Э. МЕНДЕЛЬСОН

Введение в математическую логику

Э. МЕНДЕЛЬСОН

Введение в математическую логику

Перевод с английского
Ф. А. КАБАКОВА

Под редакцией
С. И. АДЯНА

ИЗДАНИЕ ВТОРОЕ, ИСПРАВЛЕННОЕ

ИЗДАТЕЛЬСТВО «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1976

518
М 50
УДК 519.95

Introduction to Mathematical Logic

by
Elliott Mendelson

Associate Professor of Mathematics
Queens College
Flushing, New York

D. VAN NOSTRAND COMPANY, INC.

PRINCETON, NEW JERSEY
TORONTO NEW YORK LONDON

Эллиот Мендельсон
ВВЕДЕНИЕ В МАТЕМАТИЧЕСКУЮ ЛОГИКУ

М., 1976 г., 320 стр. с илл.

Редактор *В. В. Донченко*
Техн. редактор *А. П. Колесникова*
Корректор *Л. С. Сомова*

Печать с матриц. Подписано к печати 18/III 1976 г. Бумага 60×90¹/₁₆. Физ. печ. л. 20. Условн. печ. л. 20. Уч.- изд. л. 21,61. Тираж 33 000 экз. Цена книги 1 р. 65 к. Заказ 552.

Издательство «Наука»
Главная редакция физико-математической литературы
117071, Москва, В-71, Ленинский проспект, 15

Отпечатано во 2-й типографии изд-ва «Наука», Москва, Шубинский пер., 10, заказ 473, с матриц ордена Трудового Красного Знамени Ленинградского производственно-технического объединения «Печатный Двор» имени А. М. Горького Союзполиграфпрома при Государственном комитете Совета Министров СССР по делам издательств, полиграфии и книжной торговли. 197136, Ленинград, П-136, Гатчинская ул., 26.

М $\frac{20203-051}{053(02)-76}$ 50-76

Оглавление

От редактора перевода

В книге Э. Мендельсона «Введение в математическую логику» дается доступное для начинающего читателя и достаточно полное изложение основных разделов современной математической логики и многих ее приложений. Наряду с такими разделами, как логика высказываний, исчисление предикатов, формальная арифметика и теория алгоритмов, в ней освещены также теория моделей и аксиоматическая теория множеств, отсутствующие в книге С. К. Клини «Введение в метаматематику», которая до настоящего времени служила наиболее полным пособием по математической логике. Следует однако отметить, что в отличие от книги С. К. Клини в этой книге по существу не затрагиваются интуиционистское и конструктивное направления математической логики.

Изложение материала в книге ясное и лаконичное. Основной текст перемежается с большим числом примеров и упражнений. В упражнения автор вынес также некоторые результаты, используемые затем в основном тексте. Это, наряду с лаконичностью изложения, способствовало сокращению размеров книги при весьма обширном содержании.

Переводчик и редактор перевода позволили себе без специальных оговорок и примечаний исправить ряд неточностей и опечаток, имевшихся в оригинале, а также привести терминологию и обозначения в соответствие с принятыми в русской литературе.

Книгу Э. Мендельсона можно рекомендовать в качестве пособия не только студентам и аспирантам, специализирующимся по математической логике, но также всякому, кто захочет начать систематическое изучение этого предмета.

Во втором издании книги исправлены опечатки и отдельные погрешности, замеченные после выхода в свет первого издания. Редактор благодарен Н. М. Нагорному и А. Л. Семенову, указавшим на ряд неточностей, допущенных в первом издании книги.

С. И. Адян

Предисловие

В этой книге мы попытались представить сжатое введение в некоторые основные разделы математической логики. Чтобы дать полное и точное изложение основных и наиболее важных вопросов, мы опустили такие дополнительные темы, как модальная, комбинаторная и интуиционистская логики, а также некоторые интересные, но более специальные вопросы, как, например, степени рекурсивной неразрешимости.

Придерживаясь того мнения, что начинающим следует предлагать наиболее естественные и легкие доказательства, мы применяем самые непринужденные теоретико-множественные методы. Значение требования конструктивных доказательств может быть оценено только после известного опыта занятий математической логикой. В конце концов, если уж нам предстоит быть изгнанными из «канторова рая» (как назвал Гильберт неконструктивную теорию множеств), то по крайней мере мы должны знать, чего лишаемся.

Пять глав книги удобно распределить на два семестра, а для курса в один семестр вполне подойдут главы с 1 по 3 (при этом можно, если это потребуется для ускорения, опустить §§ 5 и 6 главы 1 и §§ 10—12 главы 2). Мы будем отмечать верхним индексом D упражнения, которые, вероятно, будут трудны для начинающего, и верхним индексом A — упражнения, предполагающие знакомство с материалом, недостаточно освещенным в тексте.

Настоящая книга представляет собой расширенное воспроизведение записей полугодового курса лекций по математической логике, читанного автором с 1958 по 1960 г. в Колумбийском университете, а в 1961 и 1962 гг. в Куинс колледже. Автор надеется, что эта книга может быть прочитана без особого труда всяким, кто имеет некоторый опыт абстрактного математического мышления; при этом каких-либо конкретных предварительных знаний не требуется. Автор хотел бы поблагодарить Дж. Баркли Россера за поддержку и руководство во время аспирантских занятий логикой, а также с признательностью отметить несомненное влияние, оказанное на него книгами Гильберта и Бернайса [1934, 1939], Клини [1952], Россера [1953] и Чёрча [1956].

Эллиот Мендельсон

Queens, New York,
Январь 1963

Введение

Согласно одному из самых распространенных определений, логика есть анализ методов рассуждений. Изучая эти методы, логика интересуется в первую очередь формой, а не содержанием доводов в том или ином рассуждении. Рассмотрим, например, следующие два вывода:

(1) Все люди смертны. Сократ—человек. Следовательно, Сократ смертен.

(2) Все кролики любят морковь. Себастьян — кролик. Следовательно, Себастьян любит морковь.

Оба эти вывода имеют одну и ту же форму: все A суть B; S есть A; следовательно, S есть B. Истинность или ложность отдельных посылок или заключений не интересует логика. Он желает лишь знать, вытекает ли истинность заключения из истинности посылок. Систематическая формализация и каталогизация правильных способов рассуждений — одна из основных задач логика. Если при этом логик применяет математический аппарат, и его исследования посвящены в первую очередь изучению математических рассуждений, то предмет его занятий может быть назван математической логикой. Мы можем сузить область математической логики, если скажем, что главная ее цель — дать точное и адекватное определение понятия «математическое доказательство».

Безупречные определения имеют малую ценность в начале изучения предмета. Лучший способ понять, что такое математическая логика, состоит в том, чтобы приняться за ее изучение. Мы рекомендуем студенту начать читать эту книгу, даже если (и в особенности если) он имеет сомнения относительно значения и целей предмета.

Хотя логика и является основой всех остальных наук, тем не менее присущее ей, наряду с фундаментальностью, свойство самоочевидности действовало расхолаживающе на стремление к сколько-нибудь глубоким логическим исследованиям вплоть до девятнадцатого столетия, когда интерес к логике оживился под влиянием открытия неевклидовых геометрий и стремления обеспечить строгое обоснование анализа. Этот новый интерес оставался все еще не столь жгучим до тех пор, пока на исходе столетия математический мир не был потрясен открытием парадоксов, т. е. рассуждений, приводящих к противоречиям. Наиболее важными из этих парадоксов являются следующие.

Логические парадоксы

(1) (Рассел, 1902). Под множеством мы понимаем всякое собрание каких-либо объектов. Примерами множеств являются множество всех

четных чисел, множество всех саксофонистов в Бруклине и т. д. Объекты, из которых состоит множество, называются его элементами. Множества сами могут быть элементами множеств, так, например, множество всех множеств целых чисел имеет своими элементами множества. Большинство множеств не являются элементами самих себя. Например, множество всех котов не является элементом самого себя, потому что оно само не кот. Возможны, однако, и такие множества, которые принадлежат самим себе как элементы, — например, множество всех множеств. Рассмотрим теперь множество A всех таких множеств X, что X не есть элемент X. Согласно определению, если A есть элемент A, то A также и не есть элемент A, и если A не есть элемент A, то A есть элемент A. В любом случае A есть элемент A и A не есть элемент A.

(2) (Кантор, 1899). Этот парадокс требует некоторых сведений из теории кардинальных чисел, и может быть опущен читателем, если он не знаком с этой теорией. Кардинальное число $\overline{\overline{Y}}$ множества Y определяется как множество всех множеств X, равномощных с множеством Y (т. е. таких X, для которых существует взаимно однозначное соответствие между Y и X, см. стр. 15). Мы определяем $\overline{\overline{Y}} \leqslant \overline{\overline{Z}}$ как условие равномощности Y с некоторым подмножеством множества Z, а $\overline{\overline{Y}} < \overline{\overline{Z}}$ — как $\overline{\overline{Y}} \leqslant \overline{\overline{Z}}$ и $\overline{\overline{Y}} \neq \overline{\overline{Z}}$. Кантор доказал, что если $\mathscr{P}(Y)$ есть множество всех подмножеств множества Y, то $\overline{\overline{Y}} < \overline{\overline{\mathscr{P}(Y)}}$ (см. стр. 202). Пусть C — универсальное множество, т. е. множество всех множеств. Так как $\mathscr{P}(C)$ есть подмножество множества C, то, очевидно, $\overline{\overline{\mathscr{P}(C)}} \leqslant \overline{\overline{C}}$. С другой стороны, по теореме Кантора $\overline{\overline{C}} < \overline{\overline{\mathscr{P}(C)}}$. Теорема же Шрёдера — Бернштейна (см. стр. 201) утверждает, что если $\overline{\overline{Y}} \leqslant \overline{\overline{Z}}$ и $\overline{\overline{Z}} \leqslant \overline{\overline{Y}}$, то $\overline{\overline{Y}} = \overline{\overline{Z}}$. Следовательно, $\overline{\overline{C}} = \overline{\overline{\mathscr{P}(C)}}$, что находится в противоречии с $\overline{\overline{C}} < \overline{\overline{\mathscr{P}(C)}}$.

