматов.

2. Существует ли для каждого 2-ЭМ-автомата эквивалентный детерминированный 2-ЭМ-автомат, неизвестно. Можно, однако, предполагать, что множество
$D=\{(uc, vuw)\,|\,u, v, w\in F^+(Y)\}$, где $c\notin Y$ и $|Y|=2$, являющееся, очевидно, реакцией соответствующего 2-ЭМ-автомата, не может допускаться никаким детерминированным 2-ЭМ-автоматом.

ПОЛНОСТЬЮ ОПРЕДЕЛЕННЫЕ ДЕТЕРМИНИРОВАННЫЕ 2-ЭМ-АВТОМАТЫ

Из ДРС-автомата мы смогли путем добавления единственного состояния построить полностью определенный детерминированный эквивалентный автомат (РС-автомат). Ниже мы увидим, что в

случае детерминированных 2-ЭМ-автоматов соответствующее построение невозможно.

Определение 8.6.7. Детерминированный 2-ЭМ-автомат называется *полностью определенным* детерминированным 2-ЭМ-автоматом, если t* является всюду определенным отображением, т. е. если выполняется равенство $\mathrm{pr}_{1,2,3}(\tau^*) = Z \times F(X) \times F(Y)$.

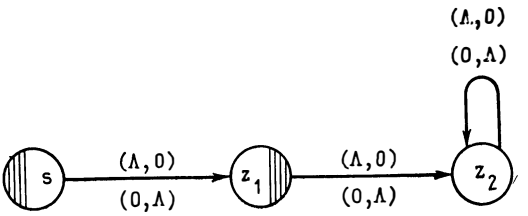


Рис. 8.6.5. Полностью определенный детерминированный 2-ЭМ-автомат с реакцией {(0, Λ), (Λ, 0)}

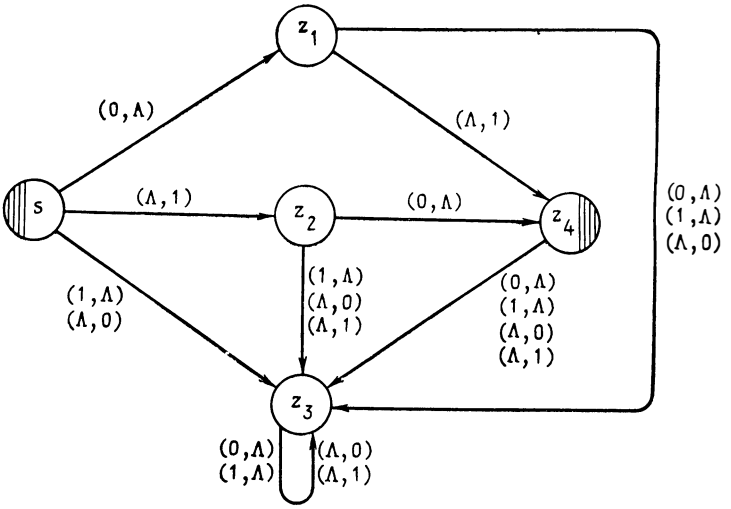


Рис. 8.6.6. Полностью определенный детерминированный 2-ЭМ-автомат с реакцией {(0, 1)}

Пример 8.6.8. 1. На рис. 8.6.5 изображен граф полностью определенного детерминированного 2-ЭМ-автомата над ({0}, {0}), допускающего множество {(0, Λ), (Λ, 0)}.

2. На рис. 8.6.6 изображен граф полностью определенного детерминированного 2-ЭМ-автомат над ({0, 1}, {0, 1}), допускающего множество {(0, 1)}.

3. Пусть A — полностью определенный детерминированный 2-ЭМ-автомат в обычных обозначениях. Тогда $\bar{A} = (Z, X, Y, t, s, Z - F)$ — полностью определенный детерминированный 2-ЭМ-автомат, допускающий дополнение $F(X) \times F(Y) - L(A)$ реакции автомата A. Читателю рекомендуется сравнить этот факт с доказа-

тельством теоремы 5.5.5 и обратить внимание на то, что автомат A полностью определен и детерминирован.

4. Пусть A_1 и A_2 — алфавитные полностью определенные детерминированные 2-ЭМ-автоматы над (X, Y).
Тогда

$$A=(Z_1\times Z_2,\ X,\ Y,\ t,\ (s_1, s_2),\ F_1\times F_2),$$

где $\tau=\{((z_1, z_2),\ x,\ y,\ (z_1', z_2'))\mid (z_1, x, y, z_1')\in\tau_1,\ (z_2, x, y, z_2')\in\in\tau_2\}$ — полностью определенный детерминированный 2-ЭМ-автомат, допускающий пересечение реакций $L(A_1)\cap L(A_2)$ автоматов A_1 и A_2 (см. упражнение 5.16). Действительно, автомат A полностью определен и при произвольных z_i из Z_i (при $i=1,2$), произвольной паре слов (u, v) из $F(X)\times F(Y)$, произвольной паре входов (x, y) из $(X\cup\Lambda)\times(Y\cup\Lambda)$ и при $t^*((z_1, z_2),\ u,\ v)=(z_1', z_2')$ выполняется равенство

$t(t^*((z_1, z_2),\ u,\ v),\ x,\ y)=(t_1(z_1', x, y),\ t_2(z_2', x, y))$. Отсюда полной индукцией по $|u|+|v|$ получаем, что всегда выполнено равенство

$$t^*((z_1, z_2),\ u,\ v)=(t_1^*(z_1, u, v),\ t_2^*(z_2, u, v)).$$

Итак, автомат A также является детерминированным и пара (u, v) допускается этим автоматом тогда и только тогда, когда она допускается и автоматом A_1, и автоматом A_2.

Обобщение этой конструкции приведено в пп. 3 и 4 упражнения 8.11.

5. Пусть A_1 и A_2 — РС-автоматы над X и Y соответственно. Пусть тогда A — следующий 2-ЭМ-автомат:

$$A=(Z_1\times Z_2,\ X,\ Y,\ t,\ (s_1, s_2),\ F_1\times F_2),\ \text{где}$$

$$\tau=\{((z_1, z_2),\ x,\ \Lambda,\ (z_1', z_2))\mid (z_1, x, z_1')\in\tau_1\}\cup$$

$$\cup\{((z_1, z_2),\ \Lambda,\ y,\ (z_1, z_2'))\mid (z_2, y, z_2')\in\tau_2\}.$$

Для любой пары слов (u, v) из $F(X)\times F(Y)$ выполняется равенство $t^*((z_1, z_2),\ u,\ v)=(t_1^*(z_1, u),\ t_2^*(z_2, v))$. Поскольку t_1^* и t_2^* — полностью определенные отображения, то и t^* оказывается полностью определенным отображением. Итак, A — полностью определенный детерминированный 2-ЭМ-автомат с реакцией $L(A_1)\times\times L(A_2)$.

Замечания. 1. Алфавитный детерминированный 2-ЭМ-автомат является полностью определенным детерминированным 2-ЭМ-автоматом, если $pr_{1,2,3}(\tau)=Z\times X\times\Lambda\cup Z\times\Lambda\times Y$.

2. Для каждого полностью определенного детерминированного 2-ЭМ-автомата A можно построить эквивалентный алфавитный полностью определенный детерминированный 2-ЭМ-автомат

$A'=(Z, X, Y, t', s, F)$, полагая

$\tau'=(Z\times X\times\Lambda\times Z\cup Z\times\Lambda\times Y\times Z)\cap\tau^*$.

Таким образом, в дальнейшем мы может ограничиться рассмотрением алфавитных детерминированных 2-ЭМ-автоматов, удовлетворяющих условию из п.1 данных замечаний.

3. Пусть A — алфавитный полностью определенный детерминированный 2-ЭМ-автомат. Тогда для любого состояния z и произвольной пары слов (u, v) из $F(X)\times F(Y)$ справедливы равенства

$$t^*(z, u, v) = t^*(t^*(z, u, \Lambda), \Lambda, v) =$$
$$= t^*(t^*(z, \Lambda, v), u, \Lambda).$$

Итак, читающие головки автомата A могут передвигаться в произвольном порядке. Поэтому мы можем заменить («эквивалентно») автомат A на последовательное соединение двух НРС-автоматов A_1 и A_2, каждый из которых считывает только одну ленту:

$$A_1 = (Z, X, t_1, s, Z),\ \tau_1 = pr_{1,2,4}(\tau),$$
$$A_2 = (Z, Y, t_2, Z, F),\ \tau_2 = pr_{1,3,4}(\tau).$$

Пара входных слов (u, v) считывается при этом таким образом, что сначала A_1 прочитывает слово u, а после этого автомат A_2 начинает работу в состоянии, в котором A_1 ее закончил, и прочитывает слово v. (См. по этому поводу также упражнение 8.10, п. 2.)

Из данного замечания и примера 8.6.8 вытекают факты, демонстрирующие очень тесную связь между РС-автоматами и полностью определенными детерминированными 2-ЭМ-автоматами.

Теорема 8.6.9. 1. Множество реакций полностью определенных детерминированных 2-ЭМ-автоматов над (X, Y) образует булеву алгебру (с теоретико-множественными операциями).

2. Подмножество L произведения моноидов $F(X)\times F(Y)$ является реакцией некоторого полностью определенного детерминированного 2-ЭМ-автомата над (X, Y) тогда и только тогда, когда оно является объединением конечного числа декартовых произведений $R\times R'$ рациональных подмножеств R и R′ моноидов F(X) и F(Y) соответственно.

3. Пусть отображение $k: F(X)\times F(Y)\to F(X\cup Y)$ определено условием: $k(u, v) = uv$ для всех (u, v) из $F(X)\times F(Y)$. Отображение k называется *конкатенацией.*

Для каждого полностью определенного детерминированного 2-ЭМ-автомата A над (X, Y) множество $k(L(A))$ является рациональным подмножеством моноида $F(X\cup Y)$.

4. Если $X\cap Y = \varnothing$, то для $L\subseteq F(X)\times F(Y)$ из включения $k(L)\in \in Rat(X\cup Y)$ следует, что L — реакция некоторого полностью определенного детерминированного 2-ЭМ-автомата.

Доказательство. 1. Из пп. 3 и 4 примера 8.6.8 немедленно вытекает замкнутость относительно операций пересечения и дополнения, поскольку на основе п.2 замечаний к примеру 8.6.8 мы можем ограничиться рассмотрением только алфавитных полностью определенных детерминированных 2-ЭМ-автоматов. Замкнутость относительно операции объединения вытекает из закона Моргана.

2. Пусть A — полностью определенный детерминированный 2-ЭМ-автомат над (X, Y). На основе упомянутого замечания мы

можем предполагать, что A — алфавитный автомат. Пункт 3 замечания может быть уточнен: автомат A можно заменить объединением конечного числа последовательных соединений пар НРС-автоматов. А именно, для каждого состояния z автомата A можно определить следующие два НРС-автомата:

$A_1(z) = (Z, X, t_1, s, z)$, где $\tau_1 = pr_{1,2,4}(\tau)$;

$A_2(z) = (Z, Y, t_2, z, F)$, где $\tau_2 = pr_{1,3,4}(\tau)$.

Автомат A_i работает с i-й входной лентой. Пусть (u, v) — пара слов из $F(X) \times F(Y)$ и $z' = t^*(s, u, \Lambda)$. Слово u будет допускаться автоматом $A_1(z')$ и v — автоматом $A_2(z')$ тогда и только тогда, когда пара (u, v) будет допускаться автоматом A. Итак, выполняется равенство

$$L(A) = \cup\{L(A_1(z')) \times L(A_2(z')) \mid z' \in Z\}.$$

Таким образом, реакция каждого полностью определенного детерминированного 2-ЭМ-автомата оказывается конечным объединением декартовых произведений соответствующих пар рациональных множеств.

Поскольку из п.5 примера 8.6.8 следует, что декартово произведение двух рациональных множеств допускается соответствующим полностью определенным детерминированным 2-ЭМ-автоматом, и поскольку каждое конечное объединение таких декартовых произведений оказывается снова реакцией некоторого полностью определенного детерминированного 2-ЭМ-автомата (утверждение 1), то утверждение 2 теоремы доказано.

3. Пусть $R \in Rat(X)$ и $R' \in Rat(Y)$. Тогда $k(R \times R') = RR'$ — рациональное подмножество моноида $F(X \cup Y)$.

Далее очевидно, что $k(M \cup M') = k(M) \cup k(M')$ и что если множества $k(M)$ и $k(M')$ оба рациональны, то рационально и множество $k(M \cup M')$. Поэтому из утверждения 2 немедленно вытекает и утверждение 3 теоремы.

4. Если $k(L) \in Rat(X \cup Y)$, то $k(L) \subseteq X^*Y^*$ и существует РС-автомат A, допускающий множество $k(L)$. В доказательстве п.2 было показано, что автомат A можно заменить конечным числом последовательных соединений пар, состоящих из НРС-автомата над X и НРС-автомата над Y каждая. Поэтому $k(L)$ оказывается конечным объединением произведений вида RR' таких, что $R \in Rat(X)$ и $R' \in Rat(Y)$. Поскольку $k(R \times R') = RR'$ и для $M \subset R \times R'$ всегда выполнено $k(M) \subset RR'$, то утверждение 4 теперь немедленно вытекает из п.2. ∎

Следствие 8.6.10. 1. Каждое конечное подмножество произведения $F(X) \times F(Y)$ является реакцией некоторого полностью определенного детерминированного 2-ЭМ-автомата над (X, Y).

2. Произведение реакций двух полностью определенных детерминированных 2-ЭМ-автоматов над (X, Y) снова является реакцией некоторого полностью определенного детерминированного 2-ЭМ-автомата над (X, Y).

3. Назовем подмножество E произведения $F(X)\times F(Y)$ *различимым*, если существуют конечный моноид $(M, \circ)$ и гомоморфизм h из $(F(X)\times F(Y), \cdot)$ на $(M, \circ)$ такие, что $E=h^{-1}(h(E))$. Тогда для $L\subseteq F(X)\times F(Y)$ верно следующее высказывание: множество L различимо тогда и только тогда, когда L является реакцией некоторого полностью определенного детерминированного 2-ЭМ-автомата над (X, Y).

4. Порожденный реакцией некоторого полностью определенного детерминированного 2-ЭМ-автомата над (X, Y) подмоноид произведения $F(X)\times F(Y)$ не обязательно снова оказывается реакцией некоторого полностью определенного детерминированного 2-ЭМ-автомата.

5. Существуют алфавитные детерминированные 2-ЭМ-автоматы такие, что для них не существует эквивалентных полностью определенных детерминированных 2-ЭМ-автоматов.

6. Для каждого полностью определенного детерминированного 2-ЭМ-автомата можно построить эквивалентный 2-ЭЭШ-автомат. Обратное неверно.

Доказательство. Пункт 1 вследствие равенства $\{(u, v)\}=\{u\}\times\{v\}$ вытекает из п. 2 теоремы 8.6.9.

Пункт 2 равным образом вытекает из п.2 теоремы 8.6.9, поскольку выполняются равенства $(R_1\times R_2)\cdot(R_1'\times R_2')=R_1R_1'\times\times R_2R_2'$ и $(M\cup M')\cdot M''=M\cdot M''\cup M'\cdot M''$.

Пункт 3. 1) Так как для любого отображения f выполняются равенства $f(U_1\cup U_2)=f(U_1)\cup f(U_2)$ и $f^{-1}(V_1\cup V_2)=f^{-1}(V_1)\cup f^{-1}(V_2)$, то по теореме 8.6.9, п.2 нам достаточно лишь показать, что все декартовы произведения $R_1\times R_2$ при $R_1\in Rat(X)$ и $R_2\in Rat(Y)$ являются различимыми множествами. По теореме Клини—Майхилла (см. следствие 5.5.4) существуют конечные моноиды $(M_1, \circ)$ и $(M_2, \circ)$ и гомоморфизмы h_2 из F(X) на M_1 и h_2 из F(Y) на M_2 такие, что при $i=1,2$ выполнены равенства $R_i=h_i^{-1}(h_i(R_i))$. Тогда, как нетрудно убедиться, отображение

$$h: F(X)\times F(Y)\to M_1\times M_2 \text{ такое, что } h(u, v)=(h_1(u), h_2(v))$$

оказывается гомоморфизмом из $(F(X)\times F(Y), \circ)$ на прямое произведение моноидов $(M_1, \circ)$ и $(M_2, \circ)$ и выполняется равенство $R_1\times R_2=h^{-1}(h(R_1\times R_2))$, т. е. множество $R_1\times R_2$ различимо.