(3) (Бурали-Форти, 1897). Этот парадокс аналогичен парадоксу Кантора. Он возникает в теории порядковых чисел и будет понятен только тому, кто уже знаком с теорией порядковых чисел. Для любого порядкового числа существует порядковое число, его превосходящее. Однако порядковое число, определяемое множеством всех порядковых чисел, является наибольшим порядковым числом.

Семантические парадоксы

(4) Парадокс лжеца. Некто говорит: «Я лгу». Если он при этом лжет, то сказанное им есть ложь, и, следовательно, он не лжет. Если же он при этом не лжет, то сказанное им есть истина, и, следовательно, он лжет. В любом случае оказывается, что он лжет и не лжет одновременно *).

*) С парадоксом лжеца имеет сходство известный еще в древности (см., например, «Послание к Титу св. апостола Павла», 1, 12) так называемый «парадокс критянина». Критский философ Эпименид сказал: «Все критяне — лжецы». Если то, что он сказал, верно, то, поскольку Эпименид сам критянин, сказанное

(5) (Ришар, 1905). С помощью некоторых фраз русского языка могут быть охарактеризованы те или иные вещественные числа. Например, фраза «отношение длины окружности к длине диаметра в круге» характеризует число π. Все фразы русского языка могут быть перенумерованы некоторым стандартным способом, а именно: упорядочим сперва лексикографически (т. е. как в словаре) все фразы, содержащие в точности k букв, а затем поместим все фразы из k букв впереди всех фраз с бóльшим числом букв. Теперь можно перенумеровать все те фразы русского языка, которые характеризуют то или иное вещественное число. Для этого достаточно в стандартной нумерации всех фраз опустить все остальные фразы. Число, получающее при такой нумерации номер n, назовем n-м числом Ришара. Рассмотрим такую фразу: «Вещественное число, у которого n-й десятичный знак равен 1, если у n-го числа Ришара n-й десятичный знак не равен 1, и n-й десятичный знак равен 2, если у n-го числа Ришара n-й десятичный знак равен 1». Эта фраза определяет некоторое число Ришара, допустим, k-е; однако, согласно определению, оно отличается от k-го числа Ришара в k-м десятичном знаке.

(6) (Берри, 1906). Существует лишь конечное число слогов в русском языке. Следовательно, имеется лишь конечное число таких фраз русского языка, которые содержат не более пятидесяти слогов. Поэтому с помощью таких фраз можно охарактеризовать только конечное число натуральных чисел. Пусть k есть *наименьшее из натуральных чисел, которые не характеризуются никакой фразой русского языка, содержащей не более пятидесяти слогов*. Напечатанная курсивом фраза характеризует число k и содержит не более пятидесяти слогов.

(7) (Греллинг, 1908). Прилагательное называется *автологическим*, если свойство, которое оно обозначает, присуще ему самому. Прилагательное называется *гетерологическим*, если свойство, которое оно обозначает, ему самому не присуще. Так, например, прилагательные «многосложный», «русский» являются автологическими, а прилагательные «односложный», «французский», «голубой» — гетерологическими. Рассмотрим прилагательное «гетерологический». Если это прилагательное гетерологично, то оно негетерологично, если же оно негетерологично, то оно гетерологично. Итак, в любом случае прилагательное «гетерологический» является гетерологическим и негетерологическим одновременно.

Все эти парадоксы являются подлинными в том смысле, что они не содержат явных логических изъянов. В логических парадоксах используются только понятия теории множеств, в то время как в парадоксах семантических применяются такие понятия, как «характеризовать»,

---

им есть ложь. Следовательно, то, что он сказал, есть ложь. Тогда должен быть такой критянин, который не лжет. Последнее не является логически невозможным, и мы здесь не имеем настоящего парадокса. Тем не менее тот факт, что произнесение Эпименидом этого ложного высказывания может повлечь за собой существование критянина, который не лжет, до некоторой степени обескураживает.

«истинный», «прилагательное», которое вовсе не обязаны появляться в обычном математическом языке. Ввиду этого логические парадоксы представляют собой куда бо́льшую угрозу спокойствию духа математиков, чем парадоксы семантические.

Анализ парадоксов привел к различным планам их устранения. Все эти планы предлагают тем или иным путем ограничивать «наивные» понятия, участвующие в выводе этих парадоксов. Рассел обратил внимание на то, что во всех этих парадоксах имеет место самоотнесение понятий. Он предложил снабдить каждый объект некоторым неотрицательным целым числом — «типом» этого объекта. После этого высказывание «x есть элемент множества y» должно считаться *осмысленным* тогда и только тогда, когда тип y на единицу больше типа x. Этот подход, систематически развитый Расселом и Уайтхедом [1910—1913] в так называемую теорию типов, приводит к цели, когда речь идет об устранении известных парадоксов *), однако он громоздок в практическом применении и имеет также некоторые другие недостатки. Другое острие критики логических парадоксов было нацелено на содержащееся в них допущение, состоящее в том, что для любого свойства $P(x)$ существует соответствующее множество всех элементов x, обладающих свойством $P(x)$. Стоит лишь отвергнуть это допущение, и логические парадоксы становятся невозможными **). Однако при этом необходимо принять некоторые новые постулаты для того, чтобы мы могли, опираясь на них, доказать существование таких множеств, в которых повседневно нуждаются практически работающие математики. Первая такая аксиоматическая теория множеств была построена Цермело [1908]. В главе 4 мы рассмотрим одну аксиоматическую теорию множеств, которая ведет свое происхождение от системы Цермело (с некоторыми изменениями, принадлежащими фон Нейману, Р. Робинсону, Бернайсу и Гёделю). Существуют также различные смешанные теории, соединяющие в себе те или иные черты теории типов и аксиоматической теории множеств; примером теории такого рода может служить система NF Куайна (см. Россер [1953]).

Более глубокое истолкование парадоксов было предпринято Брауэром и его интуиционистской школой (см. Гейтинг [1956]). Интуиционисты отказываются признавать универсальный характер некоторых основных законов логики таких, например, как закон исключенного третьего: *P или не P*. Этот закон, утверждают они, верен для конечных

*) Так, например, парадокс Рассела зависит от существования множества A всех множеств, которые не являются элементами самих себя. Так как, согласно теории типов, бессмысленно говорить о том, что какое-то множество принадлежит самому себе, то такого множества не может быть.

**) Парадокс Рассела в таком случае доказывает, что не существует множества A всех множеств, которые не принадлежат самим себе в качестве элемента, а парадоксы Кантора и Бурали-Форти показывают, что не существует универсального множества и не существует множества всех ординальных чисел. Семантические же парадоксы теперь не могут быть даже сформулированы, поскольку они включают в себя понятия, не выразимые внутри этой системы

множеств, но нет никаких оснований распространять его без всяких ограничений на все множества. Точно так же, говорят интуиционисты, необоснованным является заключение, что утверждение «существует объект x такой, что не $P(x)$» следует из утверждения «неверно, что для любого x $P(x)$». По их мнению, мы только тогда можем согласиться с утверждением существования объекта, обладающего тем или иным свойством, когда мы владеем методом построения (или отыскания) такого объекта. Разумеется, если мы подчинимся суровым интуиционистским требованиям, то парадоксы станут невыводимыми (или даже лишенными смысла), но, увы, в таком же положении тогда окажутся и многие столь любимые теоремы повседневной математики, и по этой причине интуиционизм нашел себе мало приверженцев среди математиков.

Какой бы мы, однако, не избрали подход к проблеме парадоксов, следует сперва исследовать язык логики и математики, чтобы разобраться в том, какие в ней могут быть употреблены символы, как из этих символов составляются термы, формулы, утверждения и доказательства, что может и что не может быть доказано, если исходить из тех или иных аксиом и правил вывода. В этом состоит одна из задач математической логики, и пока это не сделано, нет и базы для сопоставления соперничающих точек зрения на основания логики и математики. Глубокие и опустошительные результаты Гёделя, Тарского, Чёрча, Россера, Клини и многих других были богатой наградой за вложенный труд и завоевали для математической логики положение независимой ветви математики.

Для тех, кто является абсолютным новичком, мы теперь кратко изложим некоторые основные понятия и факты, используемые в книге. Впрочем, мы рекомендуем читателю опустить сейчас этот обзор и лишь обращаться к нему в дальнейшем по мере необходимости для справок.

Множество есть собрание объектов *). Объекты этого собрания называются *элементами* множества. Мы будем писать «$x \in y$» вместо утверждения, что «x есть элемент y». (В том же смысле мы будем понимать высказывания «x принадлежит y» и «y содержит x».) Отрицание утверждения «$x \in y$» будет обозначаться через «$x \notin y$».

Запись «$x \subseteq y$» означает, что каждый элемент множества x является также элементом множества y или, другими словами, что x есть *подмножество* y (или x *включено в* y). Желая выразить тот факт, что t и s обозначают один и тот же объект, мы будем писать «$t = s$».

*) Мы здесь не будем уточнять, какие собрания объектов являются множествами. Однако мы будем избегать употребления таких связанных с понятием множества идей и процедур, которые могут привести к парадоксам. Все излагаемые здесь результаты могут быть формализованы в аксиоматической теории множеств, рассмотренной в главе 4. Термин «класс» иногда употребляют как синоним термина «множество», но мы его здесь избегаем, поскольку он в главе 4 употребляется в другом значении. Если свойство $P(x)$ определяет некоторое множество, то это множество часто обозначают через $\{x \mid P(x)\}$ или $\hat{x}(P(x))$.

Как обычно, «$t \neq s$» означает отрицание «$t = s$». Для множеств x и y мы говорим, что $x = y$ в том и только в том случае, если $x \subseteq y$ и $y \subseteq x$, т. е. в том и только в том случае, если x и y имеют одни и те же элементы. Если $x \subseteq y$, но $x \neq y$, то мы говорим, что x есть *собственное* подмножество y, и пишем $x \subset y$.

Объединение $x \cup y$ множеств x и y определяется как множество всех объектов, являющихся элементами хотя бы одного из множеств x и y. Отсюда сразу следует, что $x \cup x = x$, $x \cup y = y \cup x$ и $(x \cup y) \cup z = x \cup (y \cup z)$. *Пересечение* $x \cap y$ есть множество элементов, принадлежащих и x и y. Нетрудно проверить, что $x \cap x = x$, $x \cap y = y \cap x$, $x \cap (y \cap z) = (x \cap y) \cap z$, $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$ и $x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$. *Относительным дополнением* $x - y$ называется множество тех элементов x, которые не являются элементами y. Мы постулируем также существование пустого множества 0, т. е. множества, которое вовсе не имеет элементов. Легко видеть, что $x \cap 0 = 0$, $x \cup 0 = x$, $x - 0 = x$, $x - x = 0$. Два множества x и y называются *непересекающимися*, если $x \cap y = 0$.

Пусть даны какие-нибудь объекты $b_1, \ldots, b_k$; множество, элементами которого являются все эти объекты и только они, обозначается через $\{b_1, \ldots, b_k\}$. В частности, $\{x, y\}$ есть множество с двумя элементами x и y; если при этом $x \neq y$, то $\{x, y\}$ называется *неупорядоченной парой* (или просто *парой*) объектов x и y. Множество $\{x, x\}$ обозначается также через $\{x\}$ и называется *одноэлементным множеством* с элементом x. Заметим, что $\{x, y\} = \{y, x\}$. Через $\langle b_1, \ldots, b_n \rangle$ мы обозначаем *упорядоченную n-ку объектов* $b_1, \ldots, b_n$. Основное свойство упорядоченных n-ок состоит в том, что $\langle b_1, \ldots, b_n \rangle = \langle c_1, \ldots, c_n \rangle$ тогда и только тогда, когда $b_1 = c_1, \ldots, b_n = c_n$. Так, в частности, $\langle b_1, b_2 \rangle = \langle b_2, b_1 \rangle$ в том и только в том случае, если $b_1 = b_2$. Упорядоченные двойки называются *упорядоченными парами*. Если X — множество и n — целое положительное число, то через X^n мы обозначаем множество всех упорядоченных n-ок $\langle b_1, \ldots, b_n \rangle$ элементов $b_1, \ldots, b_n$ множества X; при этом мы условимся под X^1 понимать X. X^n называется *n-кратным декартовым произведением X на себя* или *n-й декартовой степенью* множества X. Если Y и Z — множества, то $Y \times Z$ означает множество всех таких упорядоченных пар $\langle y, z \rangle$, что $y \in Y$ и $z \in Z$. $Y \times Z$ называется *декартовым произведением* множеств Y и Z.

Под *n-местным отношением* (*отношением с n аргументами*) на множестве X мы понимаем всякое подмножество множества X^n, т. е. всякое множество n-ок элементов X. Например, 3-местное отношение «между» для точек на прямой представляет собой множество всех троек $\langle x, y, z \rangle$ таких, что точка x лежит между точками y и z. Двуместное отношение называют также *бинарным* отношением; например, бинарное отношение отцовства на множестве всех людей есть множество всех упорядоченных пар $\langle x, y \rangle$ таких, что x и y — люди и x есть отец y. Одноместное отношение на X есть подмножество X и называется *свойством* на X.

Пусть R — бинарное отношение на множестве X. *Областью определения* R называется множество всех y таких, что $\langle y, z\rangle \in R$ хотя бы при одном z; *множеством значений* R называется множество всех z таких, что $\langle y, z\rangle \in R$ хотя бы при одном y; наконец, объединение области определения и множества значений R называется *полем* отношения R. Отношение R^{-1}, *обратное к* R, определяется как множество всех упорядоченных пар $\langle y, z\rangle$ таких, что $\langle z, y\rangle \in R$. Так, например, область определения отношения $<$ на множестве ω всех неотрицательных целых чисел есть ω, множеством значений этого отношения служит $\omega - \{0\}$, а обратным отношением является отношение $>$.

Замечание. Часто вместо $\langle x, y\rangle \in R$ пишут xRy. Так, в приведенном примере мы обычно пишем $x < y$ вместо $\langle x, y\rangle \in <$.

Бинарное отношение R называется *рефлексивным*, если xRx для любого x из поля отношения R, *симметричным*, если из xRy следует yRx, и *транзитивным*, если из xRy и yRz следует xRz. Например, отношение $\leqslant$ на множестве целых чисел рефлексивно и транзитивно, но не симметрично. Отношение «иметь по крайней мере одного общего родителя» на множестве людей рефлексивно и симметрично, но не транзитивно.

Бинарное рефлексивное, симметричное и транзитивное отношение называется *отношением эквивалентности*. Примеры отношений эквивалентности: (1) отношение *тождества* 1_X на произвольном множестве X, состоящее из всех пар $\langle y, y\rangle$, где $y \in X$; (2) отношение параллельности между прямыми в плоскости; (3) отношение $x \equiv y \pmod n$, означающее, что x и y целые и $x - y$ делится на данное фиксированное целое положительное число n; (4) отношение между прямолинейными направленными отрезками в трехмерном пространстве, имеющее место тогда и только тогда, когда отрезки имеют одинаковые направление и длину; (5) отношение конгруэнтности на множестве треугольников в плоскости; (6) отношение подобия на множестве треугольников в плоскости. Пусть дано отношение эквивалентности R на множестве X и некоторый элемент y множества X. Определим $[y]$ как множество всех таких z из X, для которых yRz. Множество $[y]$ называется *классом* R*-эквивалентности*, определяемым элементом y. Легко видеть, что $[y] = [z]$ тогда и только тогда, когда yRz, и если $[y] \neq [z]$, то $[y] \cap [z] = 0$, т. е. различные классы R-эквивалентности не имеют общих элементов. Таким образом, X полностью разбивается на классы R-эквивалентности В примере (1) классами эквивалентности являются одноэлементные множества $\{y\}$, где $y \in X$. В примере (2) классы эквивалентности могут рассматриваться как направления в данной плоскости. В примере (3) имеется n классов эквивалентности, k-й класс эквивалентности, ($k = 0, 1, \ldots, n-1$) состоит из всех тех чисел, которые при делении на n дают в остатке k. В (4) классы эквивалентности суть трехмерные векторы.

Бинарное отношение f называется *функцией*, если из $\langle x, y\rangle \in f$ и $\langle x, z\rangle \in f$ следует $y = z$. Для любого x из области определения

функции f существует единственный элемент y такой, что $\langle x, y\rangle \in f$; этот элемент y обозначается через $f(x)$. Если x принадлежит области определения f, то говорят, что $f(x)$ определено. Если f есть функция с областью определения X и множеством значений Y, то говорят, что f *отображает* X *на* Y. Если f отображает X на Y и $Y \subseteq Z$, то говорят, что f *отображает* X *в* Z. Например, если $f(x) = 2x$ для любого целого x, то мы можем сказать, что f отображает множество всех целых чисел на множество всех четных чисел и что f отображает множество всех целых чисел в множество всех целых чисел. Функция, область определения которой состоит из n-ок, называется функцией от n аргументов. (*Всюду определенной*) *функцией от* n *аргументов на множестве* X называется всякая функция, у которой область определения совпадает с X^n. Обычно вместо $f(\langle x_1, \ldots, x_n\rangle)$ мы пишем $f(x_1, \ldots, x_n)$. *Частичной функцией от* n *аргументов на множестве* X называется всякая функция, областью определения которой служит какое-нибудь подмножество X^n. Например, обычное деление является частичной, но не всюду определенной, функцией от двух аргументов на множестве целых чисел (поскольку деление на нуль не определено). Если f есть функция с областью определения X и множеством значений Y, то *ограничением* f_Z *функции* f *множеством* Z называется функция $f \cap (Z \times Y)$. Очевидно, $f_Z(u) = v$ тогда и только тогда, когда $u \in Z$ и $f(u) = v$. *Образом множества* Z *при отображении посредством функции* f называется множество значений функции f_Z. *Прообразом множества* W *при отображении посредством функции* f называется множество всех тех элементов u из области определения функции f, для которых $f(u) \in W$. Говорят что функция f *отображает* множество X на множество (в множество) Y, если X есть подмножество области определения f, а образом X при отображении посредством f является множество Y (подмножество множества Y). Под *n-местной операцией* (или *операцией с* n *аргументами*) *на множестве* X мы понимаем функцию, отображающую X^n в X. Например, обычное сложение является бинарной (т. е. двуместной) операцией на множестве натуральных чисел $\{0, 1, 2, \ldots\}$. Обычное вычитание не является бинарной операцией на множестве натуральных чисел, однако является бинарной операцией на множестве всех целых чисел.