2) Пусть h — гомоморфизм из $(F(X)\times F(Y), \circ)$ на моноид $(M, \circ)$. Тогда $M_1=h(F(X)\times\Lambda)$ и $M_2=h(\Lambda\times F(Y))$ — подмоноиды моноида $(M, \circ)$ такие, что $M_1\circ M_2=M$. Далее, сужение h на $F(X)\times\Lambda$ [или h на $\Lambda\times F(Y)$] можно рассматривать как гомоморфизм h_1 (как h_2) из F(X) на $(M_1, \circ)$ [соответственно из F(Y) на $(M_2, \circ)$].

Если теперь E — различимое подмножество произведения $F(X)\times F(Y)$, то существует гомоморфизм h из $F(X)\times F(Y)$ на некоторый конечный моноид $(M, \circ)$ такой, что $E=h^{-1}(h(E))$. Поскольку в этом случае множество h(E) конечно, то E оказывается объединением конечного числа множеств вида $h^{-1}(m)$ при $m\in M$.

Из сказанного следует, что каждое m из M может быть запи-

сано (возможно, многими способами, но конечным их числом) в виде $m=m_1 \circ m_2$, где $m_i \in M_i$ при $i=1,2$. Итак, имеем

$$h^{-1}(m)=\{h^{-1}(m_1)\cdot h^{-1}(m_2) \mid m=m_1 \circ m_2\}=$$
$$=\{h_1^{-1}(m_1)\times h_2^{-1}(m_2) \mid m=m_1 \circ m_2\}.$$

Очевидно что каждое множество $h_i^{-1}(m_i)$ при $i=1,2$ является рациональным, так что E по теореме 8.6.9, п.2 оказывается реакцией некоторого полностью определенного детерминированного 2-ЭМ-автомата.

Пункт 4. Из п.1 доказательства следует, что множество $\{(0,1)\}$ является реакцией соответствующего полностью определенного детерминированного 2-ЭМ-автомата над $(\{0\}, \{1\})$ (см. также п.2 примера 8.6.8).

Порожденным множеством $\{(0,1)\}$ подмоноидом произведения $F(\{0\})\times F(\{1\})$ оказывается подмоноид $U_0=\{(0^n, 1^n) \mid n\in \mathbf{N}_0\}$.

По теореме 8.6.9, п.3 множество U_0 недопустимо никаким полностью определенным детерминированным 2-ЭМ-автоматом, поскольку множество $k(U_0)=\{0^n1^n \mid n\in \mathbf{N}_0\}$ по теореме 5.4.12 не является рациональным подмножеством моноида $F(\{0,1\})$.

Пункт 5 вытекает из доказательства п.4, так как множество U_0 допускается соответствующим алфавитным детерминированным 2-ЭМ-автоматом. Иным примером является множество из п.2 примера 8.5.2.

Пункт 6 вытекает непосредственно из следствия 8.5.4, п. 2 теоремы 8.6.9 и из только что проведенного доказательства п.5 теоремы. ■

Замечание. Если мы обозначим символом $Erk(X, Y)$ множество всех различимых подмножеств произведения $F(X)\times F(Y)$, то в отличие от случая $F(X)$ получим следующую иерархию: $Erk(X, Y)\subset$ {реакции 2-ЭЭШ-автоматов над (X, Y)}$\subset$ {реакции алфавитных детерминированных 2-ЭМ-автоматов над (X, Y)}$\subset$ $\subset Rat(X, Y)$.

8.7. ДВУЛЕНТОЧНЫЕ АВТОМАТЫ РАБИНА — СКОТТА

Поскольку вопрос о том, является ли данный 2-ЭМ-автомат детерминированным, неразрешим, представляется особенно интересным изучение специальных классов детерминированных 2-ЭМ-автоматов, для которых легко может быть решен вопрос о принадлежности им данных 2-ЭМ-автоматов. Один из них — класс функционирующих детерминированным образом 2-ЭЭШ-автоматов из разд. 8.5. Как и в этом случае, для определяемого ниже класса автоматов важную роль играет выбор лент при считывании, но только тогда, когда встречающиеся 2-ЭМ-автоматы оказываются локально детерминированными (в противном случае автоматы данного типа эквивалентны общим 2-ЭМ-автоматам).

Мы будем рассматривать алфавитные 2-ЭМ-автоматы, которые в каждом состоянии могут считывать символы только с одной из входных лент. При этом, однако (в отличие от случая 2-ЭЭШ-ав-

томатов), допускается произвольный порядок использования лент. Как и в случае 2-ЭЭШ-автоматов, мы разобьем множество состояний на два множества Z_1 и Z_2 и будем считать, что автомат, находящийся в любом состоянии из множества Z_i, может считывать информацию только с i-й ленты. При этом переходы таких автоматов можно записывать в виде троек (z, x, z'), которые в зависимости от того, принадлежит ли z множеству Z_1 или Z_2, понимаются как переходы (z, x, Λ, z') или (z, Λ, x, z') 2-ЭМ-автомата. Удобно также считать, что $X=Y$.

Определение 8.7.1. *Двуленточный автомат Рабина—Скотта* (коротко: 2-РС-автомат) *над X* есть шестерка

$A=(Z_1, Z_2, X, t, s, F)$, где $Z_1 \cap Z_2 = \varnothing$, такая, что $A'=(Z_1 \cup Z_2, X, t, s, F)$ — РС-автомат.

Способ функционирования автомата A определяется тем, что A работает как 2-ЭМ-автомат $A''=(Z_1 \cup Z_2, X, X, t'', s, F)$,

где $\tau''=\{(z_1, x, \Lambda, z') \mid (z_1, x, z') \in \tau, z_1 \in Z_1\} \cup$

$\cup \{(z_2, \Lambda, x, z'') \mid (z_2, x, z'') \in \tau, z_2 \in Z_2\}$.

Реакция автомата A, обозначаемая $L(A)$, равна реакции автомата $A'': L(A)=L(A'')$. Если A оказывается ДРС-автоматом, то A называется *частично определенным 2-РС-автоматом.* Заменяя A′ на НРС-автомат, получаем определение *недетерминированного 2-РС-автомата.*

Пример 8.7.2. 1. Автомат $A=(Z_1, Z_2, X, t, s, z)$, где $Z_1=\{s, z\}$, $Z_2=\{z_x \mid x \in X\}$ и $\tau=\cup\{\{(s, x, z_x), (z_x, x, z), (z, x, z_x\} \mid x \in X\}$, есть 2-РС-автомат с реакцией $L(A)=\{(w, w) \mid w \in F^+(X)\}$.

2. Множества U и V из доказательства теоремы 8.4.11 являются реакциями 2-РС-автоматов над $\{0,1\}$; на рис. 8.7.1 изображен граф 2-РС-автомата A, допускающего множество U. Совершенно аналогично строится 2-РС-автомат с реакцией V.

На базе определения возникают две возможности для представления автомата A с помощью графа:

а) строится граф РС-автомата A′ из определения 8.7.1, и для каждой вершины (состояния) с помощью метки $i \in \{1,2\}$ указывается, принадлежит ли это состояние множеству Z_1 (при $i=1$) или множеству Z_2 (при $i=2$);

б) строится граф 2-ЭМ-автомата A″ из определения 8.7.1.

На рис. 8.7.1 приведен граф, полученный по способу а).

3. Как и в случае ДРС-автоматов, когда с помощью добавления единственного нового состояния удавалось провести доопределение, для частично определенного 2-РС-автомата можно построить эквивалентный 2-РС-автомат: пусть A — частично определенный 2-РС-автомат и $0 \notin Z_1 \cup Z_2$; тогда $A_0=(Z_1 \cup 0, Z_2, X, t_0, s, F)$, где $\tau_0=\tau \cup \{(z, x, 0) \mid t(z, x)=\varnothing\} \cup 0 \times X \times 0$, есть 2-РС-автомат такой, что $L(A_0)=L(A)$.

Итак, в дальнейших примерах нам нужно задавать только частично определенные 2-РС-автоматы с требуемыми реакциями.

На рис. 8.6.2 изображен, например, граф (полученный по способу б) из п. 2) частично определенного 2-РС-автомата, допуска-

ющего множество W из доказательства следствия 8.5.4, так что это множество W оказывается реакцией некоторого 2-РС-автомата.

Если из графа, изображенного на рис. 8.6.2, исключить начальное состояние и цикл с меткой $(\Lambda, 0)$ у состояния z_1 и сделать состояние z_1 начальным, то получится граф частично определенного 2-РС-автомата с реакцией $\{(0^k1^m, 1^k) \mid k, m \in \mathbf{N}\}$.

Если теперь исключить и финальное состояние и сделать состояние z_3 финальным, то получится граф частично определенного 2-РС-автомата с реакцией $\{(0^k, 1^k) \mid k \in \mathbf{N}\}$.

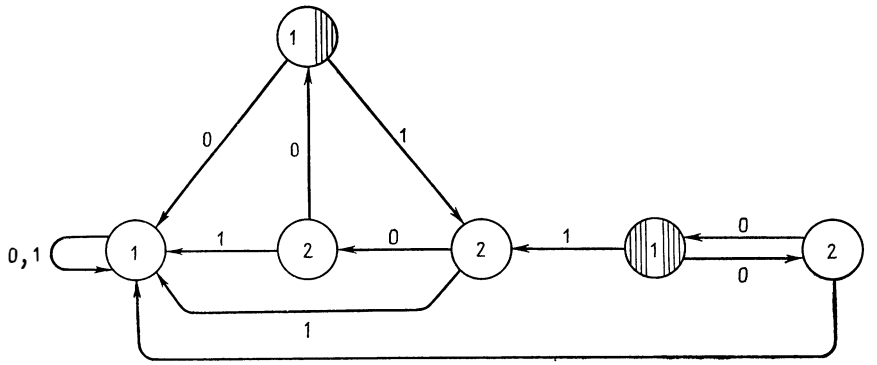


Рис. 8.7.1. 2-РС-автомат с реакцией U

4. Пусть E — префиксный код над X, т. е. подмножество полугруппы $F^+(X)$ со свойством $E \cap EF^+(X) = \varnothing$ (т. е. ни один собственный префикс ни одного слова из E не принадлежит E) — см. упражнение 4.5. Пусть, кроме того, допускается, что $E = \{\Lambda\}$.

Пусть, далее, A_E—D-минимальный ДРС-автомат с реакцией E и z — финальное состояние этого автомата. Тогда, находясь в состоянии z, автомат A_E не может больше считывать никакие знаки с входной ленты. Действительно, в противном случае вследствие D-минимальности автомат A_E должен был бы при считывании некоторой непустой последовательности знаков переходить из состояния z в некоторое финальное же состояние z', так что в состоянии z допускался бы некоторый префикс слова, допускаемого в состоянии z', что противоречит предположению о множестве E.

Допустим теперь, что R — произвольное рациональное подмножество моноида F(X) и A_R — допускающий это множество РС-автомат. Тогда можно построить 2-РС-автомат A с реакцией $L(A) = E \times R$: A_E считывает первую ленту; к каждому финальному состоянию z автомата A_E присоединяется автомат A_R, причем его начальным состоянием считается z; автомат A_R считывает вторую ленту. Итак, пусть $A = (Z_E - F_E, (Z_R - s_R) \cup F_E, X, t, s_E, F_R)$ с $\tau = \tau_E \cup (\tau_R \cap (Z_R - s_R) \times X \times (Z_R - s_R)) \cup \{(z, x, z') \mid (s_R, x, z') \in \tau_R, z \in F_E\} \cup \{(z, x, z_0) \mid (z, x, s_R) \in \tau_R\}$, где z_0 — произвольным образом

выбранное финальное состояние автомата A_E (здесь считается, что $Z_R \cap Z_E = \varnothing$).

Если в описанной конструкции поменять местами ленты, т. е. заставить A_E считывать вторую, а A_R — первую ленту, то будет получен 2-РС-автомат с реакцией $R \times E$.

Кроме того, ясно, что A_R можно рассматривать и как 2-РС-автомат с реакцией $R \times \Lambda$, и как 2-РС-автомат с реакцией $\Lambda \times R$.

5. Для каждого алфавитного 2-ЭМ-автомата A над (X, X) описываемым ниже способом можно построить недетерминированный 2-РС-автомат A′, с той же реакцией. Пусть z_1 — некоторое состояние автомата A, в котором он может считывать входы с обеих лент. Если у A таких состояний нет, то он уже является недетерминированным 2-РС-автоматом. В противном случае добавим к состоянию z_1 состояние z_2 так, чтобы возник 2-ЭМ-автомат A_1, который в состоянии z_i при $i = 1,2$ считывает вход только с i-й ленты. Для этого все исходящие из вершины z_1 ребра в графе автомата A, помеченные парами вида (Λ, y) при $y \in Y$, проведем из z_2 и все ведущие в z_1 ребра проведем также в z_2. Итак, пусть $A_1 = (Z \cup z_2, X, X, t_1, S_1, F)$, где

$$S_1 = \begin{cases} S \cup z_2, \text{ если } z_1 \in S, \\ S \text{ в противном случае;} \end{cases}$$

$$\tau_1 = \tau - (\tau \cap z_1 \times \Lambda \times X \times Z) \cup \{(z_2, \Lambda, y, z') \mid (z_1, \Lambda, y, z') \in \tau\} \cup \{(z', x, y, z_2) \mid (z', x, y, z_1) \in \tau\}.$$

Очевидно, что $L(A_1) = L(A)$ и что число состояний, в которых возможно считывание с обеих лент, у A_1 на одно меньше, чем у A.

Теперь снова применим описанную конструкцию к A_1 вместо A. Поскольку множество Z конечно, то после конечного числа шагов будет получен искомый 2-РС-автомат.

Замечание. Из определения 8.7.1 вытекает, что 2-РС-автоматы можно рассматривать как алфавитные 2-ЭМ-автоматы, так что для их реакций выполняются необходимые условия из пп. 1 и 3 следствия 8.4.4 и из теоремы 8.4.7. В отличие от случая детерминированных 2-ЭМ-автоматов (см. теорему 8.6.3) тривиальным образом разрешим вопрос о том, является ли данный 2-ЭМ-автомат 2-РС-автоматом. В то же время вопрос о том, существует ли для данного 2-ЭМ-автомата эквивалентный 2-РС-автомат, неразрешим — см. упражнение 8.11, п. 5.

Приведенная ниже теорема дает очень полезный критерий того, что данное множество не является реакцией никакого 2-РС-автомата. Она показывает, что 2-РС-автоматы обладают свойствами, весьма отличными от свойств 2-ЭМ-автоматов.

Теорема 8.7.3. 1. 2-ЭМ-автомат A″, соответствующий по определению 8.7.1 некоторому 2-РС-автомату A, является алфавитным детерминированным 2-ЭМ-автоматом, однако не для каждого алфавитного 2-ЭМ-автомата существует эквивалентный 2-РС-автомат.

2. Пусть A — 2-РС-автомат над X и u, v, u′ и v′ — слова из $F(X)$. Из включения $\{(u, vv'), (uu', v)\} \subseteq L(A)$ вытекает тогда, что $u' = \Lambda$ или $v' = \Lambda$.

3. Множество всех реакций 2-РС-автоматов над X не замкнуто ни относительно булевых операций, ни относительно операций произведения и образования подмоноида. Оно содержит не все конечные подмножества множества $F(X)^2$ и не содержит множеств вида $F(X)^2 - E$, где E — конечное подмножество множества $F(X)^2$.

4. Множества реакций 2-РС-автоматов над X и полностью определенных детерминированных 2-ЭМ-автоматов (или 2-ЭЭШ-автоматов над (X, X) не сравнимы, т. е. ни одно из этих множеств не содержит другое и их пересечение не пусто.

5. Вопрос о дизъюнктности реакций двух 2-РС-автоматов неразрешим.

Доказательство. 1. При $u=v=\Lambda$ и $u'=v'=0$ из п.2 немедленно вытекает, что множество $\{(\Lambda, 0), (0, \Lambda)\}$ не является реакцией никакого 2-РС-автомата. Это же множество, конечно, — реакция некоторого алфавитного детерминированного 2-ЭМ-автомата.

Пусть теперь A — 2-РС-автомат и A″ — соответствующий ему 2-ЭМ-автомат. Необходимо для каждого состояния z автомата A и каждой пары (u, v) из $F(X)^2$ таких, что $t''^*(z, u, v) \neq \varnothing$, показать, что $|t''^*(z, u, v)| = 1$. Мы сделаем это для произвольного, но фиксированного z полной индукцией по $|uv|$.

Если $|uv|=0$, т. е. $u=v=\Lambda$, то из определения 2-РС-автомата следует, что $t''^*(z, u, v) = t''(z, \Lambda, \Lambda) = z$.

Если $|uv|=1$, то либо $u \in X$ и $v=\Lambda$, либо $u=\Lambda$ и $v \in X$. В обоих случаях по определению 2-РС-автомата $|t''^*(z, u, v)| = |t''(z, u, v)| \leqslant 1$.

Предположим теперь, что утверждение выполнено для всех пар (u, v) из $F(X)^2$ таких, что $|uv| \leqslant r$, и что (u′, v′) — пара из $F(X)^2$ такая, что $|u'v'| = r+1$ и $t''^*(z, u', v') \neq \varnothing$.

Мы рассмотрим только случай, когда $(u', v') = (ux, v')$ при $x \in X$ и $|uv'| = r$. Случай $(u', v') = (u', vx)$, $x \in X$ разбирается аналогично.

Поскольку автомат A алфавитный, то из соотношения $t''^*(z, u', v') \neq \varnothing$ вытекает существование такого состояния, что автомат находится в нем после считывания слова u с первой ленты. Иначе говоря, отсюда вытекает существование префикса w слова v′ такого, что $t''^*(z, u, w) \neq \varnothing$.

Пусть w′ — префикс максимальной длины слова v′ такой, что $t''^*(z, u, w') \neq \varnothing$. По предположению индукции в этом случае имеем $|t''^*(z, u, w')| = 1$.

Пусть $z' = t''^*(z, u, w')$.

Если бы выполнялось включение $z' \in Z_2$, то по определению 2-РС-автомата должно бы было существовать x в X такое, что слово w′x было бы префиксом слова v′ и были бы верны соотношения $\varnothing \neq t''(z', \Lambda, x) = t''^*(z, u, w'x)$, так как по предположению индукции $|t''^*(z, u, w'x)| = 1$. Это противоречит, однако, максимальности слова w′. Итак, $z' \in Z_1$.

Для любого префикса $\bar{w}$ слова w' такого, что $\bar{w}\neq w'$ и $t''^*(z, u, \bar{w})\neq\varnothing$, по предположению индукции выполнены равенство $t''^*(z, u, \bar{w})|=1$ и включение $\bar{z}=t''^*(z, u, \bar{w})\in Z_2$, поскольку в противном случае состояние z' не могло бы быть достигнуто из состояния $\bar{z}$ при считывании остающейся части слова w'.

Пусть теперь $v'=w'w''$ и $z''=t''(z', x, \Lambda)$. Тогда $t''^*(z, u' v')=$ $=t''^*(z, ux, v')=t''^*(t''(t''^*(z, u, w'), x, \Lambda), \Lambda, w'')=t''^*(z'', \Lambda, w'')$, а это множество по определению 2-РС-автомата одноэлементно, поскольку оно возникает при считывании автоматом, находящимся в состоянии z'', только символов со второй ленты. Таким образом, в данном случае 2-ЭМ-автомат A'' работает как РС-автомат A' из определения 8.7.1, т. е. $t''^*(z'', \Lambda, w'')=t^*(z'', w)$.

Тем самым п.1 теоремы доказан.

2. Пусть A и A'' заданы, как в определении 8.7.1, и u, v, u' и v' — слова из $F(X)$ такие, что

$$\{(u, vv'), (uu', v)\}\subseteq L(A).$$

Предположим, что $u'\neq\Lambda$, т. е., что $u'=xu''$ при $x\in X$. По соображениям, приведенным во второй части доказательства утверждения 1, из включения $(uu', v)\in L(A)$ вытекает существование слов w и w' в $F(X)$ и состояния z в Z_1 таких, что $t''^*(s, u, w)=z$, $t''(z, x, \Lambda)=t''^*(s, ux, w)$ и $ww'=v$.

Из включения $(u, vv')\in L(A)$ должно на основе второй части доказательства утверждения 1 следовать, что $t''^*(s, u, vv')=$ $=t''^*(t''^*(s, u, w), \Lambda, w', v')=t''^*(z, \Lambda, w', v')$, но это невозможно, так как $z\in Z_1$. Отсюда вытекает, что $w'v'=\Lambda$, так что $v'=\Lambda$.

Аналогичным образом доказывается, что из $v'\neq\Lambda$ вытекает $u'=\Lambda$.

3. То, что не каждое конечное подмножество множества $F(X)^1$ является реакцией некоторого 2-РС-автомата, мы уже показали в п.1 доказательства.

Из п.2 примера 8.7.2 и доказательства теоремы 8.4.11 вытекает незамкнутость относительно операции пересечения.

Реакции обоих подавтоматов на рис. 8.6.3 являются реакциями 2-РС-автоматов. Объединение же этих реакций, как следует из теоремы 8.6.6 и п.1 данной теоремы, таковым не является.

Пусть E — конечное (или пустое) подмножество множества $F(X)^2$, $k=\max\{\max(|w|, |w'|)\,|\,(w, w')\in E\}$ и $(u, v)\in F(X)^2$, причем $|u|>k$ и $|v|>k$.

Тогда $\{(u, vv'), (uu', v)\}\subseteq F(X)^2-E$ при $u'=v'=x$, где $x\in X$.

Из утверждения 2 поэтому получаем, что множество $F(X)^2-E$ не может быть реакцией никакого 2-РС-автомата.

Поскольку, очевидно, имеются конечные множества, являющиеся реакциями 2-РС-автоматов, то из сказанного сразу вытекает незамкнутость относительно операции дополнения.

Из п.4 примера 8.7.2 следует, что $\Lambda\times F(X)$ и $F(X)\times\Lambda$ — реакции соответствующих 2-РС-автоматов. Из доказанного выше, однако, получаем, что их произведение $F(X)^2=\Lambda\times F(X))\cdot(F(X)\times$

$\times\Lambda$) не является реакцией никакого 2-РС-автомата:

$A=(s, \{z_2, z_2'\}, X, t, s, \{s, z_2, z_2'\})$,

где $\tau=s\times X\times z_2\cup z_2\times X\times z_2'$, — частично определенный 2-РС-автомат над X с реакцией $L(A)=(X\cup\Lambda)^2$. Как следует из п.3 примера 8.7.2, тогда существует также и 2-РС-автомат с той же реакцией. Порожденный же множеством $(X\cup\Lambda)^2$ подмоноид моноида $F(X)^2$ не является допустимым для какого-либо 2-РС-автомата множеством $F(X)^2$ (см. выше).

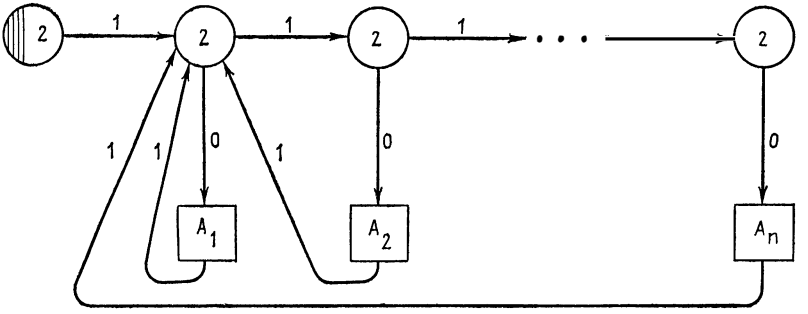


Рис. 8.7.2. 2-РС-автомат $A(W_n)$

Утверждение 4 с учетом следствия 8.6.10 (соответственно следствия 8.5.4) непосредственно получаем из п.3.

5) Для доказательства мы используем неразрешимость общей проблемы соответствий Поста (см. лемму 8.3.5).

Пусть $W_n=\{w_1, w_2, ..., w_n\}\subseteq F(X)$ с $X=\{0, 1\}$. Мы опишем ниже способ построения 2-РС-автомата $A(W_n)$ с реакцией:

$$L(A(W_n))=\{(w_{i_1}w_{i_2}\dots w_{i_p}, 1^{i_1}01^{i_2}0\dots 1^{i_p}0)\mid p\in\mathbf{N}, 1\leqslant i_j\leqslant n \text{ при } 1\leqslant j\leqslant p\}.$$

Пусть A_i — очевидным образом легко задаваемый РС-автомат с единственным финальным состоянием и реакцией $\{w_i\}$.

2-РС-автомат $A(W_n)$ считывает сначала символы с второй ленты. Прочитав на ней слово 1^i0 при $1\leqslant i\leqslant n$, он переходит к считыванию первой ленты, используя для этого автомат A_i. Если автомат A_i переходит в финальное состояние, то $A(W_n)$ снова переходит к считыванию второй ленты. Если он обнаруживает на этой ленте символ 1, то он переходит в состояние, в которое он переходил из начального состояния при прочтении первого символа 1. Автомат $A(W_n)$ имеет вид, показанный на рис. 8.7.2.

Итак, пусть $A_i=(Z_{1i}\cup z_{2i}, X, t_i, s_i, z_{2i})$ — РС-автомат, где $z_{2i}\notin Z_{1i}$ и $L(A_i)=w_i$ при $i=1, ..., n$. Пусть, далее, $Z_0=\{z_{0j}\mid j=0, 1, ..., n\}$, где $Z_0\cap(Z_{1i}\cup z_{2i})=\varnothing$ и $(Z_{1i}\cup z_{2i})\cap(Z_{1j}\cup z_{2j})=\varnothing$ при $1\leqslant j<i\leqslant n$.

Тогда

$$A(W_n)=(Z_{11}\cup\dots\cup Z_{1n}, Z_0\cup\{z_{21}, z_{22}, ..., z_{2n}\}, X, t, z_{00}, \{z_{21}, ..., z_{2n}\}),$$

где $\tau = \{(z_{0j}, 1, z_{0,j+1}) \mid j = 0, \ldots, n-1\} \cup \tau_1 \cup \tau_2 \cup \ldots \cup \tau_n \cup \{(z_{0i}, 0, s_i) \mid i = 1, \ldots, n\} \cup \{z_{2i}, 1, z_{01}) \mid i = 1, \ldots, n\}$,
есть частично определенный 2-РС-автомат с искомой реакцией.

Как следует из п.3 примера 8.7.2 существует и требуемый 2-РС-автомат $A(W_n)$.

Пусть теперь Q — случай проблемы соответствий Поста над X (как в определении 8.3.4). Положим $U_n = \{u_1, u_2, \ldots, u_n\}$ и $V_n = \{v_1, v_2, \ldots, v_n\}$.

Тогда можно, как только что было показано, построить 2-РС-автоматы $A(U_n)$ и $A(V_n)$. Очевидно, что соотношение $L(A(U_n)) \cap L(A(V_n)) = \varnothing$ верно тогда и только тогда, когда Q не имеет решения. ■

Другие варианты 2-ЭМ-автоматов описаны в упражнении 8.12.

8.8. ОБОБЩЕНИЯ

Содержание предыдущих разделов может быть обобщено двумя способами: вместо двух можно рассматривать $n \geqslant 2$ входных лент и вместо моноида $(F(X) \times F(Y), \cdot)$ можно рассматривать произвольные моноиды.

МНОГОЛЕНТОЧНЫЕ АВТОМАТЫ

Легко видеть, что определения из разд. 8.5—8.7 допускают непосредственное обобщение на случай, когда рассматриваются автоматы с n входными лентами ($n \in \mathbf{N}$). Тогда имеется n входных алфавитов $X_1, \ldots, X_n$ и исследуются подмножества прямого произведения $(F(X_1) \times \ldots \times F(X_n), \cdot)$. На этот моноид легко перенести и понятия рационального и различимого подмножества. В определении n-ЭЭШ-автоматов нужно требовать, чтобы автомат одновременно считывал по одному символу с каждой из лент, на которой он еще не дошел до конца слова. В случае n-РС-автоматов множество состояний должно разделяться на n дизъюнктных подмножеств.

Сразу видно, что все результаты из разд. 8.5—8.7 можно без сложностей распространить на случай n-ЭМ-автоматов соответствующих типов. Кроме того, имеется, например, следующий факт.

Пусть $\overline{pr}_i$ обозначает операцию проектирования произведения $F(X_1) \times \ldots \times F(X_n)$ на $F(X_1) \times \ldots \times F(X_{i-1}) \times F(X_{i+1}) \times \ldots \times F(X_n)$ $(1 \leqslant i \leqslant n)$, соответствующую отбрасыванию i-й компоненты. Если L — реакция некоторого n-ЭМ-автомата (или n-ЭЭШ-автомата) над $(X_1, \ldots, X_n)$, то $\overline{pr}_i(L)$ является реакцией некоторого $(n-1)$-ЭМ-автомата (соответственно — n-ЭЭШ-автомата) над $(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n)$ и $\overline{pr}^{-1}{}_{n+1}(L) = L \times F(X_{n+1})$ — реакцией некоторого $(n+1)$-ЭВМ-автомата (соответственно — $(n+1)$-ЭЭШ-автомата) над $(X_1, \ldots, X_{n+1})$.

Отметим, далее, что каждый алфавитный n-ЭМ-автомат над $(X_1, \ldots, X_n)$ может также рассматриваться как n-ЭМ-автомат над

$(X_{i_1},\ldots, X_{i_n})$, где $i_1, \ldots, i_n$ — некоторая перестановка индексов $1, \ldots, n$, и как 2-ЭМ-автомат над (Y, X_n), где $Y = (X_1 \cup \Lambda) \times \ldots \times (X_{n-1} \cup \Lambda)$.

Некоторый n-ЭМ-автомат A при $n \geqslant 3$ можно еще большим числом способов, чем 2-ЭМ-автоматы, использовать для определения допустимых слов. Кроме обработки слова w в виде $(w, w, \ldots, w)$ здесь возникают следующие возможности. Слово w разлагается на n подслов $w = w_1 w_2 \ldots w_n$. Пусть для каждого $i = 1, \ldots, n$ f_i либо тождественное, либо зеркальное отображение. Тогда слово w считается допустимым, если набор $(f_1(w_1), \ldots, f_n(w_n))$ допускается автоматом A.

Поскольку описанный процесс разложения слова на подслова порождает дополнительную недетерминированность, то можно, например, требовать, чтобы все подслова имели одинаковую длину (или чтобы соотносились определенным образом).

АВТОМАТЫ НАД МОНОИДАМИ

Пусть $(M, \circ)$ — произвольный моноид. Тогда можно ввести понятия рационального и различимого множеств точно так же, как в случае моноидов $F(X)$ и $(F(X) \times F(Y), \cdot)$.

В дальнейшем мы вместо $(M, \circ)$ будем писать M, так как ясно, о какой операции идет речь.

Определение 8.8.1. 1. Множество $\mathrm{Rat}(M)$ *рациональных подмножеств* моноида M есть наименьшее подмножество $\mathscr{R}$ булеана $\mathscr{P}(M)$, удовлетворяющее следующим условиям:

1) $\varnothing \in \mathscr{R}$ и $\{m\} \in \mathscr{R}$ при любом m из M;

2) если U и V — элементы $\mathscr{R}$, то $\mathscr{R}$ содержит также и $U \cup V$ и $U \circ V = \{u \circ v \mid u \in U, v \in V\}$;

3) вместе с U множество $\mathscr{R}$ содержит и порожденный множеством U подмоноид U^* моноида M: $U^* = U^0 \cup U^1 \cup \ldots \cup U^i \cup \ldots$, где $U^0 = \{e\}$, e — единичный элемент моноида M, и $U^{i+1} = U^i \circ U$ при всех i из **N**.

2. Подмножество E моноида M называется *различимым*, если существует гомоморфизм h из M на некоторый конечный моноид такой, что $E = h^{-1}(h(E))$.

Символом $\mathrm{Erk}(M)$ обозначается множество всех различимых подмножеств моноида M.

Из разд. 8.4 и 8.6 мы уже знаем, что, вообще говоря, $\mathrm{Rat}(M) \neq \mathrm{Erk}(M)$, что $\mathrm{Rat}(M)$ не замкнуто относительно операций пересечения и дополнения и что $\mathrm{Erk}(M)$ не замкнуто относительно операции образования подмоноида. То, что множество $\mathrm{Erk}(M)$ также, вообще говоря, не замкнуто относительно операции произведения, показывает следующий пример.

Пример 8.8.2. Пусть M — коммутативный аддитивный моноид, возникающий из коммутативного аддитивного моноида Z целых чисел при присоединении к нему элементов e и a со следующими законами сложения: $a + a = 0$, $e + m = m + e = m$ для всех m из M, $a + z = z + a = z$ для всех z из **Z**.