Если f и g — функции, то композиция $f \circ g$ этих функций (иногда обозначаемая также через fg) есть, по определению, такая функция, что $(f \circ g)(x) = f(g(x))$; $(f \circ g)(x)$ определено тогда и только тогда, когда определены $g(x)$ и $f(g(x))$. Например, если $g(x) = x^2$ и $f(x) = x + 1$, то $(f \circ g)(x) = x^2 + 1$ и $(g \circ f)(x) = (x + 1)^2$. Или, например, если $g(x) = -x$ для каждого вещественного числа x, а $f(x) = \sqrt{x}$ для каждого неотрицательного вещественного x, то $(f \circ g)(x)$ определено только для $x \leqslant 0$ и $(f \circ g)(x) = \sqrt{-x}$. Функция f, для которой из $f(x) = f(y)$ следует $x = y$, называется *взаимно однозначной* функцией (или (1-1)-функцией).

Примеры. (1) Отношение тождества I_X на множестве X есть взаимно однозначная функция; (2) взаимно однозначной является функция $f(x)=2x$, где x — произвольное целое число; (3) функция $f(x)=x^2$, где x — произвольное целое число, не является взаимно однозначной, поскольку $f(-1)=f(1)$. Заметим, что функция f будет взаимно однозначной тогда и только тогда, когда обратное отношение f^{-1} есть функция. Если X есть область определения, а Y — множество значений взаимно однозначной функции f, то о функции f говорят, что она есть *взаимно однозначное соответствие* (или (1-1)-*соответствие*) *между множествами* X *и* Y; при этом f^{-1} оказывается взаимно однозначным соответствием между Y и X, $(f^{-1}\circ f)=I_X$ и $(f\circ f^{-1})=I_Y$. Если f есть взаимно однозначное соответствие между X и Y, а g есть взаимно однозначное соответствие между Y и Z, то $g\circ f$ есть взаимно однозначное соответствие между X и Z. Множества X и Y называются *равномощными* (сокращенно $X\simeq Y$), если существует взаимно однозначное соответствие между X и Y. Очевидно, $X\simeq X$, из $X\simeq Y$ следует $Y\simeq X$ и из $X\simeq Y$ и $Y\simeq Z$ следует $X\simeq Z$. Можно доказать (см. теорему Шрёдера — Бернштейна, стр. 201), что если $X\simeq Y_1\subseteq Y$ и $Y\simeq X_1\subseteq X$, то $X\simeq Y$. Если $X\simeq Y$, то иногда говорят, что X и Y *имеют одну и ту же мощность* (или, иначе, *имеют одно и то же кардинальное число*), а если X равномощно с некоторым подмножеством Y, но при этом Y не равномощно ни с каким подмножеством X, то говорят, что *мощность* (*кардинальное число*) X *меньше мощности* (*кардинального числа*) Y *).

Множество X называется *счетным*, если оно равномощно с множеством положительных целых чисел. Говорят также, что счетное множество имеет мощность $\aleph_0$, а всякое множество, равномощное с множеством всех подмножеств какого-нибудь счетного множества, имеет мощность $2^{\aleph_0}$ (или имеет *мощность континуума*). Множество называется *конечным*, если оно пустое или если оно равномощно с множеством всех целых положительных чисел $\{1, 2, \ldots, n\}$, не превосходящих какого-нибудь целого положительного числа n. Множество, не являющееся конечным, называется *бесконечным*. Множество называется *не более чем счетным*, если оно конечно или счетно. Очевидно, всякое подмножество счетного множества не более чем счетно. *Счетной последовательностью* называется всякая функция s, областью определения которой служит множество целых положительных чисел. Обычно вместо $s(n)$ пишут s_n. *Конечной последовательностью* называется всякая функция, для которой существует такое целое положительное n, что ее область определения совпадает с множеством $\{1, 2, \ldots, n\}$.

---

*) Мощность множества X можно определять как собрание $[X]$ всех множеств, равномощных с X. При этом в одних системах теории множеств такое $[X]$ может не существовать, в то время как в других системах (см. стр. 201—202) всегда существует, но может не являться множеством. Для кардинальных чисел $[X]$ и $[Y]$ отношение $[X]\leqslant[Y]$ может быть определено как утверждение того, что X равномощно с некоторым подмножеством Y.

Пусть $P(x, y_1, \ldots, y_k)$ — какое-нибудь отношение на множестве неотрицательных целых чисел. В частности, P может содержать только одну переменную x, т. е. оно может быть свойством. Если $P(0, y_1, \ldots, y_k)$ выполнено и для любого n из $P(n, y_1, \ldots, y_k)$ следует $P(n+1, y_1, \ldots, y_k)$, то $P(x, y_1, \ldots, y_k)$ выполнено для всех целых неотрицательных x (*принцип математической индукции*). При применении этого принципа для доказательства того, что при любом n из $P(n, y_1, \ldots, y_k)$ следует $P(n+1, y_1, \ldots, y_k)$, обычно допускают $P(n, y_1, \ldots, y_k)$ и затем выводят $P(n+1, y_1, \ldots, y_k)$; в таком выводе $P(n, y_1, \ldots, y_k)$ называется *индуктивным предположением*. Если отношение P содержит переменные $y_1, \ldots, y_k$, отличные от x, то говорят, что доказательство утверждения «при любом x $P(x)$» ведется *индукцией по* x. Такой же принцип индукции справедлив для множества целых чисел, бóльших заданного числа j.

Пример. Чтобы с помощью математической индукции доказать, что сумма первых n нечетных чисел, т. е. $1+3+5+\ldots+(2n-1)$, равна n^2, доказывают сначала, что $1=1^2$ (т. е. $P(1)$), а затем доказывают, что из $1+3+5+\ldots+(2n-1)=n^2$ следует $1+3+5+\ldots+(2n-1)+(2n+1)=(n+1)^2$ (т. е. что из $P(n)$ следует $P(n+1)$). Из принципа математической индукции можно вывести следующий *принцип полной индукции*: если для любого неотрицательного целого x из предположения, что $P(u, y_1, \ldots, y_k)$ верно при всех u, меньших x, следует верность $P(x, y_1, \ldots, y_k)$, то $P(x, y_1, \ldots, y_k)$ верно при всех неотрицательных целых x. (Упражнение. С помощью принципа полной индукции доказать, что каждое целое число, большее единицы, делится на некоторое простое число.)

Транзитивное бинарное отношение R, для которого xRx ложно при любом x из поля R, называется *частичным упорядочением*. (Если R есть частичное упорядочение, то отношение R', представляющее собой объединение R и множества всех упорядоченных пар $\langle x, x\rangle$, где x принадлежит полю R, называется *рефлексивным частичным упорядочением*; термин «частичное упорядочение» употребляется в литературе как в указанном выше смысле, так и в смысле рефлексивного частичного упорядочения. Заметим, что (xRy и yRx) невозможно, если R — частичное упорядочение. Если R — рефлексивное частичное упорядочение, то из (xRy и yRx) следует $x=y$.) (*Рефлексивным*) *полным упорядочением* (или просто *упорядочением*) называется такое (рефлексивное) частичное упорядочение, при котором для любых x и y из поля R либо $x=y$, либо xRy, либо yRx.

Примеры. (1) Отношение $<$ на множестве целых чисел является полным упорядочением, а отношение $\leqslant$ — рефлексивным полным упорядочением; (2) отношение $\subset$ на множестве всех подмножеств множества положительных целых чисел является частичным упорядочением, но не полным упорядочением, а отношение $\subseteq$ на том же множестве является рефлексивным частичным упорядочением, но не рефлексивным полным упорядочением. Пусть C — поле отношения R и B — подмножество C:

элемент y из B называется *R-наименьшим* (или *наименьшим относительно отношения R*) *элементом в B*, если для любого элемента z из B, отличного от y, справедливо yRz. Полное упорядочение называется *вполне упорядочением* (или *вполне упорядочивающим отношением*), если всякое непустое подмножество поля R имеет R-наименьший элемент.