Пусть, далее, $\bar{M}$ — гомоморфный образ моноида M при отображении $\bar{h}$, определенном соотношениями $\bar{h}(e)=\bar{e}$, $\bar{h}(a)=\bar{a}$ и $h(z)=\bar{0}$ для всех z из **Z**.

Тогда {a} оказывается различимым подмножеством моноида M и выполняется равенство $\{a\}+\{a\}=\{0\}$.

Допустим, что {0} — различимое подмножество моноида M. Тогда должны существовать конечный моноид M′ и гомоморфизм h из M на M′ такие, что $\{0\}=h^{-1}(h(0))$. В этом случае должно существовать и число $z\geqslant|M'|$ такое, что $h(z)=h(0)$, поскольку не все элементы h(1), h(2), ... могут быть различны, а из $h(i)=h(j)$ (при $i>j$) следует, что $h(i-j)=h(0)$. Следовательно, в этом случае и z принадлежит $h^{-1}(h(0))$, так что наше предположение ложно.

Теперь, естественно, возникает вопрос, могут ли быть обобщены на случай произвольных моноидов понятия 2-ЭМ-автоматов, детерминированных 2-ЭМ-автоматов, полностью определенных детерминированных 2-ЭМ-автоматов и высказывания из разд. 8.4 и 8.6.

Определение 8.8.3. *Автоматом Уоляспера* (коротко: У-автоматом) называется пятерка $A=(Z, X, t, S, F)$, где X — конечное подмножество моноида M и (Z, X, t, S, F) может рассматриваться как побуквенный НРС-автомат A_F над F(X) в смысле определения 5.2.1, причем операция в M не принимается во внимание, т. е. где Z — конечное множество, $S, F\subseteq Z$ и $t=(Z\times X, Z, \tau)$ — соответствие с графиком $\tau\subseteq Z\times X\times Z$.

Автомат A называется *локально детерминированным* (или *слабо определенным),* если автомат A_F детерминирован (соответственно — полностью определен)в смысле определения 5.4.1, т. е. если t является частичным отображением и $|S|=1$ (соответственно — если t является всюду определенным отображением).

Автомат A_F называется *фундаментальным* для A НРС-автоматом.

Последовательностное соответствие t^* определяется в два этапа.

1. Пусть t_F^* — последовательностное соответствие автомата A_F, т. е. пусть $\tau_F{}^0=\{(z, \Lambda, z)\,|\,z\in Z\}$, $\tau_F{}^1=\tau$ и при $i\in\mathbf{N}$

$\tau_F{}^{i+1}=\{(z, wx, z')\,|$ существует $z''\in Z$ такое, что $(z, w, z'')\in\tau^1$ и $(z'', x, z')\in\tau\}$;

тогда $\tau_F{}^*=\bigcup\{\tau_1{}^i\,|\,i\in N_0\}$ и $t_F{}^*=(Z\times F(X), Z, \tau_F{}^*)$.

2. $t^*(z, m)=\bigcup\{t_F{}^*(z, x_1, \ldots, x_n)\,|\,x_1\circ x_2\circ\ldots\circ x_n=m,\ n\in\mathbf{N},\ x_i\in X$ при $i=1, \ldots, n\}$ для всех z из Z и всех m из M.

Реакцией автомата A называется множество

$L(A)=\{m\in M\,|\,t^*(S, m)\cap F\neq\varnothing\}$.

Автомат A называется *детерминированным У-автоматом*, если $|S|=1$ и t^* является частичным отображением.

Автомат A называется *сильно детерминированным У-автоматом,* если A является детерминированным У-автоматом и X — базис подмоноида X^* моноида M, т. е. если для $Y\subseteq X$ из $Y^*=X^*$ следует, что $Y=X$.

Автомат A называется *полностью определенным детерминированным У-автоматом,* если A — слабо определенный детерминированный У-автомат и X — порождающая система для M, т. е. если $X^* = M$.

Автомат A называется мультипликативным У-автоматом, если для всех $z \in Z$ и всех $m, m' \in M$ выполнено условие $t^*(t^*(z, m), m') = t^*(z, m \circ m')$.

Множество всех реакций У-автоматов будем обозначать WA(M), всех реакций детерминированных У-автоматов — DWA(M), всех реакций полностью определенных детерминированных У-автоматов — VDWA(M) и всех реакций мультипликативных У-автоматов — MWA(M).

Замечания. 1. Сильно детерминированный У-автомат над F(X) [над $F(X) \times F(Y)$] является ДРС-автоматом (алфавитным детерминированным 2-ЭМ-автоматом).

2. Не являющийся алфавитным НРС-автомат может не быть мультипликативным — см. п.2) замечаний к определению 5.2.2.

Многие результаты из предыдущих разделов могут быть в основном перенесены на У-автоматы и на определенные выше специальные классы таких автоматов. Мы ограничимся здесь следующей теоремой.

Теорема 8.8.4 (Уоляспер). Пусть M — конечно-порожденный моноид. Тогда $\mathrm{Erk}(M) = \mathrm{VDWA}(M) = \mathrm{MWA}(M) \subseteq \mathrm{WA}(M) = \mathrm{Rat}(M)$.

Если, кроме того, M имеет базис, то

$\mathrm{Erk}(M) \subseteq \mathrm{SDWA}(M) \subseteq \mathrm{Rat}(M)$ [1].

Существует моноид M, для которого включения строгие.

Набросок доказательства. Очевидно, что каждый полностью определенный детерминированный У-автомат является мультипликативным. Для мультипликативного У-автомата соответствия t_m^* из Z в себя (определенные равенством $t_m^*(z) = t_m^*(z, m)$) образуют моноид (моноид переходов). Как и в доказательстве теоремы 5.4.4, можно показать, что подмножество моноида M различимо тогда и только тогда, когда оно является реакцией некоторого мультипликативного У-автомата над M.

Равенство $\mathrm{Rat}(M) = \mathrm{WA}(M)$, как и в теореме 8.4.10, немедленно вытекает из того, что для естественного гомоморфизма $\nu_{X,M}$ из F(X) в M, определенного вложением X в M, выполняется следующее.

1) $\nu_{X,M}(L(A_F)) = L(A)$ — для любого У-автомата A с входным множеством X;

2) $\mathrm{Rat}(X^*) = \nu_{X,M}(\mathrm{Rat}(X))$, где X^* рассматривается как (под)моноид (моноида M).

Если у M имеется конечная порождающая система X, то $\mathrm{Rat}(X^*) = \mathrm{Rat}(M)$, так что Rat(M) оказывается множеством всех

---

[1] SDWA(M) — множество реакций сильно детерминированных У-автоматов.— *Прим. перев.*

реакций У-автоматов с входным множеством X и покрывает поэтому множество Erk(X).

Если X оказывается даже базисом моноида M, то любой полностью определенный детерминированный У-автомат с входным множеством X оказывается и сильно детерминированным У-автоматом.

Приведенные в условии включения оказываются, в частности, строгими, если рассматривается случай $M=F(X)\times F(Y)$. ■

Замечание. Если моноид M не является конечно-порожденным, то, хотя и выполняется включение $M\in Erk(M)$, но не существует полностью определенных детерминированных У-автоматов над M и неверно, что $M\in Rat(M)$.

Опишем, наконец, метод, с помощью которого можно получить отличную от конкатенации операцию над множеством слов в некотором алфавите X, т. е. можно построить моноид, отличный от свободного моноида F(X).

Пример 8.8.5. Пусть X — конечное множество. Символом W(X) обозначим множество всех слов над X, т. е. множество всех элементов моноида F(X).

1. *У-отображением* относительно X называется отображение f из W(X) в себя со следующими свойствами.

1) Для каждого $w\in W(X)$ слово $f(w)$ является кусочным подсловом слова w и $\bar{f}(w)$ — остатком от слова w, получающимся при исключении входящих в $f(w)$ подслов. При этом $f(\bar{f}(w))=\Lambda$. Иначе говоря, для любого слова w из W(X) существует разложение $w=u_1v_1u_2v_2\ldots u_nv_n$ с $u_i, v_i\in W(X)$ такое, что $f(w)=u_1u_2\ldots u_n$, $\bar{f}(w)=v_1v_2\ldots v_n$ и $f(v_1v_2\ldots v_n)=\Lambda$.

2) Для каждой пары слов u, v из $W(X)-\Lambda$ такой, что $f(v)=\Lambda$, существует единственное слово w в W(X) такое, что $f(w)=u$ и $\bar{f}(w)=v$.

Из 1) и 2) для всех w и w′ из w(x) следует, что если $w\neq w'$ и $f(w)=f(w')$, то $\bar{f}(w)\neq\bar{f}(w')$.

Примером У-отображения является отображение f_m, определяемое равенствами $f_m(x_1\ldots x_{2n-1})=\bar{f}_m(x_1\ldots x_{2n})=x_n$, где все x_i принадлежат X.

В этом случае $f_m(x)=\Lambda$ и $f_m(xy)=y$ для $x, y\in X$.

2. УШ-операция[1] $\circ_f$ над W(X) определяется следующим образом. Пусть для u и v из W(X)

$$u\circ_f v=\begin{cases} u, \text{ если } f(v)=v;\\ w, \text{ где } w \text{ — слово из } W(X), \text{ для которого}\\ f(w)=u \text{ и } \bar{f}(w)=v, \text{ если } f(v)=\Lambda;\\ (u\circ_f f(v))\circ_f\bar{f}(v), \text{ если } \Lambda\neq f(v) \text{ и } f(v)\neq v.\end{cases}$$

Нетрудно видеть, что операция $\circ_f$ определена корректно.

[1] УШ — начальные буквы фамилий Уоляспера и Шнорра, см. обзор литературы. — *Прим. перев.*

Действительно, для случая $f(v)=v$ или $f(v)=\Lambda$ значение $u\circ_f v$ определено однозначно, а поскольку из неравенств $f(v)\neq\Lambda$ и $f(v)\neq v$ следует, что $|f(v)|<|v|$ и $|\bar{f}(v)|<|v|$, то утверждение о корректности возникает при использовании полной индукции по длине второго операнда.

Так как $f(\Lambda)=\Lambda$, то Λ оказывается единичным элементом относительно $\circ_f$.

Ассоциативность операции $\circ_f$ может быть доказана полной индукцией по длине самого правого операнда.

Пусть u, v и v′ — слова из $W(X)-\Lambda$.

Если $f(v')=v'$, то $(u\circ_f v)\circ_f v'=u\circ_f v=u\circ_f(v\circ_f v')$.

Если $f(v')=\Lambda$, то $v\circ_f v'=w'$, где $f(w')=v$ и $\bar{f}(w')=v'$. Если бы выполнялось равенство $f(w')=w'$, то было бы выполнено и $\Lambda=\bar{f}(w')=v'$. Поэтому имеем $f(w')\neq\Lambda$, $f(w')\neq w'$ и $u\circ_f w'=(u\circ_f f(w'))\circ_f\bar{f}(w')=(u\circ_f v)\circ_f v'$.

Если $\Lambda\neq f(v')\neq v'$, то слова $f(v')$ и $\bar{f}(v')$ короче, чем v, так что по предположению индукции

$$(u\circ_f v)\circ_f v'=[(u\circ_f v)\circ_f f(v')]\circ_f\bar{f}(v')=$$

$$=(u\circ_f[v\circ_f f(v')]\circ_f\bar{f}(v')=$$

$$=u\circ_f([v\circ_f f(v')]\circ_f\bar{f}(v'))=u\circ_f(v\circ_f v').$$

3. Если обозначить определенную описанным выше отображением f_m УШ-операцию символом $\circ_m$, то, например, для $X=\{0, 1\}$ и $n\in\mathbf{N}$ будет справедливо равенство $0^n1^n=(1\circ_m 0)\circ_m(1\circ_m 0)\circ_m\ldots\ldots\circ_m(1\circ_m 0)$.

Действительно, для u и u′ из W(X) таких, что $|u|=|u'|$, имеем $uu'\circ_m 01=(uu'\circ_m 1)\circ_m 0=u1u'\circ_m 0=u01u'$.

У-автомат над $(W(X), \circ_m)$, допускающий множество $\{0^n1^n|n\in\mathbf{N}\}$, можно, таким образом, представить себе как автомат с одной входной лентой и с двумя читающими головками, которые в начале работы находятся в середине ленты и передвигаются поочередно (одна налево, другая — направо).

Нетрудно убедиться в том, что $W(X, \circ_m)$ — свободный моноид. Действительно, для $u\in W(X)$ и $x\in X$ всегда $|u\circ_m x|=|u|+1$ и из $u\circ_m x=v\circ_m x'$ при $v\in W(X)$ и $x'\in X$ следует, что $u=v$ и $x=x'$.

4. Пусть $d=(s_1, \ldots, s_n; d_1, \ldots, d_n)\in\mathbf{N}^n\{-1, +1\}^n$ и $s=s_1+s_2+\ldots+s_n$. Пусть тогда отображение f_d из W(X) в себя определено следующим образом:

w из W(X) записывается в виде

$w=w_0w_1w_1'w_2w_2'\ldots w_nw_n'$ с $|w_0|<s$ и, если $|w|\geqslant s$, то

$$|w_i|=\begin{cases}ks_i, & \text{если } d_i=+1,\\ s_i & \text{в противном случае;}\end{cases}$$

$$|w'_i|=\begin{cases}s_i, & \text{если } d_i=+1,\\ ks_i & \text{в противном случае,}\end{cases}$$

где k определяется условием $(k+1)s+|w_0|=|w|$; тогда $f_d(w)=w_0v_1v_2\ldots v_n$, где

$$v_i=\begin{cases}w_i, & \text{если } d_i=+1,\\ w'_i & \text{в противном случае.}\end{cases}$$

Поскольку приведенное разложение слова w всегда существует и определено однозначно (так как k и $|w_0|$ могут быть единственным образом найдены путем деления с остатком $|w|$ на s), то f_d является корректно определенным отображением и $f_d(w)$ оказывается кусочным подсловом слова w. Очевидно, что $\bar{f}_d(w)=v_1'v_2'\ldots v_n'$, где

$$v'_i=\begin{cases}w'_i, & \text{если } d_i=+1,\\ w_i & \text{в противном случае.}\end{cases}$$

Так как $|\bar{f}_d(w)|=s$, то $f_d(\bar{f}_d(w))=\Lambda$.

Поскольку слово $\bar{f}_d(w)$ может быть в точности одним способом выделено из слова w, то и условие 2) выполнено, т. е. f_d является У-отображением.

Пусть символ $\circ_d$ обозначает УШ-операцию, полученную методом из п. 2) на базе f_d.

Тогда $\circ_d$ при $d=(1;+1)$ в точности совпадает с конкатенацией, т. е. моноид $(W(X), \circ_d)$ изоморфен моноиду $F(X)$.

Пусть $d=(1, 1; +1, -1)$. Для $w\in W(X)-\Lambda$ и $x, y\in X$ в этом случае $f_d(x)=x$ и $f_d(x, y)=\Lambda$, так что $w\circ_d x=w$ и $w\circ_d(xy)=w_0w_1xyw_2$, где $w=w_0w_1w_2$ с $|w_1|=|w_2|$ и $|w_0|\leqslant 1$. У-автомат над $(W(X), \circ_d)$ мы можем представить себе как автомат с двумя головками, которые в начале работы располагаются на середине ленты и в процессе работы синхронно передвигаются друг от друга на одну ячейку за такт. Такой автомат можно, конечно, заменить на 2-ЭЭШ-автомат, в который слово w вводится в виде пары слов (u, v) такой, что $|v|\leqslant|u|\leqslant|v|+1$ и $w=u\tilde{v}$.

Рассматривая оба частных случая выбора d, нетрудно понять, что описанные в конце предыдущего раздела детерминированные методы обработки входных слов с помощью разложения их на подслова с фиксированным соотношением между их длинами оказываются частными случаями таких методов, представимых с помощью У-автоматов над $(W(X), \circ_d)$ при произвольных d.

В этом разделе были обрисованы в общих чертах разнообразные возможности обобщения теории конечных автоматов на случай произвольных моноидов. Следует указать также, что описанными здесь методами можно исследовать и преобразования произвольных моноидов (см. разд. 8.2).

УПРАЖНЕНИЯ

8.1. (Гинзбург, Роуз.) 1. Пусть M — конечный преобразователь. Не используя следствие 8.6.2, покажите, что для любого R из $\mathrm{Rat}(Y)$ множество $M^{-1}(R)=\{w\in F(X)\mid T_M(w)\subseteq R\}$ рационально.