Примеры. (1) Отношение $<$ на множестве неотрицательных целых чисел является вполне упорядочением; (2) отношение $<$ на множестве неотрицательных рациональных чисел является полным упорядочением, но не вполне упорядочением; (3) отношение $<$ на множестве всех целых чисел является полным упорядочением, но не вполне упорядочением. Каждому вполне упорядочению R с полем X соответствует следующий *принцип полной индукции*: если свойство P таково, что для любого элемента u множества X из того, что свойством P обладает всякий элемент z множества X, для которого zRu, следует, что u обладает свойством P, то свойством P обладают все элементы из X. Если множество X бесконечно, то доказательство, использующее этот принцип, называется доказательством *по трансфинитной индукции*. Говорят, что *множество X может быть вполне упорядочено*, если существует вполне упорядочение, поле которого включает X. В современной математике применяется допущение, носящее название *принципа вполне упорядочения*, согласно которому всякое множество может быть вполне упорядочено. По вопросу о законности этого принципа возникла, однако, серьезная полемика. Принцип вполне упорядочения эквивалентен (в обычной аксиоматике теории множеств) *аксиоме выбора* (*мультипликативной аксиоме*): каково бы ни было множество X непустых, попарно непересекающихся множеств, существует множество Y (называемое *множеством выбора*), которое содержит в точности по одному элементу из каждого множества, являющегося элементом X.

Пусть B — непустое множество, f — функция, отображающая B в B, и g — функция, отображающая B^2 в B. Условимся писать x' вместо $f(x)$ и $x \cap y$ вместо $g(x, y)$. Назовем теперь упорядоченную тройку $\langle B, f, g\rangle$ *булевой алгеброй*, если для любых x, y и z из B выполнены условия:

(i) $x \cap y = y \cap x$;

(ii) $x \cap (y \cap z) = (x \cap y) \cap z$;

(iii) $x \cap y' = z \cap z'$ тогда и только тогда, когда $x \cap y = x$.

Для $(x' \cap y')'$ введем обозначение $x \cup y$ и будем писать $x \leqslant y$ вместо $x \cap y = x$. Легко показать, что $z \cap z' = w \cap w'$ для любых w, z из B; будем обозначать значение $z \cap z'$ через 0. (Не следует смешивать введенные сейчас символы $\cap$, $\cup$, 0 с соответствующими символами, применяемыми в теории множеств.) Введем, наконец, символ 1 для обозначения $0'$. Мы теперь имеем: $z \cup z' = 1$ для любого z из B, $\leqslant$ является рефлексивным частичным упорядочением и $\langle B, f, \cup\rangle$ есть булева алгебра. *Идеалом* в $\langle B, f, g\rangle$ называется всякое непустое подмножество J множества B такое, что: (1) если $x \in J$ и $y \in J$, то $x \cup y \in J$, и (2) если $x \in J$ и $y \in B$, то $x \cap y \in J$. Очевидно, $\{0\}$ и B — идеалы. Всякий идеал,

отличный от B, называется *собственным идеалом*. Собственный идеал называется *максимальным идеалом*, если он не содержится ни в каком другом собственном идеале. Можно показать, что собственный идеал J является максимальным тогда и только тогда, когда для любого u из B либо $u \in J$, либо $u' \in J$. Из принципа вполне упорядочения (или из аксиомы выбора) вытекает, что каждая булева алгебра содержит максимальный идеал или, что эквивалентно, всякий собственный идеал включен в некоторый максимальный идеал.

Пример. Пусть B есть множество всех подмножеств некоторого множества X; для $Y \in B$ пусть $Y' = X - Y$, а для Y и Z из B пусть $Y \cap Z$ означает обычное теоретико-множественное пересечение множеств Y и Z. Тогда упорядоченная тройка $\langle B, ', \cap \rangle$ оказывается булевой алгеброй. Роль 0 в B играет пустое множество 0, а 1 есть X. Пусть u — произвольный элемент множества X и J_u — множество всех подмножеств X, которые не содержат u. Тогда J_u есть максимальный идеал. Более детальное изложение теории булевых алгебр см., например, у Сикорского [1960].

Глава 1

Исчисление высказываний

§ 1. Пропозициональные связки. Истинностные таблицы

Из высказываний путем соединения их различными способами можно составлять новые, более сложные высказывания. Мы будем рассматривать одни только *истинностно-функциональные* комбинации, в которых истинность или ложность новых высказываний определяется истинностью или ложностью составляющих высказываний.

Отрицание является одной из простейших операций над высказываниями. Хотя в разговорном языке то или иное высказывание может быть отрицаемо многими способами, мы здесь будем это делать одним способом, помещая знак отрицания $\neg$ перед всем высказыванием. Так, если A есть высказывание, то $\neg A$ обозначает отрицание A и читается «не A».

Истинностно-функциональный характер отрицания становится ясным из рассмотрения следующей *истинностной таблицы*:

A	$\neg A$
И	Л
Л	И

Когда A истинно, $\neg A$ ложно; когда A ложно, $\neg A$ истинно. Буквы И и Л мы употребляем для обозначения *истинностных значений*: «истина» и «ложь».

Другой распространенной истинностно-функциональной операцией является *конъюнкция*: «и». Конъюнкция высказываний A и B будет обозначаться через $A \& B$, она имеет следующую истинностную таблицу:

A	B	$A \& B$
И	И	И
Л	И	Л
И	Л	Л
Л	Л	Л

Высказывание $A \& B$ истинно тогда и только тогда, когда истинны оба высказывания A и B. Высказывания A и B называются *конъюнктивными членами* или *членами конъюнкции* $A \& B$. Заметим, что в истинностной таблице для конъюнкции имеются четыре строки соответственно числу возможных распределений истинностных значений для A и B.

В разговорных языках связка «или» употребляется в двух различных смыслах — разделительном и соединительном. В первом случае утверждение «A или B» означает, что утверждается одно и только одно из высказываний A и B, а во втором случае — хотя бы одно из этих высказываний. Для связки «или» в этом втором, соединительном смысле мы и введем специальный знак: $\vee$. Эта операция имеет следующую истинностную таблицу:

A	B	$A \vee B$
И	И	И
Л	И	И
И	Л	И
Л	Л	Л

Таким образом, $A \vee B$ ложно тогда и только тогда, когда и A и B ложны. Высказывание «$A \vee B$» называется *дизъюнкцией* с *дизъюнктивными членами* A и B.

Упражнение

Построить истинностную таблицу для «или» в разделительном смысле.

Другой важной истинностно-функциональной операцией является *следование*: «если A, то B». Смысл обычного употребления здесь неясен. Разумеется, высказывание «если A, то B» ложно, когда *посылка* A истинна, а *заключение* B ложно. Однако в других случаях, при обычном употреблении этой связки, мы не имеем вполне определенного истинностного значения. Неясно, например, истинными или ложными следует считать высказывания:

(1) Если $1 + 1 = 2$, то Париж есть столица Франции.
(2) Если $1 + 1 \neq 2$, то Париж есть столица Франции.
(3) Если $1 + 1 \neq 2$, то Рим есть столица Франции.

Смысл их неясен, поскольку мы привыкли к тому, что между посылкой и заключением имеется определенная (обычно причинная) связь. Мы условимся считать, что «если A, то B» ложно тогда и только тогда, когда истинно A и ложно B. Таким образом, высказывания (1) — (3) будут считаться истинными. Обозначим «если A, то B» через $A \supset B$. Это последнее выражение называется *импликацией*. Вот истинностная таблица для $\supset$:

A	B	$A \supset B$
И	И	И
Л	И	И
И	Л	Л
Л	Л	И

Такое уточнение смысла высказывания «если A, то B» не противоречит обычной практике, скорее даже ее расширяет *).

Известным оправданием приведенной истинностной таблицы для $\supset$ может служить наше желание, чтобы высказывание «если A и B, то B» было всегда истинным. Так, случай, когда A и B истинны, оправдывает первую строку в нашей истинностной таблице для $\supset$, поскольку «A и B» и B оба истинны. Если A ложно и B истинно, то «A и B» ложно, в то время как B истинно. Это соответствует второй строке таблицы. Наконец, если A ложно и B ложно, то «A и B» ложно и B ложно. Это дает нам четвертую строку таблицы. Еще больше уверенности в разумности нашего определения придает нам смысл таких предложений, как, например: «Для любого x, если x есть нечетное целое положительное число, то x^2 есть нечетное целое положительное число». Здесь утверждается, что для любого x предложение «если x есть нечетное целое положительное число, то x^2 есть нечетное целое положительное число» истинно. При этом мы, разумеется, не хотим рассматривать как контрпримеры к нашему общему утверждению случаи, когда x не есть нечетное целое положительное число. Это обеспечивается второй и четвертой строками нашей таблицы истинности. Наконец, каждый случай, когда x и x^2 суть нечетные целые положительные числа, подтверждает наше общее утверждение. Это соответствует первой строке нашей таблицы.

Обозначим выражение «A тогда и только тогда, когда B» через «$A \equiv B$». Такое выражение называется *эквивалентностью*. Очевидно, $A \equiv B$ истинно тогда и только тогда, когда A и B имеют одно и то же истинностное значение. Поэтому мы имеем следующую истинностную таблицу:

A	B	$A \equiv B$
И	И	И
Л	И	Л
И	Л	Л
Л	Л	И

*) Иногда встречается некоторое не истинностно-функциональное понимание высказывания «если A, то B», связанное с законами причинности. Высказывание «если этот кусок железа положен в воду в момент времени t, то железо растворится» рассматривается как ложное даже в том случае, если кусок железа не положен в воду в момент времени t, т. е. даже если посылка ложна. Другое не истинностно-функциональное употребление связки «если..., то...» имеет место в так называемых контрфактических условных предложениях, таких как содержательно ложное высказывание «если сэр Вальтер Скотт не написал ни одного романа, то не было гражданской войны в США». При истинностно-функциональном подходе это высказывание следовало бы признать истинным ввиду ложности посылки. К счастью, математика и логика не нуждаются в законах причинности и контрфактических условных предложениях. Подробнее об условных предложениях и других связках см. Куайн [1951].

Символы $\neg$, &, $\vee$, $\supset$, $\equiv$ будем называть *пропозициональными связками* *). Всякое высказывание, построенное при помощи этих связок, имеет некоторое истинностное значение, зависящее от истинностных значений составляющих высказываний.

Мы будем применять термин *пропозициональная форма* для выражений, построенных из *пропозициональных букв* A, B, C и т. д. с помощью пропозициональных связок. Точнее:

(1) Все пропозициональные буквы (заглавные буквы латинского алфавита) и такие же буквы с числовыми индексами **)) суть пропозициональные формы.

(2) Если $\mathscr{A}$ и $\mathscr{B}$ — пропозициональные формы, то $(\neg\mathscr{A})$, $(\mathscr{A}\ \&\ \mathscr{B})$, $(\mathscr{A}\vee\mathscr{B})$, $(\mathscr{A}\supset\mathscr{B})$ и $(\mathscr{A}\equiv\mathscr{B})$ — тоже пропозициональные формы.

(3) Только те выражения являются пропозициональными формами, для которых это следует из (1) и (2) ***).

Каждому распределению истинностных значений пропозициональных букв, входящих в ту или иную пропозициональную форму, соответствует, согласно истинностным таблицам для пропозициональных связок, некоторое истинностное значение этой пропозициональной формы.

Таким образом, всякая пропозициональная форма определяет некоторую истинностную функцию, которая графически может быть представлена истинностной таблицей для этой пропозициональной формы. Так, например, пропозициональная форма $(((\neg A)\vee B)\supset C)$ имеет следующую истинностную таблицу:

A	B	C	$(\neg A)$	$((\neg A)\vee B)$	$(((\neg A)\vee B)\supset C)$
И	И	И	Л	И	И
Л	И	И	И	И	И
И	Л	И	Л	Л	И
Л	Л	И	И	И	И
И	И	Л	Л	И	Л
Л	И	Л	И	И	Л
И	Л	Л	Л	Л	И
Л	Л	Л	И	И	Л

*) При введении новых терминов мы будем избегать применения кавычек, если это не будет вызывать недоразумений. Строго говоря, в данном предложении в кавычки следовало взять каждую связку (см. Куайн [1951], стр. 23—27).

**) Например A_1, A_2, A_{17}, B_{31}, C_2, ...

***) Иначе это определение можно сформулировать следующим образом: $\mathscr{C}$ есть пропозициональная форма тогда и только тогда, когда существует такая конечная последовательность $\mathscr{A}_1$, $\mathscr{A}_2$, ..., $\mathscr{A}_n$, что $\mathscr{A}_n=\mathscr{C}$ и для каждого i $(1\leqslant i\leqslant n)$ $\mathscr{A}_i$ является или буквой, или отрицанием, конъюнкцией, дизъюнкцией, импликацией или эквивалентностью предшествующих в этой последовательности выражений. Заметим, что рукописные латинские буквы $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ и т. д. употребляются нами для произвольных выражений, тогда как печатные латинские буквы применяются лишь как пропозициональные буквы.

Здесь каждая строка содержит некоторое распределение истинностных значений для букв A, B, C и соответствующие истинностные значения, принимаемые различными пропозициональными формами, которые возникают при построении формы $(((\neg A) \vee B) \supset C)$.

Для формы $((A \equiv B) \supset ((\neg A) \& B))$ истинностная таблица будет следующая:

A	B	$(A \equiv B)$	$(\neg A)$	$((\neg A) \& B)$	$((A \equiv B) \supset ((\neg A) \& B))$
И	И	И	Л	Л	Л
Л	И	Л	И	И	И
И	Л	Л	Л	Л	И
Л	Л	И	И	Л	Л

Если в пропозициональной форме имеется n различных букв, то тогда возможны 2^n различных распределений истинностных значений для букв и, следовательно, истинностная таблица для такой формы содержит 2^n строк.

Упражнение

Построить истинностные таблицы для пропозициональных форм $((A \supset B) \vee (\neg A))$ и $((A \supset (B \supset C)) \supset ((A \supset B) \supset (B \supset C)))$.

Составление истинностной таблицы можно сократить следующим образом. Выпишем форму, для которой надо составить истинностную таблицу. Для каждого распределения истинностных значений пропозициональных букв, входящих в данную форму, под всеми вхождениями каждой из этих букв подпишем соответствующее истинностное значение. Затем шаг за шагом под каждой пропозициональной связкой будем выписывать истинностные значения той составляющей пропозициональной формы, для которой эта связка — главная *). Например, для $((A \equiv B) \supset ((\neg A) \& B))$ мы получаем

$((A$	$\equiv$	$B)$	$\supset$	$((\neg$	$A)$	$\&$	$B))$
И	И	И	Л	Л	И	Л	И
Л	Л	И	И	И	Л	И	И
И	Л	Л	И	Л	И	Л	Л
Л	И	Л	Л	И	Л	Л	Л

Упражнения

1. Написать сокращенные истинностные таблицы для $((A \supset B) \& A)$ и $((A \vee (\neg C)) \equiv B)$.

2. Записать следующие высказывания в виде пропозициональных форм, употребляя пропозициональные буквы для обозначения атомарных

*) Главной связкой пропозициональной формы называется та связка, которая при построении формы применяется последней.

высказываний, т. е. таких высказываний, которые уже не построены из каких-либо других высказываний.

(a) Если мистер Джонс счастлив, то миссис Джонс несчастлива, и если мистер Джонс несчастлив, то миссис Джонс счастлива.

(b) Или Сэм пойдет на вечеринку, и Макс не пойдет на нее; или Сэм не пойдет на вечеринку, и Макс отлично проведет время.

(c) Необходимое и достаточное условие счастья для шейха состоит в том, чтобы иметь вино, женщин и услаждать свой слух пением.

(d) Фиорелло ходит в кино только в том случае, когда там показывают комедию.

(e) Для того чтобы x было нечетным, достаточно, чтобы x было простым.

(f) Необходимым условием сходимости последовательности s является ограниченность s.

(g) Взятку платят тогда и только тогда, когда товар доставлен.

(h) «Гиганты» выиграют приз, если «Хитрецы» сегодня не выиграют.

(i) Если x положительно, то x^2 положительно.

§ 2. Тавтологии

Истинностной функцией от n аргументов называется всякая функция от n аргументов, принимающая истинностные значения И или Л, если аргументы ее пробегают те же значения. Как мы видели, всякая пропозициональная форма определяет некоторую истинностную функцию *).

Пропозициональная форма, которая истинна независимо от того, какие значения принимают встречающиеся в ней пропозициональные буквы, называется *тавтологией.* Пропозициональная форма является тавтологией тогда и только тогда, когда соответствующая истинностная функция принимает только значение И, или, что то же, если в ее таб-

---

*) Для большей точности следовало бы пересчитать все пропозициональные буквы, например, в порядке $A, B, \ldots, Z, A_1, B_1, \ldots, Z_1, A_2, \ldots$ Если теперь некоторая пропозициональная форма содержит i_1-ю, ..., i_n-ю пропозициональные буквы из этого пересчета (где $i_1 < \ldots < i_n$), то соответствующая истинностная функция должна иметь своими аргументами $x_{i_1}, \ldots, x_{i_n}$ в том же порядке, при этом x_{i_j} соответствует i_j-й пропозициональной букве. Например, $(A \supset B)$ порождает истинностную функцию

x_1	x_2	$f(x_1, x_2)$
И	И	И
Л	И	И
И	Л	Л
Л	Л	И

в то время как $(B \supset A)$ порождает истинностную функцию

x_1	x_2	$f(x_1, x_2)$
И	И	И
Л	И	Л
И	Л	И
Л	Л	И

лице истинности столбец под самой пропозициональной формой состоит только из букв И. Если $(\mathscr{A} \supset \mathscr{B})$ является тавтологией, то говорят, что $\mathscr{A}$ *логически влечет* $\mathscr{B}$ или что $\mathscr{B}$ является *логическим следствием* $\mathscr{A}$ (в исчислении высказываний). Если $(\mathscr{A} \equiv \mathscr{B})$ есть тавтология, то говорят, что $\mathscr{A}$ и $\mathscr{B}$ *логически эквивалентны* (в исчислении высказываний) *). Примерами тавтологий являются $(A \vee (\neg A))$ («закон исключенного третьего»), $(\neg(A \& (\neg A)))$ и $(A \equiv (\neg(\neg A)))$. Отметим также, что $(A \& B)$ логически влечет A, $(A \& (A \supset B))$ логически влечет B, а $(A \supset B)$ и $((\neg A) \vee B)$ логически эквивалентны. Истинностные таблицы дают нам эффективную процедуру для решения вопроса о том, является ли данная пропозициональная форма тавтологией.