2. Докажите, что отображение h из $F(X)$ в $F(Y)$ является порождаемым некоторым конечным преобразованием тогда и только тогда, когда выполнены следующие условия:

а) для любого w из $F(X)$ и любого префикса u слова w (т. е. $uv=w$ при подходящем v) $h(u)$ является префиксом $h(w)$ [т. е. $h(u)v'=h(w)$ при подходящем v'];

б) существует натуральное число k такое, что для всех w из $F(X)$ и всех x из X выполнено неравенство $|h(wx)|-|h(w)|\leqslant k$;

в) $h(\Lambda)=\Lambda$;

г) $h^{-1}(R)$ — рациональное множество при любом R из $\mathrm{Rat}(Y)$.

3. Пусть $X=Y=\{a, b\}$ и $h: F(X)\to F(Y)$ определено условием

$$h(w)=\begin{cases} a^{2i+1}b^{|v|}, & \text{если } w=a^ibuv \text{ при } |u|=i\geqslant 0,\\ a^{|w|} & \text{в противном случае.}\end{cases}$$

Покажите, что h удовлетворяет условиям а)—в) и что при рациональном R рационально $h(R)$, но что при этом h не является преобразованием, порождаемым каким-либо конечным преобразователем.

4. Пусть $X=\{a, b, c\}$ и $L=\{a, b\}^*c$.

Покажите, что для каждого $R\neq\varnothing$ из $\mathrm{Rat}(X)$ существует конечный преобразователь M такой, что $M(L)=R$, но не существует конечных преобразователей M таких, что $M(\{a, b\}^*)=L$ или $M(\{a, b\}^*-\Lambda)=L$.

8.2.* (Саломон.) Подмножество L моноида $F(X)$ называется ограниченным, если в $F(X)$ существуют слова $w_1, w_2, \ldots, w_n$ такие, что $L\subseteq w_1^*w_2^*\ldots w_n^*$.

1. Пусть M — конечный преобразователь с допускающими состояниями. Докажите, что при любом ограниченном рациональном множестве R и множество $M(R)$ ограничено (и рационально) и что отсюда, например, следует, что рациональное множество R не ограничено, если существует конечный преобразователь с допускающими состояниями M такой, что $M(R)=\{0, 1\}^*$.

2. Пусть $R\subseteq\mathrm{Rat}(X)$ и A — сокращенный ДРС-автомат, допускающий множество R. С использованием п.1 докажите, что множество R не ограничено тогда и только тогда, когда A имеет перекрывающиеся циклы, т. е. когда существуют состояния z_1, z_2 и z_3 автомата A, слова u и v из $F(X)$ и различные буквы x и x′ из X такие, что

$$f^*(z_2, u)=z_1,\ f^*(z_1, x)=z_2,$$

$$f^*(z_2, v)=z_3,\ f^*(z_3, x')=z_2.$$

[Указание Обратите внимание на пример 8.2.1.]

3. Пусть R — произвольное не ограниченное рациональное множество. Используя п.2, докажите, что для любого рационального множества R′ существует конечный преобразователь с допускающими состояниями M такой, что $M(R)=R'$.

4. Докажите, что существует алгоритм, решающий для любых двух ограниченных рациональных множеств R и R′ вопрос о существовании конечного преобразователя с допускающими состояниями M такого, что $M(R)=R'$.

5. Используя полученные выше результаты, докажите, что существует алгоритм, решающий для любых двух рациональных множеств R и R′ вопрос о существовании конечного преобразователя с допускающими состояниями M такого, что $M(R)=R'$.

8.3. 1. Докажите, что вопрос об эквивалентности конечных преобразователей с допускающими состояниями разрешим (используйте п. 1 теоремы 5.5.9 и п.1 теоремы 8.3.2).

2. Покажите, что для произвольных а-преобразователей M и M' с входным алфавитом X и выходным алфавитом Y и для произвольных множеств R и R', где $R \in Rat(X)$ и $R' \in Rat(Y)$, разрешимы следующие вопросы:

а) Пусто ли множество $M(R)$?

б) Бесконечно ли множество $M(R)$?

в) Выполняется ли включение $M(R) \subseteq M'(R)$?

г) Выполняется ли равенство $M(R) = M'(R)$?

д) Выполняется ли включение $M(R) \subseteq R'$?

е) Выполняется ли равенство $M(R) = R'$?

[Указание. Используйте теоремы 8.2.4 и 5.5.9 и следствие 8.2.6]

3. Пусть X и Y — произвольные конечные множества и h_i при $i = 1, 2$ — гомоморфизмы из $F((X) \cup \Lambda) \times (Y \cup \Lambda))$ в $F(X)$ и в $F(Y)$ соответственно, определенные условием: $h_i(x, y) = pr_i(x, y)$ для $(x, y) \in (X \cup \Lambda) \times (Y \cup \Lambda)$.

Приведите пример двух различных рациональных множеств R и R' из $\mathscr{P}(F((X \cup \Lambda) \times (Y \cup \Lambda)))$ таких, что при любом подмножестве L моноида $F(X)$ выполнено равенство

$$h_2(h_1^{-1}(L) \cap R) = h_2(h_1^{-1}(L) \cap R').$$

8.4. 1. (Элго, Мезей.) Докажите, что для каждого а-преобразователя M существует эквивалентный алфавитный а-преобразователь M' (см. замечание к определению 8.2.2 и п.1 теоремы 6.2.7).

2. (Элго, Мезей.) Докажите, что суперпозиция двух а-преобразовательных отображений снова является а-преобразовательным отображением. [Указание См. упражнение 5.16, п.1.] Для двух данных алфавитных а-преобразователей постройте а-преобразователь, имеющий множеством состояний декартово произведение множеств состояний исходных преобразователей. Покажите, что построенный а-преобразователь оказывается Λ-свободным, если таковы исходные а-преобразователи.]

3. (Ниват.) Используя п. 1, покажите, что в п.1 теоремы 8.2.4 можно также предполагать, что h_1 и h_2 являются алфавитными гомоморфизмами и что R — стандартное множество (см. значение к теореме 8.2.4).

4. (Элго, Мезей.) Докажите, что класс всех рациональных преобразований является наименьшим классом соответствий между конечно-порожденными свободными моноидами, содержащим гомоморфизмы свободных моноидов и сохраняющие длину слов соответствия (при которых каждый элемент образа данного слова имеет длину, равную длине этого слова) и замкнутым относительно суперпозиций и операции перехода к обратному соответствию (k^{-1} для k).

5. (Боассон, Ниват). Покажите, что для любого а-преобразователя M следующие высказывания эквивалентны:

а) для любого v из $F(Y)$ множество $M^{-1}(\{v\})$ конечно и для всякого u из $F^+(X)$ выполнено включение $M(\{u\}) \subseteq F^+(Y)$;

б) существуют конечное множество P, множество R в $Rat(P)$, гомоморфизм g_1 из $F(P)$ в $F(X)$ и Λ-свободный алфавитный гомоморфизм g_2 из $F(P)$ в $F(Y)$ такие, что графиком T_M оказывается множество $\{(g_1(w), g_2(w)) \mid w \in R\}$, т. е. такие, что при любом $L \subseteq F(X)$ выполнено равенство $M(L) = g_2(g_1^{-1}(L) \cap R)$.

8.5. Докажите, что следующие отображения являются а-преобразовательными.

1. Рациональные подстановки.

2. При $R \in \mathrm{Rat}(X)$ v_R, d_R и p_R — следующие отображения из $\mathcal{P}(F(X))$ в себя: для $L \subseteq F(X)$ по определению $v_R(L) = L \cup R$, $d_R(L) = L \cap R$, $p_R(L) = RL$.

3. При $R \in \mathrm{Rat}(X)$ q_R (соответственно q'_R) — отображение, сопоставляющее каждому $L \subseteq F(X)$ его левое частное множество (соответственно — правое частное) по R (см. определение 5.5.6).

4. При $R \in \mathrm{Rat}(X)$ f_R — отображение, отвечающее соответствию с графиком $\{(u, v) \in F(X) \times F(X) \mid uv \in R\}$.

5. $f : F(X) \to F(X)$, где f определено соотношениями $f(\Lambda) = \Lambda$ и $f(x_1x_2 \ldots x_n) = x_1x_3 \ldots x_m$ при $n \in \mathbf{N}$, $x_i \in X$ при $i = 1, \ldots, n$ и $n = m$, если n — нечетное число, и $m = n-1$ в противном случае.

8.6. (Берстел.) Пусть r — произвольное рациональное число, $0 \leqslant r \leqslant 1$, $W_r = \{a^n b^k \mid n \in \mathbf{N}_0$ и $nr \leqslant k \leqslant n\}$ и $L = \{a^n b^n \mid n \in \mathbf{N}_0\}$.
Пусть, далее U и V определены, как в следствии 8.2.7. Докажите следующее.

1) Существует a-преобразователь M_r такой, что $M_r(W_r) = U$. [Указание. См. упражнение 3.12.]

2. Не существует a-преобразователя M такого, что $M(V) = L$. [Указание. Подробно просмотрите доказательство следствия. 8.2.7]

3. Не существует a-преобразователя M такого, что $M(V) = W_r$. [Указание. Результат можно получить несложным изменением доказательства следствия 8.2.7 или вывести из следствия 8.2.7 с помощью утверждения 1.]

8.7. (Ибарра) Рассматриваются Λ-свободные недетерминированные конечные преобразователи с допускающими состояниями и Λ-свободные недетерминированные конечные преобразователи над $X \times Y$, т. е. с входным алфавитом X и выходным — Y.

1. Докажите, что следующие высказывания эквивалентны:

а) при $|X| \geqslant 2$ вопрос об эквивалентности Λ-свободных недетерминированных конечных преобразователей с допускающими состояниями над $X \times \{1\}$ разрешим;

б) вопрос об эквивалентности Λ-свободных недетерминированных конечных преобразователей над $\{0, 1\} \times \{1\}$ разрешим.

2*. Докажите, что не существует алгоритма, решающего при произвольном X, является ли некоторый Λ-свободный недетерминированный конечный преобразователь с допускающими состояниями над $X \times \{1\}$ эквивалентным следующему Λ-свободному недетерминированному конечному преобразователю с допускающими состояниями

$M_X = (z, X, 1, t, z, z\}$, где $t(z, x) = \{(1^k, z) \mid k = 1, 2, 3\}$ — для всех $x \in X$.

3. Из п.2 выведите утверждение о том, что не существует алгоритма построения Λ-свободного недетерминированного конечного преобразователя с допускающими состояниями с минимальным числом состояний, эквивалентного данному Λ-свободному недетерминированному конечному преобразователю с допускающими состояниями над $X \times \{1\}$.

4. Из пп. 1 и 2 выведите утверждение о неразрешимости вопроса об эквивалентности Λ-свободных недетерминированных конечных преобразователей с допускающими состояниями вида $M = (Z, \{0, 1\}, 1, t, s)$, обладающих свойством: из $(1^k, z') \in t(z, x)$ следует, что $k = 1, 2, 3$ для $z \in Z$ и $x \in \{0, 1\}$.

5*. Докажите утверждения, возникающие из утверждений 1—3 при замене входных алфавитов на выходные и обратно. Выведите отсюда утверждение о неразрешимости вопроса об эквивалентности Λ-свободных недетерминирован-

ных конечных преобразователей с допускающими состояниями вида $M=(Z, 1, \{0, 1\}, t, s)$ таких, что $|w|\in\{2, 3, 6\}$ при $(w, z')\in t(z, 1)$.

8.8. 1. Докажите, что каждый случай проблемы соответствий Поста либо не имеет решения, либо имеет бесконечно много решений.

2. Докажите, что следующая ослабленная проблема соответствий Поста разрешима.

Случай ослабленной проблемы соответствий Поста над X есть четверка $Q=(X, n, u, v)$, где $n\in\mathbf{N}$, $u=(u_1, \ldots, u_n)$, $v=(v_1, \ldots, v_n)$ и u_i и v_i — элементы моноида $F(X)$. Случай Q имеет решение, если существуют последовательности чисел $i_1, \ldots, i_p$ и $j_1, \ldots, j_q$ такие, что $u_{i_1}u_{i_2}\ldots u_{i_p}=v_{j_1}v_{j_2}\ldots v_{j_q}$.

Общая ослабленная проблема соответствий Поста над X состоит в том, чтобы для каждого случая этой проблемы над X установить, имеет ли он решение.

3. Докажите, что существует алгоритм, который для любых двух конечных множеств X и Y, любых двух частичных автоматов Мили A и A′ с X и Y в качестве входного и выходного алфавитов и для любых двух состояний z (автомата A) и z′ (автомата A′) определяет, имеется ли в $F^+(X)$ слово w такое, что $g^*(z, w)=g'^*(z', w)$.

4. Докажите, что не существует алгоритма, который для любых двух конечных множеств X и Y и для любых двух конечных преобразователей M и M′ с X и Y в качестве входного и выходного алфавитов определяет, имеется ли в $F^+(X)$ слово такое, что $M(\{w\})=M'(\{w\})$.

5. Пусть X и Y — конечные множества и h_1 — определенный для всех x из X и всех y из Y равенством $h_1(x, y)=x$ гомоморфизм из $F((X\cup\Lambda)\times(Y\cup\Lambda))$ ь $F(X)$. Докажите, что не существует алгоритма, определяющего для любых двух рациональных подмножеств R и R′ моноида $F((X\cup\Lambda)\times(Y\cup\Lambda))$, выполняется ли для всех слов w из $F(X)$ равенство $h_1^{-1}(w)\cap R=h_1^{-1}(w)\cap R'$.

8.9. 1. Докажите, что множество $\{(0^m1^n, 1^n0^m)\,|\,m, n\in\mathbf{N}\}$ не допускается никаким 2-ЭМ-автоматом. [Указание. Действуйте так же, как в доказательстве следствия 8.7.2, или используйте утверждение из п.2 данного упражнения и следствие 8.2.8, или используйте утверждение из п.3 данного упражнения.]

2. Докажите, что если $R\in Rat(X)$ и A — 2-ЭМ-автомат над (X, Y), то множества $R\times F(Y)\cap L(A)$ и $F(X)\times R\cap L(A)$ также являются реакциями 2-ЭМ-автоматов над (X, Y) (см. также п. 3 упражнения 8.11).

3. С помощью п.1 следствия 8.4.4 или теоремы 8.4 7 перенесите на случай 2-ЭМ-автоматов теорему об итеративном подслове (см. теорему 5.4.8) и uvw-теорему (см. следствие 5.4.10).

4. По аналогии с доказательством пп. 2 и 3 теоремы 5.5.9 докажите с помощью п.3 данного упражнения, что для 2-ЭМ-автоматов разрешим вопрос о пустоте или о бесконечности реакции.

5. Докажите следствие 8.2.7 с помощью п.3 и сравните это доказательство с приведенным в тексте.

6. (Элго, Мезей, Миркин.) Докажите приведенное ниже утверждение и выведите из него, что график W отображения, переводящего каждое слово в зеркальное для него (см. доказательство следствий 8.2.8 и 8.4.4), не может быть реакцией никакого 2-ЭМ-автомата.

Для $U\subseteq F(X)\times F(X)$ следующие высказывания эквивалентны:

а) $U\in Rat(X, Y)$ и $|u|=|u'|$ для всех $(u, u')\in U$;

б) Пусть $P=X\times Y$; тогда для естественного гомоморфизма ν_P (см. следствие 8.4.6) выполняется включение $U\in\nu_P(Rat(P))$. [Указание. При иссле-

довании W учтите, что в п.б) гомоморфизм ν_P инъективен, и рассмотрите в F(P) множества $U'=(0, 0)^*(1, 1)(0, 0)^*$ и $V'=\nu_P^{-1}(\nu_P(U')\cup W)$.]

8.10. 1. Модифицируйте определение 2-ЭЭШ-автоматов, требуя, чтобы автомат до тех пор, пока это возможно, попеременно считывал по одному символу с каждой ленты (вместо одновременного считывания). Докажите, что теорема 8.5 3 остается справедливой для таких модифицированных 2-ЭЭ-автоматов при замене P_0 на $P'_0=\{(x, \Lambda)(\Lambda, y) \mid (x, y)\in P_0\}$.

2. Обобщите высказывания из разд. 8.5 следующим образом. Пусть P — конечное подмножество произведения $F(X)\times F(Y)$ и V — рациональное подмножество моноида F(P) такое, что $\nu_P(V)=F(X)+F(Y)$ и что сужение $\varphi_{P, V}=\nu_P/V$ гомоморфизма ν_P на V инъективно.

2-ЭМ-автомат A называется 2-ЭМ-автоматом с программой чтения V, если реакция фундаментального для него HPC-автомата принадлежит V, т. е. если последовательность меток на ребрах любого пути из начального в некоторое финальное состояние в графе автомата A принадлежит V.

(**Примеры.** Пусть P определено, как в теореме 8.5.3. Если V задано, как в теореме 8 5.3, то 2-ЭМ-автомат с программой чтения V оказывается 2-ЭЭШ-автоматом. Если $V'=(P_1P_2)^*(P_1^*\cup P_2^*)$, то 2-ЭМ-автомат с программой чтения V′ оказывается модифицированным 2-ЭЭШ-автоматом из п.1. Если $V''=P_1^*P_2^*$, то 2-ЭМ-автомат с программой чтения V″ оказывается 2-ЭМ-автоматом, который сначала целиком считывает слово с первой ленты и затем считывает слово со второй ленты.)

Тогда высказывания 2—4 теоремы 8.5.3 и первые три высказывания следствия 8 5.4 остаются верными, если везде заменить термин «2-ЭЭШ-автомат» на термин «2-ЭМ-автомат с программой чтения V» и β — на $\varphi^{-1}{}_{P, V}$. [Указание. Действуйте, как в разд. 8.5, и докажите, что для $R\in Rat(X)$ верны соотношения $\varphi^{-1}{}_{P, V}(R\times F(Y))=\nu_P^{-1}(R\times F(Y))\cap\Lambda$ и $\nu_P^{-1}(R\times F(Y))\in Rat(P)$.]

8.11. 1. Докажите, что вопрос о том, является ли данный алфавитный 2-ЭМ-автомат детерминированным 2-ЭМ-автоматом, неразрешим.

2. Постройте детерминированный 2-ЭМ-автомат, допускающий множество M из теоремы 8.6.6.

3. Два 2-ЭМ-автомата A_1 и A_2 над (X, Y) можно назвать совместными, если для всех (u, v) из $F(X)\times F(Y)$ и всех z_i из Z_i при $i=1, 2$ выполнено условие: $t_1^*(z_1, u, v)\neq\varnothing$ тогда и только тогда, когда $t_2^*(z_2, u, v)\neq\varnothing$.

Докажите, что если A_1 и A_2 — совместные 2-ЭМ-автоматы и A_1 детерминирован, то $L(A_1)\cap L(A_2)\in Rat(X, Y)$.

4. (Уоляспер.) Выведите из п.3, что пересечение любого рационального и любого различимого подмножества произведения $F(X)\times F(Y)$ является рациональным множеством.

5. (Штарк.) Докажите, что вопрос о существовании для данного 2-ЭМ-автомата эквивалентного 2-РС-автомата неразрешим.

8.12.* В литературе часто рассматриваются 2-ЭМ-автоматы с маркировкой входных лент. При этом предполагается, что имеется особый символ $*$, не входящий во входные алфавиты рассматриваемого 2-ЭМ-автомата ($*\notin X\cup Y$). Этот знак помещается в конце каждого из входных слов, так что рассматриваемые пары входных слов имеют вид $(u*, v*)$, где $u\in F(X)$ и $v\in F(Y)$. Наконец, способ функционирования таких 2-ЭМ-автоматов имеет следующие особенности: допускается использование символа $*$ как входного символа; если автомат на

одной из лент считывает символ *, то считывание этой ленты прекращается; пара слов допускается, если автомат после считывания обоих маркеров (символов *) переходит в некоторое выделенное состояние a (множество финальных состояний состоит, таким образом, только из a). Далее, часто вводится также «отказывающее» состояние r, в котором автомат остается в том случае, когда на вход подается не являющаяся допустимой пара слов. В состояние r автомат может перейти (как и в состояние a) только после считывания обоих маркеров.

1. Дайте формальное описание 2-ЭМ-автоматов с маркерами и докажите, что для каждого 2-ЭМ-автомата с маркерами существует эквивалентный «обычный» 2-ЭМ-автомат, и наоборот.

2. Перенесите определение детерминированного 2-ЭМ-автомата на 2-ЭМ-автоматы с маркерами и покажите, что множество M из теоремы 8.6.6 допускается некоторым алфавитным детерминированным 2-ЭМ-автоматом с маркером.

3. Перенесите понятие полностью определенного детерминированного 2-ЭМ-автомата на случай 2-ЭМ-автоматов с маркерами и докажите, что некоторое множество L в точности тогда является реакцией полностью определенного детерминированного 2-ЭМ-автомата с маркерами, когда оно допускается некоторым полностью определенным детерминированным 2-ЭМ-автоматом.

[Указание. При построении полностью определенного детерминированного 2-ЭМ-автомата с маркерами, эквивалентного данному алфавитному полностью определенному детерминированному 2-ЭМ-автомату, действуйте, как в доказательстве п.2 теоремы 8.6.9. Обратное построение осуществляйте в два этапа:

а) для каждого алфавитного полностью определенного детерминированного 2-ЭМ-автомата с маркерами A' над (X, Y) постройте алфавитный полностью определенный детерминированный 2-ЭМ-автомат A'' над $(X \cup *, Y \cup *)$. Здесь * рассматривается как обычный входной символ (не как маркер), для которого выполняется включение $L(A'') = L(A') \cdot (*, *) \subseteq F(X)* \times F(Y)*$, т. е $L(A') = \{(u, v) \mid (u*, v*) \in L(A'')\}$;

б) для каждого полностью определенного детерминированного 2-ЭМ-автомата A над $(X \cup *, Y \cup *)$ с реакцией $L(A'') \subseteq F(X)* \times F(Y)*$ постройте полностью определенный детерминированный 2-ЭМ-автомат A''' над (X, Y) с реакцией $L(A'') = L(A''') \cdot (*, *)$.]

4. (Розенберг.) Перенесите определение 2-РС-автомата на случай 2-ЭМ-автоматов с маркерами и докажите, что класс реакций таких автоматов, называемых двуленточными автоматами Розенберга (коротко: 2-Р-автоматами), замкнут относительно операции дополнения, но не замкнут относительно операций пересечения, объединения, произведения и образования подмоноида и строго включает в себя класс реакций 2-РС-автоматов. [Указание. Покажите, что множество $\{(0, \Lambda), (\Lambda, 0)\}$ является реакцией некоторого 2-Р-автомата и что каждый 2-РС-автомат может быть преобразован в эквивалентный 2-Р-автомат (как в п 1.) Чтобы доказать замкнутость относительно операции дополнения, сначала доопределите рассматриваемый 2-Р-автомат и потом действуйте так же, как в доказательстве теоремы 5.5.5 (см. [32]). Доказывая незамкнутость, рассмотрите 2-Р-автоматы над $X = \{0, 1, 2\}$ и докажите при $E = \{(0, 0), (1, 1)\}$, $G = \{(2, 2)\}$ и $H = \{(0, \Lambda), (1, \Lambda)\}$, что множество $J = E^*GH^*$ является реакцией некоторого 2-Р-автомата, а множества J^2 и J^* таковыми не являются; рассматривая пересечения, действуйте так же, как в случае 2-РС-автоматов]

5. (Рабин, Скотт.) Преобразуйте определение 2-РС-автоматов с маркерами так, чтобы пара слов допускалась уже тогда, когда автомат считывает первый

маркер (если при этом он переходит в некоторое финальное состояние), независимо от того, что еще записано на второй ленте. Исследуйте класс реакций таких автоматов, в частности для таких автоматов проблема эквивалентности разрешима [3].

ОБЗОР ЛИТЕРАТУРЫ

Последовательностные машины Гинзбурга (конечные преобразователи) являются частным случаем рассмотренных в [30] конечных преобразователей. Независимо они были определены в [13] и в основном в рамках теории контекстно-свободных языков исследованы в [17 и 18]. По этому поводу и по поводу упражнения 8.1 см. также [14]. Связь с автоматами Мили показана в упражнении 2.8.

Конечные преобразователи с допускающими состояниями были введены в [27]. На этой работе основано упражнение 8.2.

Теорема 8.3.2, п.2 и ее доказательство взяты из [19]. Приведенное в упражнении 8.7 уточнение этого результата доказано в [20]. О проблеме соответствий Поста см. в списке литературы к гл. 4 и 6 соответственно учебники [9 и 1].

Понятие преобразования введено в [30]. В современном виде это понятие и соответствующие автоматы (в виде 2-ЭМ-автоматов) были определены и подробно исследованы в [11]. Теоремы 8.4.10, 8.4.11, следствие 8.2.8 и пп. 1, 2, 4 упражнения 8.4 взяты из этой работы. Термин «а-преобразователь» введен в работе [16], авторы которой выяснили значение а-преобразователей для теории формальных языков и провели исчерпывающее исследование этого понятия и его приложений в дальнейших работах (см. по этому поводу [15]).

После появления работ [30 и 11] дальнейшее развитие теории рациональных преобразований проводилось параллельно авторами работы [16] и французской школой — см. упоминавшийся в гл. 2 учебник [3] и работу [2].

Теорема 8.2.4 была независимо доказана в [22] и [16] и в виде теоремы 8.4.7, в [5]. Приведенное в книге доказательство ближе к доказательству в [5]. В [22] содержится приведенный в п.3 упражнения 8.4 вариант. Следствие 8.2.7, его доказательство и упражнение 8.6 заимствованы из неопубликованной работы Берстела (Страсбург, 1971).

Идея разбиения слов на подслова и одновременной обработки этих подслов с помощью нескольких читающих головок появилась в [8] и [28], см. также [9]. Независимо в [1] для частного случая разбиения на две равновеликие части, а также в [24] и [26] для общего случая была установлена связь между 2-ЭМ-автоматами и линейными грамматиками. Эти результаты были обобщены в [7], из этой работы взята идея представления, использованного в примере 8.4.8. Частично перекрывающееся с результатами из [7] независимое обобщение было проведено в [29].

Понятие автомата с несколькими читающими головками и соответствующие методы обработки слова w в виде n-ки (w, w, .., w) с помощью n-ленточного автомата были рассмотрены в [24 и 25].

Понятие ЭЭШ-автомата, теорема 8.5.3 и первое утверждение следствия 8.5.4 основаны на работе [10].

Двуленточные автоматы с состояниями, определяющими, с которой из лент ведется считывание, были введены в использованной в гл. 5 работе [41], причем в форме, приведенной в п.5 упражнения 8.12. Авторы этой работы показа-

ли, что проекции реакций таких автоматов являются рациональными множествами (см. п 3 следствия 8.4.4) и, как следствие из этого факта, что множества реакций не замкнуты относительно операции пересечения.

Двуленточные автоматы в смысле определения 8.7.1 были исследованы впервые в [21]. В этой работе было показано, что недетерминированные 2-РС-автоматы допускают в точности рациональные подмножества произведения $F(X) \times F(Y)$ и что на этот случай могут быть распространены результаты из [41] (см. список литературы к гл. 5), а также было доказано, что высказывания а) и б) из п.6 упражнения 8.9 эквивалентны. Утверждение 2) теоремы 8.7.3 является частным случаем одного общего результата из [31 и 32]. Высказывания 3 и 5 теоремы 8.7.3 были (несколько иным путем) также доказаны в [32], приведенное в книге доказательство высказывания 5 в основном соответствует работе [41] (из списка литературы к гл. 5). В [3] доказана разрешимость проблемы эквивалентности для 2-РС-автоматов.

Независимо от работы [11] в [23, 24 и 26] (см. также [12]) были введены и исследованы 2-РС-автоматы с маркерами (см. п.4 упражнения (8.12) и было, в частности, доказано высказывание, соответствующее теореме 8.4.10 (поскольку в недетерминистском случае все такие модели автоматов эквивалентны).

Во всех упомянутых работах (за исключением работы [41] из списка литературы к гл. 5) рассматривались не только двуленточные, но и многоленточные автоматы.

Понятия различимого и рационального подмножества произвольного моноида были введены Эйленбергом (см. учебник, упомянутый в гл. 2). Пример 8.8.2 принадлежит Винограду (см. учебник Эйленберга).

Определение 8.8.3 и теорема 8.8.4 (кроме высказывания о сильно детерминированных У-автоматах) получены (в несколько иной терминологии) в [33]. Понятия детерминированного 2-ЭМ-автомата и полностью определенного детерминированного 2-ЭМ-автомата являются частными случаями общего понятия из этой же работы. Высказывания 1 и 2 теоремы 8.6.9 и высказывания 3 и 4 следствия 8.6.10, а также п.3 упражнения 8.11 тоже в основном заимствованы из [33].

Способы определения У-операций с помощью У-отображений являются обобщениями способов, предложенных в [34]. Эти способы обобщают также и конструкции из [29]. У-отображение f_m и УШ-операция $\circ_m$ описаны в [29]. Соответствующая отображению f_d УШ-операция является представлением операции из [29], см. по этому поводу [6].

СПИСОК ЛИТЕРАТУРЫ

К главе 1

1 B.Buchberger, F.Lichtenberger, Mathematik für Informatiker I, Die Methode der Mathematik, 2.Aufl. Springer, Berlin, 1981.

2. G. Hotz, Informatik: Rechenanlagen, Teubner, Stuttgart, 1972.

3 P.Kandzia, H.Langmaack, Informatik: Programmierung, Teubner, Stuttgart, 1973.

4. G.Lallement, Semigroups and Combinatorial Applications, Wiley, New York, 1979.

5 H.R.Lewis, C.H.Papadimitriou, Elements of the Theory of Computation, Prentice-Hall, Englewood Cliffs, 1981.

6. K.Mehlhorn, Effiziente Algorithmen, Teubner, Stuttgart, 1977.

К главе 2

1. A.W. Burks, H. Wang, The logic of automata I, II, J.Assoc.Comput. Mach. 4 (1957) 193-218, 279-297.

2. A.R. Butz, Functions Realized by Consistent Sequential Machines, Inf. and Control 48 (1981) 147-191.

3. S. Eilenberg, Automata, Languages, and Machines, Vol.A, Academic Press New York, London, 1974.

4 F. Gécseg, I. Peák, Algebraic Theory of Automata, Akadémiai Kiadó, Budapest, 1972.

5. A. Gill, Introduction to the Theory of Finite-State Machines, McGraw-Hill, New York, 1962.

6 S. Ginsburg, Some remarks on abstract machines, Transactions Amer.Math.Soc., 96 (1960) 400-444.

7 S. Ginsburg, An Introduction to Mathematical Machine Theory, Addison-Wesley, Reading, Mass. 1962.

8 W.M. Gluschkow, Theorie der abstrakten Automaten, Dtscher Vlg. d.Wiss., Berlin 1963 (Übersetzung aus dem Russischen, Original 1961).

9. V.M. Glushkov, A.A. Letichevskii, Theory of algorithms and discrete processors; in J.T. Tou (ed.), Advances in Information Systems Science, Plenum Press, New York, 1969, 1-58.

10. J.N. Gray, M.A. Harrison, The theory of sequential relations, Inf. and Control 9 (1966) 435-468.

11. D. Gries, Describing an Algorithm by Hopcroft, Acta Inf. 2 (1973) 97-109.

12. J. Hartmanis, R.E. Stearns, Algebraic Structure of Sequential Machines, Prentice-Hall, Englewood Cliffs, New York, 1966.

13. J. Hopcroft, An n·log(n) Algorithm for Minimizing States in a Finite Automaton; in Z.Kohavi, A.Paz (Hrsgb.), Theory of Machines and Computations, Academic Press New York, London, 1971, 189-196.

14. G. Hotz, Der logische Entwurf von Schaltkreisen, W.de Gruyter, Berlin, 1974.

15 D.A.Huffman, The synthesis of sequential switching circuits, J.Franklin Institute 257 (1954) 161-190, 275-303.

16. P. Hummitzsch, Beziehungen zwischen einigen schwachen Äquivalenzen endlicher Automaten, EIK 8 (1972) 77-86.

17. P. Hummitzsch, Die Entscheidbarkeit der endlichen Ununterscheidbarkeit endlicher Automaten, Zeitschr.f.math.Logik u.Grundlagen d.Math. 17 (1971) 315-322.

18. Z. Kohavi, Switching and Finite Automata Theory, McGraw-Hill, New York, 1970.

19. D. Mange, Synthèse des machines séquentielles synchronisées, Systèmes logiques - Cahiers de la C.S.L. 4 (Juli 1972) 198-212.

20. G.H. Mealy, Method for synthesizing sequential circuits, Bell System Techn. J. 34 (1955) 1045-1079.

21. H. Minsky, Computation: Finite and Infinite Machines, Prentice Hall, Englewood Cliffs, New York, 1967.

22. H.-J.Pohl, Über die Reduzierung der Anzahl von Eingabesignalen von Automaten, Zeitschr.f.math.Logik und Grundlagen d.Math. 14 (1968), 93-96.