Упражнения

1. Определить, являются ли следующие пропозициональные формы тавтологиями:

(a) $(((A \supset B) \supset B) \supset B)$;

(b) $((A \equiv B) \equiv (A \equiv (B \equiv A)))$.

2. Доказать или опровергнуть:

(a) $(A \equiv B)$ логически влечет $(A \supset B)$;

(b) $((\neg A) \vee B)$ логически эквивалентно $((\neg B) \vee A)$.

3. Показать, что $\mathscr{A}$ и $\mathscr{B}$ логически эквивалентны тогда и только тогда, когда в соответствующих истинностных таблицах столбцы под $\mathscr{A}$ и под $\mathscr{B}$ совпадают.

Пропозициональная форма, которая ложна при всех возможных истинностных значениях ее пропозициональных букв, называется *противоречием.* Истинностная таблица для такой формы имеет в столбце под этой формой одни только буквы Л.

Пример. $(A \equiv (\neg A))$.

A	$\neg A$	$(A \equiv (\neg A))$
И	Л	Л
Л	И	Л

Другим примером противоречия является $(A \& (\neg A))$.

Заметим, что пропозициональная форма $\mathscr{A}$ является тавтологией тогда и только тогда, когда $(\neg \mathscr{A})$ есть противоречие.

Высказывание (в каком-нибудь естественном языке, вроде русского, или в какой-либо формальной теории **)), которое получается из какой-либо тавтологии посредством подстановки высказываний вместо пропозициональных букв, при условии, что вхождения одной и той же буквы

*) В дальнейшем в этой главе мы будем опускать участвующие в определениях слова «в исчислении высказываний».

**) Под формальной теорией мы понимаем всякий искусственный язык, в котором точно описываются понятия «осмысленного выражения», аксиомы и правила вывода; см. стр. 36 — 37.

замещаются одним и тем же высказыванием, называется *логически истинным* (в исчислении высказываний). О таком высказывании можно сказать, что оно истинно уже в силу одной только своей функционально-истинностной структуры. Примером может служить предложение русского языка «если идет дождь или идет снег, и не идет снег, то идет дождь», которое можно получить подстановкой в тавтологию $(((A \vee B) \& \& (\neg B)) \supset A)$. Высказывание, которое можно получить с помощью подстановки в противоречие, называется *логически ложным* (в исчислении высказываний).

Мы теперь установим несколько более общих фактов о тавтологиях.

Предложение 1.1. *Если* $\mathscr{A}$ *и* $(\mathscr{A} \supset \mathscr{B})$ *— тавтологии, то* $\mathscr{B}$ *— тавтология.*

Доказательство. Пусть $\mathscr{A}$ и $(\mathscr{A} \supset \mathscr{B})$ — тавтологии. Допустим, что при некотором распределении истинностных значений для пропозициональных букв, входящих в $\mathscr{A}$ и $\mathscr{B}$, $\mathscr{B}$ принимает значение Л. Поскольку $\mathscr{A}$ есть тавтология, то при том же распределении истинностных значений $\mathscr{A}$ принимает значение И. Тогда $(\mathscr{A} \supset \mathscr{B})$ получит значение Л. Это противоречит предположению о том, что $(\mathscr{A} \supset \mathscr{B})$ есть тавтология.

Предложение 1.2. *Если* $\mathscr{A}$ *есть тавтология, содержащая пропозициональные буквы* $A_1, A_2, \ldots, A_n$, *и* $\mathscr{B}$ *получается из* $\mathscr{A}$ *подстановкой в* $\mathscr{A}$ *пропозициональных форм* $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n$ *вместо* $A_1, A_2, \ldots, A_n$ *соответственно, то* $\mathscr{B}$ *есть тавтология, т. е. подстановка в тавтологию приводит к тавтологии.*

Доказательство. Предположим, что $\mathscr{A}$ есть тавтология, и пусть задано произвольное распределение истинностных значений для пропозициональных букв, входящих в $\mathscr{B}$. Формы $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n$ примут тогда некоторые значения $x_1, x_2, \ldots, x_n$ (каждое x_i есть И или Л); если мы придадим значения $x_1, x_2, \ldots, x_n$ соответственно буквам $A_1, A_2, \ldots, A_n$, то результирующее значение $\mathscr{A}$ совпадет с истинностным значением $\mathscr{B}$ при заданном распределении значений букв, входящих в $\mathscr{B}$. Так как $\mathscr{A}$ есть тавтология, то $\mathscr{B}$ при этом распределении значений своих аргументов примет значение И. Таким образом, $\mathscr{B}$ всегда принимает значение И.

Предложение 1.3. *Если* $\mathscr{B}_1$ *получается из* $\mathscr{A}_1$ *подстановкой* $\mathscr{B}$ *вместо одного или большего числа вхождений* $\mathscr{A}$, *то* $((\mathscr{A} \equiv \mathscr{B}) \supset \supset (\mathscr{A}_1 \equiv \mathscr{B}_1))$ *есть тавтология; и, следовательно, если* $\mathscr{A}$ *и* $\mathscr{B}$ *логически эквивалентны, то* $\mathscr{A}_1$ *и* $\mathscr{B}_1$ *тоже логически эквивалентны.*

Доказательство. Рассмотрим произвольное распределение истинностных значений для пропозициональных букв. Если $\mathscr{A}$ и $\mathscr{B}$ имеют при этом распределении противоположные значения, то $(\mathscr{A} \equiv \mathscr{B})$ принимает значение Л и тогда $((\mathscr{A} \equiv \mathscr{B}) \supset (\mathscr{A}_1 \equiv \mathscr{B}_1))$ принимает значение И. Если же $\mathscr{A}$ и $\mathscr{B}$ принимают одно и то же истинностное значение, то одинаковые истинностные значения примут также $\mathscr{A}_1$ и $\mathscr{B}_1$, поскольку $\mathscr{B}_1$ отличается от $\mathscr{A}_1$ тем только, что в некоторых местах вместо $\mathscr{A}$ содержит $\mathscr{B}$. Таким образом, в этом случае $(\mathscr{A} \equiv \mathscr{B})$ есть И, $(\mathscr{A}_1 \equiv \mathscr{B}_1)$ есть И, а потому и $((\mathscr{A} \equiv \mathscr{B}) \supset (\mathscr{A}_1 \equiv \mathscr{B}_1))$ есть И.

Введем некоторые соглашения о более экономном употреблении скобок в записях формул. Эти соглашения облегчат нам чтение сложных выражений. Во-первых, мы будем опускать в пропозициональной форме внешнюю пару скобок. (В случае пропозициональной буквы этой внешней пары скобок нет по определению.) Во-вторых, если форма содержит вхождения только одной бинарной связки (т. е. $\supset$, $\equiv$, $\vee$ или $\&$), то для каждого вхождения этой связки опускаются внешние скобки у той из двух форм, соединяемых этим вхождением, которая стоит слева.

Примеры. $A \supset B \supset A \supset C$ пишется вместо $(((A \supset B) \supset A) \supset C)$, а $B \vee B \vee A \vee (C \vee A)$ пишется вместо $(((B \vee B) \vee A) \vee (C \vee A))$.

В-третьих, договоримся считать связки упорядоченными следующим образом: $\equiv$, $\supset$, $\vee$, $\&$, $\neg$ и будем опускать во всякой пропозициональной форме все те пары скобок, без которых возможно восстановление этой формы на основе следующего правила. Каждое вхождение знака $\neg$ относится к наименьшей пропозициональной форме, следующей за ним; после расстановки всех скобок, относящихся ко всем вхождениям знака $\neg$, каждое вхождение знака $\&$ связывает наименьшие формы, окружающие это вхождение; затем (т. е. после расстановки всех скобок, относящихся ко всем вхождениям знаков $\neg$ и $\&$) каждое вхождение знака $\vee$ связывает наименьшие формы, окружающие это вхождение, и подобным же образом для $\supset$ и $\equiv$. При применении этого правила к одной и той же связке мы продвигаемся слева направо.

Примеры. В форме $A \vee \neg B \supset C \equiv A$ скобки восстанавливаются следующими шагами:

$$A \vee (\neg B) \supset C \equiv A$$
$$(A \vee (\neg B)) \supset C \equiv A$$
$$((A \vee (\neg B)) \supset C) \equiv A$$
$$(((A \vee (\neg B)) \supset C) \equiv A).$$

В качестве упражнения предлагается показать, что $D \equiv C \equiv A \,\&\, D \,\&\, B \vee \neg D \supset B$ обозначает

$$((D \equiv C) \equiv ((((A \,\&\, D) \,\&\, B) \vee (\neg D)) \supset B)).$$

Однако не всякая форма может быть записана без употребления скобок. Так, например, дальнейшее исключение скобок невозможно для форм $A \supset (B \supset C)$, $\neg(A \vee B)$, $A \,\&\, (B \supset C)$.

Упражнения

1. Исключить возможно большее число скобок в формах

$$((B \equiv ((\neg C) \vee (D \,\&\, A))) \equiv (B \supset B))$$

и

$$(((A \,\&\, (\neg B)) \,\&\, C) \vee D).$$

2. Восстановить скобки в формах $C \supset \neg(A \vee C) \,\&\, A \equiv B$ и $C \supset A \supset A \equiv \equiv \neg A \vee B$.