23 G.N. Raney, Sequential functions, J.Assoc.Comput.Mach. 5 (1958) 177-180.

24. A. Salomaa, Theory of Automata, Pergamon Press, Oxford, 1969.

25. P.H. Starke, Abstrakte Automaten, Dtscher Vlg.d.Wiss.,Berlin,1969.

26. P.H. Starke, Über die Experimentmengen determinierter Automaten, EIK 8 (1972) 67-76.

27. W. Stucky, Linear realisierbare endliche Automaten, Dissertation, Math.-Naturwiss.Fakultät, Universität Saarbrücken, 1969.

28. R. Valk, Topologische Wortmengen, topologische Automaten, zustandsendliche, stetige Abbildungen, Mitteilungen der Gesellschaft für Math. und Datenverarbeitung, Bonn, Nr. 19, 1972.

29. H.K.-G. Walter, Die relationale Äquivalenz von Automaten, Techn. Hochschule Darmstadt, FB Informatik, Bericht AFS 73-3, 1973.

30. G. Wechsung, Die Gruppe der eineindeutigen längentreuen sequentiellen Funktionen, EIK 8, (1972), 335-352.

31. S. Wendt, Entwurf komplexer Schaltwerke, Springer-Verlag, Berlin, 1974.

К главе 3

1 B.H.Barnes, J.M.Fitzgerald: Minimal experiments for input-independent machines, J.Assoc.Comput.Mach. 14 (1967) 683-686.

2 A.S.Bloch: Über Probleme, die mit sequentiellen Maschinen gelöst werden, Probleme der Kybernetik 3, Akademie-Verlag, Berlin 1963, 93-100 (Übersetzung aus dem Russischen, Original 1960).

3. W.J.Cadden: Equivalent sequential circuits, IRE Trans. on Circuit Theory, CT-6 (1959) 30-34.

4. J.H.Conway: Regular Algebra and Finite Machines, Chapman and Hall, London 1971.

5. M.Depeyrot, J.P.Marmorat, J.Mondelli: An automaton-theoretic approach to the fast Fourier transform; in J.Fox (eds.), Computers and Automata, Microwave Research Inst.Symposia Series 21, Polytechnic Press of the Polytechnic Inst.of Brooklyn, N.Y., 1971, 359-377.

6. S.Even: Rational numbers and regular events, IEEE Trans. on Electronic Computers EC-13 (1964) 740-741.

7. A.Gill: Comparison of finite-state Models, IRE Trans. on Circuit Theory CT-7 (1960) 178-179.

8. A.Gill: State identification experiments in finite automata, Inf. and Control 4 (1961) 132-154.

9. S.Ginsburg: Compatibility of states in input-independent machines, J.Assoc.Comput.Mach. 8 (1961) 400-403.

10. T.N.Hibbard: Least upper bounds on minimal terminal state experiments for two classes of sequential machines, J.Assoc. Comput.Mach. 8 (1961) 601-612.

11. O.H.Ibarra: On the equivalence of finite-state sequential machine models, IEEE Trans. on Electronic Computers EC-16 (1967) 88-90.

12. E.F.Moore: Gedanken-Experiments on sequential machines; in C.E.Shannon, J.McCarthy, Automata Studies, Ann.Math.

Studies 34, Princeton University Press, Princeton 1956, 129-153, Deutsche Übersetzung in: C.E.Shannon, J.McCarthy, Studien zur Theorie der Automaten, Rogner und Bernhard, München 1974, 151-179.

13. H.-J.Schneider: Compiler - Aufbau und Arbeitsweise, W. de Gruyter, Berlin 1975.

14 M.A.Spivak: Minimization of a Moore automaton, Cybernetics 3 (1967) 4-5.

15. P.Starke: Über Experimente an Automaten, Zeitschrift f.Mathem. Logik u.Grundlagen der Mathem. 13 (1967) 67-80.

16. R.Valk: Minimal machines with several initial states are not unique, Inf. and Control 31 (1976) 193-196.

К главе 4

1. A.V.Aho, M.J.Corasick, Efficient string matching: An aid to bibliographic search, Comm.Assoc.Comput.Mach. 18 (1975), 333-340.

2. W. Brauer, Eine Bemerkung zur Zustandsreduktion unvollständiger Automaten, Computing 5 (1970), 178-184.

3. H.-D.Ehrich, Zur Theorie und Anwendung endlicher Minimalüberdeckungen, Arbeiten des Instituts für Instrumentelle Mathematik der Technischen Universität Hannover, Nr. 2, Hannover, 1970.

4. H.-D.Ehrich, A note on state minimization of a special class of incomplete sequential machines, IEEE Trans.on Computers C-21 (1972), 500-502.

5. M.R.Garey, D.S.Johnson, Computers and Intractability, A Guide to the theory of NP-Completeness, Freeman. San Francisco, 1979

6. H.Gericke, Theorie der Verbände, Bibliographisches Institut, Mannheim, 1967.

7. S.Ginsburg, On the reduction of superfluons states in a sequential machine, J.Assoc.Comput.Mach. 6 (1959), 259-282.

8. A.Grasselli, F.Luccio, A method for minimizing the number of internal states in incompletely specified sequential networks, IEEE Trans.on Electronic Computers EC-14 (1965), 350-359.

9. M.A.Harrison, Introduction to Formal Language Theory, Addison-Wesley, Reading, Mass., 1978.

10. J.Hartmanis, R.E.Stearns, Algebraic Structure Theory of Sequential Machines, Prentice-Hall, Englewood Cliffs, N.J., 1966.

11. J.Kella, State minimization of incompletely specified sequen-

tial machines, IEEE Trans.on Computers C-19 (1970), 342-348.

12. A.A.Kurmit, Information-Lossless Automata of Finite Order, J. Wiley & Sons, New York, 1974.

13. P.Müntefering, Transformationen von partiellen Automaten, EIK 8 (1972), 269-274.

14. W.J.Ooms, Minimizing incompletely specified sequential machines, Thesis, University of Illinois, Report No UILU-ENG 73-2216, Urbana, Illinois, 1973.

15. M.C.Paull, S.H.Unger, Minimizing the number of states in incompletely specified sequential switching functions, IRE Trans.on Electronic Computers EC-8 (1959), 356-367.

16. J.-F.Perrot, Endliche Automaten und Prefixcodes; in J.Dörr, G.Hotz (Hrsgb.), Automatentheorie und formale Sprachen (Tagungsbericht, Math.Forschungsinstitut Oberwolfach 1969) Bibliographisches Institut, Mannheim, 1970, 39-53.

17. J.-F.Perrot, Groups and Automata; in Z.Kohavi, A.Paz (Hrsgb.), Theory of Machines and Computations, Academic Press, New York, 1971, 287-293.

18. R.E.Prather, Minimal solutions of Paull-Unger problems, Math.Systems Theory 3 (1969), 76-85.

19. R.E.Prather, An algebraic proof of the Paull-Unger theorem, IEEE Trans.on Computers C-20 (1971), 578-580.

20. C.V.S.Rao, N.N.Biswas, Minimization of incompletely specified sequential machines, IEEE Trans.on Computers C-24 (1975) 1089-1100.

21. A.Salomaa, Jewels of Formal Language Theory, Computer Science Press, Rockville Md., Springer-Verlag, Berlin, 1981

22. I.Tomescu, A matrix method for determining all pairs of compatible states of a sequential machine, IEEE Trans.on Computers C-21 (1972), 502-503.

К главе 5

1. D. Allen, Jr., On a characterization of the nonregular set of primes, J. Computer and System Sciences 2, (1968), 464-467.

2. D.N. Arden, Delayed-logic and finite-state machines, in Theory of Computing Machine Design, Univers.of Michigan Press, Ann Arbor, Mich., 1960, 1-35 und in:
Proc. 2nd Ann.Symp.on Switching Circuit Theory and Logical Design, Detroit, 1961, 133-151.

3. Y. Bar-Hillel, M. Perles, E. Shamir, On formal properties of simple phrase structure grammars, Zeitschr.f.Phonetik, Sprachwissenschaft und Kommunikationsforschung 14 (1961) 143-172.

4. B.H. Barnes, A programmer's view of automata, Computing Surveys 4, (1972), 221-239.

5. J. Berstel, Ensembles reconnaissables des nombres, Institut de Programmation, Université Paris VI, Prépubl.No.I.P.73.19, Paris 1973 und in:
J.-P. Crestin, M. Nivat (Hrsgb): Langages Algébriques, Actes des premières journées d'informatique théorique, Bonascre 1973, Ecole Nat.Sup.de Techniques Avancées, Paris, 1973.

6 V.G. Bodnarchuk, Gleichungssysteme in der Algebra der Ereignisse, J.f.Numer.Mathe.u.Mathem.Physik 3, (1963), 1077-1088 (in russischer Sprache - vgl. Mathem.Reviews 29, Nr.15)

7 W. Brauer, Zur Bestimmung der maximalen Untergruppen des Transitionsmonoids eines Automaten, EIK 7, (1971), 251-260.

8. A.K. Chandra, On the properties and Applications of Program Schemas, Ph.D.Thesis, Computer Science Dept., Stanford Univers., Report No. STAN-CS.73-336, 1973.

9. N. Chomsky, G.A. Miller, Finite state languages, Inform. and Control 1, (1958), 91-112.

10 N. Chomsky, M.P. Schützenberger, The algebraic theory of context-free languages, in P. Brafford, D. Hirschberg (eds.), Computer Programming and Formal Systems, North-Holland, Amsterdam, 1963, 118-161.

11. I.M. Copi, C.C. Elgot, J.B. Wright, Realization of events by logical nets, J.Assoc.Comput.Mach. 5, (1958), 181-196.

12 F.G. Cousineau, J.-F. Perrot, J.M. Rifflet, APL Programs for direct computation of a finite semigroup, in P. Gjerløf, H.J. Helms, J. Nielsen (eds), APL Congress 73, North-Holland, Amsterdam, 1973, 67-74.

13 J.P. Deschamps, Asynchronous automata and asynchronous languages, Inf. and Control 24, (1974), 122-143.

14 G. Dittrich, Analogon zum Kleeneschen Satz für asynchrone Automaten, Seminarber.Inst.f.Theorie d.Autom.u.Schaltnetzwerke 12, Gesellsch.f.Mathematik u.Datenverarbeitung, Bonn 1969.

15 S. Eilenberg, Algèbre catégorique et théorie des automates, Cours donné à l'Institut H.Poincaré, rédigé par R.Roussarie, Paris, 1967.

16. S. Eilenberg, M.P. Schützenberger, Rational Sets in Commutative

Monoids, J.Algebra 13, (1969), 173-191.

17. C.C. Elgot, J.D. Rutledge, Operations on finite automata, in: Proc.Second Ann.Symp.Switching Circuit Theory and Logical Design, Detroit, 1961, 129-132.

18. S. Ginsburg, Sets of tapes accepted by different types of automata, J.Assoc.Comput.Mach. 8, (1961), 81-86.

19. S. Ginsburg, E.H. Spanier, Quotients of Context-Free Languages, J.Assoc.Comput.Mach. 10, (1963), 487-492.

20. A. Ginzburg, A procedure for checking equality of regular expressions, J.Assoc.Comput.Mach. 14, (1967), 355-362.

21. W.M. Gluschkow, Gewisse Probleme der Synthese von Digitalrechnern, J.f.Numer.Mathem.u.Mathem.Physik 1, (1961), 371-411 (in russischer Sprache - vgl.Mathem.Reviews 31, Nr.6736).

22. J. Hartmanis, H. Shank, On the recognition of primes by automata, J.Assoc.Comput.Mach. 15, (1968), 382-389.

23. I.M. Havel, The theory of regular events I,II, Kybernetica Praha 5, (1969), 400-419, 520-544.

24. I.M. Havel, Nondeterministically recognizable sets of languages, in J. Bečvář (ed.), Mathematical Foundations of Computer Science 1975, Lecture Notes in Computer Science Vol. 32, Springer, Berlin 1975, 252-257.

25. R.C. Holt, Some deadlock properties of Computer systems, Computing Surveys 4, (1972), 179-196.

26. K. Jensen, N. Wirth, PASCAL,User Manual and Report, 2nd Edition, Lecture Notes in Computer Science 18, Springer, Berlin, 1975.

27. S.C. Kleene, Representation of events in nerve sets and finite automata, in C.E. Shannon, J. McCarthy (eds.), Automata Studies, Ann.Math.Studies 34, Princeton Univers.Press, Princeton 1956, 3-41; deutsche Übersetzung in: C.E.Shannon, J.McCarthy, Studien zur Theorie der Automaten, Rogner und Bernhard, München, 1974, 3-55.

28. A. Lentin, Equations dans les monoides libres, Gauthier-Villars, Paris, 1972.

29. R.C. Lyndon, M.P. Schützenberger, The equation $a^m = b^n c^p$ in a free group, Michigan Math.J. 9, (1962), 289-298.

30. Z. Manna, Mathematical Theory of Computation, McGraw-Hill, New York, 1974.

31. W.S. McCulloch, W. Pitts, A logical calculus of the ideas immanent in nervous activity, Bulletin of Mathematical Biophysics 5,

(1943), 115-133.

32. R. McNaughton, H. Yamada, Regular expressions and state graphs for automata, IRE Trans.on Electronic Computers EC-9, (1960), 39-47.

33. R. McNaughton, S. Papert, The syntactic monoid of a regular event, in M.A.Arbib (ed.), Algebraic Theory of Machines, Languages, and Semigroups, Academic Press, New York, 1968, 297-312.

34. R. McNaughton, S. Papert, Counter-Free Automata, Research Monograph No 65, The M.I.T. Press, Cambridge, Mass. 1971.

35. J.T. Medvedev, On a class of events representable in a finite automaton, Anhang zur russischen Übersetzung von: C.E.Shannon, J.McCarthy (eds.), Automata Studies, Publ.Agency for Foreign Literature, Moskau 1956; übersetzt von J.J.Schorr-Kon für Lincoln Lab.Rep., 34-73, 1958, abgedruckt in: E.F.Moore (ed.), Sequential Machines, Selected Papers, Addison-Wesley, Reading.Mass., 1964.

36. A.R. Meyer, L.J. Stockmeyer, Word problems requiring exponential time, in Proc. 5th Ann.Symp.on Theory of Computing, 1973, 1-9.

37 J.Myhill, Finite automata and the representation of events, Wright Air Devel.Command Techn.Rep. 57-624, (1957), 112-137.

38 G.J. Nutt, Some applications of finite state automata theory to the deadlock problem, Colorado University, Boulder, Techn.Report CU-CS-017-73, 1973.

39. G. Ott, N.H. Feinstein, Design of sequential machines from their regular expressions, J.Assoc.Comput.Mach. 8, (1961), 585-600.

40. J.-F. Perrot, Sur le calcul effectif du monoide de transition d'un automata fini, in W.D.Itzfeld (Hrsgb.) International Computing Symposium 1970, Proceedings, Gesellsch.f.Mathematik und Datenverarbeitung, Bonn 1973, 664-672.

41. M.O. Rabin, D. Scott, Finite automata and their decision problems, IBM J.Research and Development 3, (1959), 114-125; abgedruckt in E.F.Moore (ed.), Sequential Machines, Addison-Wesley, Reading, Mass., 1964, 63-91; deutsche Übersetzung in: C.E.Shannon, J.McCarthy, Studien zur Theorie der Automaten, Rogner und Bernhard, München, 1974, 327-361.

42 W. Reisig, Petrinetze - Eine Einführung, Springer, Berlin 1982.

43 L. Richter, Betriebssysteme, Teubner, Stuttgart, 1977.

44 R.W. Ritchie, Finite automata and the set of squares, J.Assoc.Comput.Mach. 10, (1963), 528-531.

45. A. Salomaa, Axiom Systems for Regular Expressions of Finite Automata, Ann.Univers.Turku, Ser.AI, 75, Turku 1964.

46. A. Salomaa, Two complete axiom systems for the algebra of regular events, J.Assoc.Comput.Mach. 13, (1966) 158-169.

47. M.P. Schützenberger, On an application of semi-group methods to some problems in coding, IRE Trans.on Information Theory IT-2, (1956), 47-60.

48 M.P. Schützenberger, Une théorie algébrique du codage, Séminaire Dubreil-Pisot, Faculté des Sciences Paris, Année 1955/56, Exposé No.15; sowie C.R.Acad.Sci. Paris 242, (1956), 862-864.

49 M.P. Schützenberger, On context-free languages and push-down automata, Inf.and Control 6 (1963) 246-264.

50 J.I. Seiferas, R. McNaughton, Regularity-preserving relations, Theor.Comp.Science 2 (1976) 147-154.

51. I. Simon, Piecewise testable events, in H.Brakhage, Automata Theory and Formal Languages, 2nd GI Conference, Lecture Notes in Computer Scinece 33, Springer-Verlag, Berlin, 1975, 214-222.

52. R.E. Stearns, J. Hartmanis, Regularity preserving modification of regular expressions, Inf.and Control 6, (1963), 55-69.

53. H.-G. Stork, Ein automatentheoretisches Modell einer Speicherhierarchie, in Lecture Notes in Comp.Science 2, Springer, Berlin 1973, 98-103.

54 T. Urponen, On Axiom Systems for Regular Expressions and on Equations Involving Languages, Ann.Univers.Turku, Ser.AI, 145, Turku 1971

55 C.C. Yang, On the modeling of demand paging algorithmes by finite automata, IEEE Trans.on Computers C-23, (1974) 870-874.

К главе 6

1 J. Albert, Th. Ottmann, Automaten, Sprachen und Maschinen für Anwender, Bibliograph.Institut, Mannheim, 1983

2 M. Brandt, Minimisierung nichtdeterministischer Akzeptoren, EIK 8, (1972) 87-98

3 W. Brauer, Zur Zustandsreduktion unvollständiger Automaten, Seminarbericht Inst.f.Theorie d.Autom.u.Schaltnetzwerke 6, Gesellschaft f.Mathematik u.Datenverarbeitung, Bonn, 1968

4. J.A. Brzozowski, Derivatives of regular expressions, J.Assoc.Comput.Mach. 11, (1964) 481-494

5 J.R. Büchi, Mathematische Theorie des Verhaltens endlicher

Automaten, Zeitschrift Angew.Math.Mech. 42, (1962) T9-T16

6. J.R. Büchi, Algebraic theory of feedback in discrete systems, Part I, in E.R. Caianiello (ed.) Automata Theory, Academic Press, New York, 1966, 70-101

7. W.M. Gluschkow, Ein weiterer Algorithmus zur Synthese abstrakter Automaten, Ukrain.Math.Journal 12, (1960) 147-156 (in russischer Sprache)

8. F. Hennie, Finite-State Models for Logical Machines, J. Wiley, New York, 1968

9. J. Hopcroft, J. Ullman, Introduction to Automata Theory, Languages and Computation, Addison-Wesley, Reading, 1979

10. K. Indermark, Zum Minimisierungsproblem bei nichtdeterministischen Automaten, Seminarbericht Institut f.Theorie d.Autom.u. Schaltnetzwerke 16, Gesellschaft f.Mathematik u.Datenverarbeitung, Bonn, 1969

11 K. Indermark, Zur Zustandsminimisierung nichtdeterministischer erkennender Automaten, Berichte d.Gesellschaft f.Mathematik u.Datenverarbeitung, Bonn, Nr. 33, (1970)

12. T. Kameda, P. Weiner, On the state minimization of nondeterministic finite automata, IEEE Trans.on Computers C-19, (1970) 617-627

13. J. Kim, State Minimization of Nondeterministic Machines, IBM T.J. Watson Research Center Yorktown Heights RC 4896, 1974

14 C.M.R. Kintala, D. Wotschke, Amounts of nondeterminism in finite automata, Acta Informatica 13 (1980) 199-204

15. O.B. Lupanow, Über den Vergleich zweier Typen endlicher Quellen, Probleme der Kybernetik Bd.6, 1966, 329-335 (Russisches Original 1963)

16. A.R. Meyer, M.J. Fischer, Economy of description by automata, grammars, and formal systems, Conference Record of 12th Annual Symposium on Switching and Automata Theory (SWAT) IEEE Comp. Soc., 1971, 188-191

17 B.G. Mirkin, On dual automata, Cybernetics 2,1 (1966) 6-9

F.R. Moore, Deterministic realization and simulation of nondeterministic automata, Ph.D.dissertation, Dept.of Electrical Engineering, Syracuse University, 1969

18. F.R. Moore, On the bounds for state-set size in the proofs of equivalence between deterministic, nondeterministic, and two-way finite automata, IEEE Trans.on Computers, TC-20, (1971) 1211-1214

19 A. Nerode, Linear automaton transformations, Proc.Amer.Mathem.Soc. 9, (1958) 541-544

20. G. Ott, On multipath automata I, Sperry Rand Res.Rep. SRRC-RR-64-69, 1969

21. M.A. Spivak, Ein Algorithmus zur abstrakten Synthese von Automaten für eine erweiterte Sprache der regulären Ereignisse, Iswest.Akad.Nauk SSSR, Techn.Kybernetik (1965) No. 1, 51-57 (in russischer Sprache - vgl. Mathematical Reviews 32, Nr. 5467)

22 M.A. Spivak, Die Entwicklung eines regulären Ausdrucks nach einer Basis und ihre Anwendungen, Dokl.Akad.Nauk SSSR 162, (1965) 520-522 (in russischer Sprache)

23. M.A. Spivak,A method of analysis of abstract automata using equations in the algebra of events, Cybernetics 1, (1965) 25-26

К главе 7

1. B.H.Barnes, A two-way automaton with fewer states than any equivalent one-way automaton, IEEE Trans. on Computers, TC-20, (1971) 474-475

2. J.Berstel, Séries rationelles, in: J.Berstel (Hrsgb.), Séries Formelles en Variables Non Commutatives et Applications, Actes de la cinquième Ecole de Printemps d'informatique théorique, mai 1977, LITP, ENSTA, Paris 1978, 5-22

3. V.G.Bodnarchuk, Automaten und Ereignisse, Ukrainische Mathem. Zeitschrift 14, (1962) 351-361 (in russischer Sprache - vgl. Mathem. Reviews 26, Nr. 3557)

4 O.L.Costich, A Medvedev characterization of sets recognized by generalized finite automata, Math.Systems Theory 6, (1972) 263-267

5 C.C.Elgot, Decision problems of finite automata design and related arithmetics, Trans.Amer.Math.Soc. 98, (1961) 21-51

6 M.Fliess, Sur certaines familles de séries formelles, Thèse Sci.Math. (doctorat d'état), Univ. Paris VII, 1973

7. St.J.Garland, D.C.Luckham, Program schemes, recursion schemes, and formal languages, J.Comp.Syst.Sci. 7, (1973) 119-160

8 J.I.Janow, Über logische Schemata von Algorithmen, Probleme der Kybernetik 1, (1962) 87-144 (Übersetzung aus dem Russischen, Original 1958)

9. B.G.Mirkin, The language of pseudoregular expressions, Cybernetics 2,6 (1966) 6-8

10. T.J.Ostrand, M.C.Paull, E.J.Weyuker, Parsing regular grammars with finite lookahead, Acta Inf. 16, (1981) 125-138

11. M.P.Schützenberger, On the definition of a family of automata, Inform. & Control 4, (1961) 245-270

12. J.C.Shepherdson, The reduction of two-way automata to one-way automata, IBM J.Research and Development 3, (1959) 198-200.

К главе 8

1. V.Amar, G.Putzolu, On a family of linear grammars, Inf. & Control 7 (1964) 283-291

2. J.Berstel, Transductions and Context-Free Languages, Teubner-Verlag, Stuttgart, 1979

3. M.Bird, The equivalence problem for deterministic two-tape automata, J.Comp.Syst.Sci. 7 (1973) 218-236

4. L.Boasson, M.Nivat, Sur diverses familles de langages fermées par transduction rationnelle, Acta Informatica 2 (1973) 180-188

5. K.H.Böhling, K.Indermark, Endliche Automaten I, Bibliograph.Institut, Mannheim, 1969

6. W.Brauer, W-automata and their language, in: A.Mazurkiewicz (ed.) Proceedings MFCS '76, LNCS 45, Springer-Verlag, Berlin (1976) 12-22

7. J.A.Brzozowski, Regular-like expressions for some irregular languages, IEEE Conf.Record 1968, Ninth Ann.Symp.on Switching and Automate Theory, Schenectady, N.Y. (1968) 278-286

8. K.Čulik, Some axiomatic systems for formal grammars and languages, in: Proceedings IFIP Congress 62, München 1962, North-Holland, Amsterdam, 1963, 134-137

9. K.Čulik, I.Havel, On multiple finite automata, in: W.Händler, E.Peschl, H.Unger, 3. Colloquium über Automatentheorie, Hannover 1965, Birkhäuser, Basel, 1967, 158-169

10. S.Eilenberg, C.C.Elgot, J.C.Shepherdson, Sets recognized by n-tape automata, J. Algebra 13 (1969) 447-464

11. C.C.Elgot, J.E.Mezei, On relations defined by generalized finite automata, IBM J. Develop. 9 (1965) 47-68

12. P.C.Fischer, A.L.Rosenberg, Multitape one-way non writing automata, J.Comp.Syst.Sci. 2 (1968) 88-101

13. S.Ginsburg, Examples of abstract machines, IRE Trans.Electron. Computers, EC11 (1962) 132-135

14. S.Ginsburg, The Mathematical Theory of Context-Free-Languages,

McGraw-Hill, New York, 1966

15. S.Ginsburg, Algebraic and Automata-Theoretic Properties of Formal Languages, North-Holland, Amsterdam, 1975

16 S.Ginsburg, S.A.Greibach, Abstract families of languages, in: S.Ginsburg, S.A.Greibach, J.E.Hopcroft (eds.) Studies in Abstract Families of Languages, Memoirs Amer.Math.Soc. 87 (1969) 1-32

17. S.Ginsburg, G.F.Rose, Operations which preserve definability in languages, J.Assoc.Comput.Mach. 10 (1963) 175-195

18. S.Ginsburg, G.F.Rose, A characterisation of machine mappings, Can.J.Math. 18 (1966) 381-388

19. T.V.Griffiths, The unsolvability of the equivalence problem for Λ-free nondeterministic generalized machines, J.Assoc.Comput.Mach. 15 (1968) 409-413

20. O.H.Ibarra, The unsolvability of the equivalence problem for ε-free NGSM's with unary input (output) alphabet and applications, in: Proc. 18th Ann.Symp.on Foundations of Computer Science (FOCS), IEEE, New York, 1977, 74-81

21. B.G.Mirkin, On the theory of multitape automata, Cybernatics 2,5 (1966) 9-14

22. M.Nivat, Transductions des langages de Chomsky, Thèse d'Etat, Univ.de Paris, 1967, und in: Ann. de l'Inst.Fourier, Grenoble 18 (1968) 339-456

23. A.L.Rosenberg, On n-tape finite state-acceptors, in: Proc. of Fifth Ann.Symp. on Switching Circuit Theory and Logical Design, IEEE Publ. S-164, 1964, 76-81

24. A.L.Rosenberg, Nonwriting Extensions of Finite Automata, Unpublished Doctoral Dissertation, Harvard Univ.Report BL-39, 1965

25. A.L.Rosenberg, On multi-head finite automata, IBM J.Res. Develop. 10 (1966) 388-394

26. A.L.Rosenberg, A machine realization of the linear context-free languages, Inf.& Control 10 (1967) 175-188

27. K.B.Salomon, The decidability of a mapping problem for generalized sequential machines with final states, J.Comp.Syst. Sci. 10 (1975) 200-218

28. H.Schnelle, CC-Automata and CF-Grammars, unveröffentlichtes Manuskript, Vortrag auf dem Colloquium on Algebraic Linguistics and Automata Theory, Jerusalem, 1964

29. C.-P.Schnorr, Freie assoziative Systeme, EIK 3 (1967), 319-340

30. M.P.Schützenberger, A remark on finite transducers, Inf.& Control 4 (1961) 185-196

31. P.H.Starke, On the representability of relations by deterministic and nondeterministic multi-tape automata, in: J.Bečvář (ed.) Proceeding MFCS '75 LNCS 32, Springer-Verlag, Berlin 1975, 114-124

32 P.H.Starke, Closedness properties and decision problems for finite multi-tape automata, Kybernetika, Praha 12 (1976) 61-75

33. S.J.Walljasper, Non-Deterministic Automata and Effective Languages, Ph.D.Thesis, Univ.of Iowa, AD-69 2421, 1969

34. G.Wechsung, Isomorphe Darstellungen der Kleeneschen Algebra der regulären Mengen, Mitt.Math.Ges. DDR, 1973, Nr.2/3, 161-171

СПИСОК РАБОТ СОВЕТСКИХ АВТОРОВ И РАБОТ, ПЕРЕВЕДЕННЫХ НА РУССКИЙ ЯЗЫК

1. **Блох А. Ш.** О задачах, решаемых последовательностными машинами// Проблемы кибернетики: Сб. статей/ Под ред. А. А. Ляпунова.—М, 1960.— Вып 3.—С. 81—88.

2. **Боднарчук В. Г.** Автоматы и события// Украинский математический журнал. — 1962.—Т. 14, № 4 —С. 351—361.

3. **Боднарчук В. Г.** Системы уравнений в алгебре событий// Журн вычисл. матем и матем. физ. — 1963.—Т. 3, № 6.—С. 1077—1088.

4. **Гилл А.** Введение в теорию конечных автоматов: Пер. с англ.—М.: Наука, 1966.—272 с.

5. **Гинзбург С.** Математическая теория контекстно-свободных языков: Пер. с англ. — М · Мир, 1970 —326 с

6 **Глушков В. М.** Абстрактная теория автоматов// Успехи матем наук — 1961.—Т. 16, № 5.—С. 3—62.

7. **Глушков В. М.** Некоторые проблемы синтеза цифровых автоматов// Журн. вычисл. матем. и матем. физ.—1961 —Т. 1, № 3.—С. 371—411.

8. **Глушков В. М.** Об одном алгоритме синтеза абстрактных автоматов// Украинский математический журнал — 1960 —Т. 12, № 2.—С. 147—156.

9 **Клини С. К.** Представление событий в нервных сетях и конечных автоматах// Автоматы: Пер с англ —М, 1956.—С 15—67.

10. **Курмит А. А.** Автоматы без потери информации конечного порядка — Рига.: Зинатне, 1972.—266 с

11. **Лупанов О. Б.** О сравнении двух типов конечных автоматов// Проблемы кибернетики: Сб. статей/ Под ред. А. А. Ляпунова. — М, 1963 —Вып. 9.— С 321—326.

12. **Мак-Нотон Р., Пейперт С.** Синтаксический моноид и регулярное событие// Алгебраическая теория автоматов, языков и полугрупп: Пер с англ — М, 1975.—С. 284—297.

13. **Медведев Ю. Т.** О классе событий, допускающих представление в конечном автомате// Автоматы. Пер. с англ. — М, 1956 —С. 385—401.

14 **Минский М.** Вычисления и автоматы: Пер. с англ —М.: Мир, 1971 — 364 с

15. **Миркин Б. Г.** О двойственных автоматах// Кибернетика — 1966.—№ 1 — С. 7—10.

16. **Миркин Б. Г.** О языке псевдорегулярных выражений// Кибернетика. — 1966.—№ 6.—С. 8—11.

17. **Мур Э. Ф.** Умозрительные эксперименты с последовательностными машинами// Автоматы: Пер. с англ.—М., 1956.—С. 179—212.
18. **Спивак М. А.** Алгоритм абстрактного синтеза автоматов для расширенного языка регулярных выражений// Изв. АН СССР. Сер. техн. кибернетика.— 1965.—№ 1.—С. 51—57.
19. **Спивак М. А.** К методу анализа абстрактных автоматов с помощью уравнений в алгебре событий// Кибернетика. — 1965.—№ 1.—С. 28.
20. **Спивак М. А.** К минимизации автомата Мура// Кибернетика. — 1967.— № 1.—С. 5, 6.
21. **Спивак М. А.** Разложение регулярного выражения по базису и его применения// Докл. АН СССР.—1965.—Т. 162, № 3.—С. 520—522.
22. **Хиббард Т. Н.** Точные верхние границы длин минимальных экспериментов, определяющих заключительное состояние, для двух классов последовательностных машин// Кибернетический сборник (новая серия): Сб. переводов/ Под ред. О. Б. Лупанова и А. А Ляпунова. — М., 1966.—Вып. 2.—С. 7—23.
23. **Янов Ю. И.** О логических схемах алгоритмов// Проблемы кибернетики: Сб. статей/ Под ред. А. А. Ляпунова. — М., 1958.—Вып. 1.— С. 75—127.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ОГЛАВЛЕНИЕ