3. Если договориться писать $\neg\mathscr{A}$, $\&\,\mathscr{A}\mathscr{B}$, $\vee\,\mathscr{A}\mathscr{B}$, $\supset\mathscr{A}\mathscr{B}$ и $\equiv\mathscr{A}\mathscr{B}$ соответственно вместо $(\neg\mathscr{A})$, $(\mathscr{A}\,\&\,\mathscr{B})$, $(\mathscr{A}\vee\mathscr{B})$, $(\mathscr{A}\supset\mathscr{B})$ и $(\mathscr{A}\equiv\mathscr{B})$, то скобки не будут нужны. Например, форма $((\neg A)\supset(B\vee(\neg D)))$ запишется теперь как $\supset\neg A\vee B\,\neg D$. Предлагаем читателю записать по этой системе форму $(A\vee((B\,\&\,(\neg D))\supset A))$. Если каждую из связок $\supset$, $\&$, $\vee$, $\equiv$ оценить числом $+1$, каждую пропозициональную букву — числом -1, а связку $\neg$ — нулем, то в этой бесскобочной системе записи произвольное выражение $\mathscr{A}$ будет пропозициональной формой тогда и только тогда, когда сумма оценок всех вхождений символов в $\mathscr{A}$ равна -1 и сумма оценок всех символов каждого собственного начального отрезка $\mathscr{A}$ неотрицательна.

4. Определить, является ли каждая из следующих форм тавтологией, противоречием или ни тем и ни другим:

(a) $A\equiv(A\vee A)$;
(b) $(A\supset B)\supset((B\supset C)\supset(A\supset C))$;
(c) $((A\supset B)\,\&\,B)\supset A$;
(d) $(\neg A)\supset(A\,\&\,B)$;
(e) $A\,\&\,(\neg(A\vee B))$;
(f) $(A\supset B)\equiv((\neg A)\vee B)$;
(g) $(A\supset B)\equiv\neg(A\,\&\,(\neg B))$.

5. Доказать, что если $\mathscr{A}\,\&\,\mathscr{B}$ есть тавтология, то тавтологиями являются $\mathscr{A}$ и $\mathscr{B}$, и что если $\mathscr{A}$ есть тавтология, то $\mathscr{A}\vee\mathscr{B}$ и $\mathscr{B}\vee\mathscr{A}$ суть тавтологии.

6. Применить предложение 1.2 для случая, когда $\mathscr{A}$ есть $(A_1\,\&\,A_2)\supset A_1$, $\mathscr{A}_1$ есть $B\,\&\,D$ и $\mathscr{A}_2$ есть $\neg B$.

7. Доказать, что каждая из перечисленных пар состоит из логически эквивалентных форм:

(a) $\neg(A\vee B)$ и $(\neg A)\,\&\,(\neg B)$;
(b) $\neg(A\,\&\,B)$ и $(\neg A)\vee(\neg B)$;
(c) $A\,\&\,(B\vee C)$ и $(A\,\&\,B)\vee(A\,\&\,C)$;
(d) $A\vee(B\,\&\,C)$ и $(A\vee B)\,\&\,(A\vee C)$;
(e) $A\vee(A\,\&\,B)$ и A;
(f) $A\supset B$ и $\neg B\supset\neg A$ (форма $\neg B\supset\neg A$ называется *контрапозицией* формы $A\supset B$);
(g) $(A\,\&\,B)\vee(\neg B)$ и $A\vee(\neg B)$;
(h) $A\,\&\,(A\vee B)$ и A;
(i) $A\,\&\,B$ и $B\,\&\,A$;
(j) $A\vee B$ и $B\vee A$;
(k) $(A\,\&\,B)\,\&\,C$ и $A\,\&\,(B\,\&\,C)$;
(l) $(A\vee B)\vee C$ и $A\vee(B\vee C)$;
(m) $A\equiv B$ и $B\equiv A$;
(n) $(A\equiv B)\equiv C$ и $A\equiv(B\equiv C)$.

8. (Принцип двойственности.)

(a) Пусть $\mathscr{A}$ есть пропозициональная форма, содержащая только связки $\neg$, $\&$ и $\vee$, а форма $\mathscr{A}'$ получается из $\mathscr{A}$ заменой в ней всюду $\&$ на $\vee$ и $\vee$ на $\&$; доказать, что $\mathscr{A}$ является тавтологией тогда и только тогда, когда тавтологией является $\neg\mathscr{A}'$. Отсюда далее: если $\mathscr{A}\supset\mathscr{B}$ — тавтология, то и $\mathscr{B}'\supset\mathscr{A}'$ — тавтология, и если $\mathscr{A}\equiv\mathscr{B}$ — тавтология, то тавтологией является и $\mathscr{A}'\equiv\mathscr{B}'$. (Указание. Использовать 7 (a) и 7 (b).)

(b) Вывести 7 (b) из 7 (a) и 7 (d) из 7 (c).

(c) Пусть $\mathscr{A}$ — пропозициональная форма, содержащая только связки $\neg$, &, $\vee$, а форма $\mathscr{A}^*$ получается из $\mathscr{A}$ заменой в $\mathscr{A}$ всюду & на $\vee$ и обратно и каждой пропозициональной буквы ее отрицанием; показать, что форме $\mathscr{A}^*$ логически эквивалентна форма $\neg\mathscr{A}$. Форма $\mathscr{A}^*$ называется *двойственной* форме $\mathscr{A}$. Найти пропозициональную форму, двойственную форме

$$(A \vee \neg B) \& A \& (\neg C \vee (A \& C)).$$

9. Пропозициональная форма, содержащая только связку $\equiv$, является тавтологической тогда и только тогда, когда всякая пропозициональная буква входит в нее четное число раз.

10. (Шеннон [1938], Хон [1960])*). Электрическая цепь, содержащая только двухпозиционные переключатели (при одном состоянии переключателя ток через него проходит, при другом — не проходит), может быть представлена с помощью диаграммы, на которой возле каждого переключателя пишется буква, истинностное значение которой (И или Л) соответствует прохождению или непрохождению тока через этот переключатель. Например, условие, при котором ток идет через контур, изображенный на рис. 1, может быть выражено с помощью пропозициональной формы $(A \& B) \vee (C \& \neg A)$. Форма $(A \& B) \vee (((C \vee A) \& \neg B)$ представляет цепь, изображенную на рис. 2.

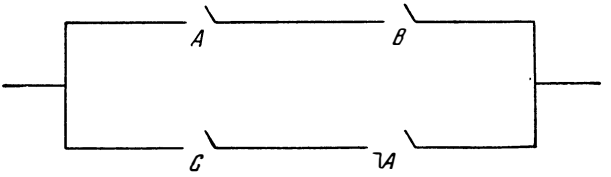


Рис. 1.

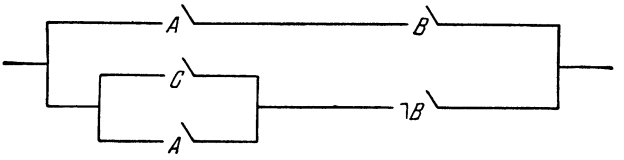


Рис. 2.

Применив упражнение 7 (d), (e), (g), (j), (l), мы можем убедиться в том, что эта последняя форма логически эквивалентна формам $((A \& B) \vee (C \vee A)) \& ((A \& B) \vee \neg B)$, $(((A \& B) \vee A) \vee C) \& (A \& \neg B)$, $(A \vee C) \& (A \vee \neg B)$ и, наконец, форме $A \vee (C \& \neg B)$. Таким образом, сеть, изображенная на рис. 2,

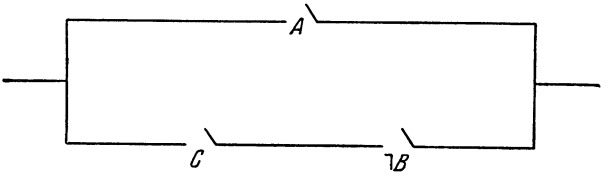


Рис. 3.

эквивалентна более простой сети, изображенной на рис. 3. (Две сети называются эквивалентными, если через одну из них ток идет тогда и только тогда, когда он идет через другую; из двух сетей та считается более простой, которая содержит меньшее число переключателей.)

*) См. также Шестаков [1941], Яблонский [1958].

(a) Для цепей, изображенных на рис. 4, 5, 6, построить эквивалентные им более простые цепи.

(b) Пусть каждый из трех членов комитета голосует «за», нажимая на кнопку. Построить по возможности более простую электрическую цепь, через которую ток проходил бы тогда и только тогда, когда не менее двух членов комитета голосуют «за».

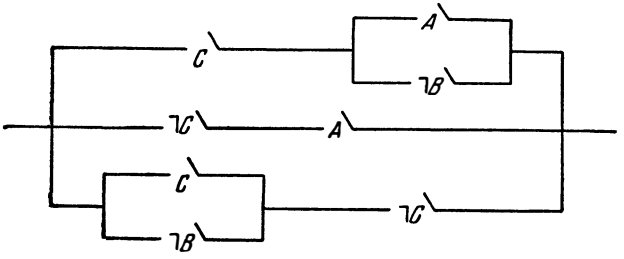


Рис. 4.

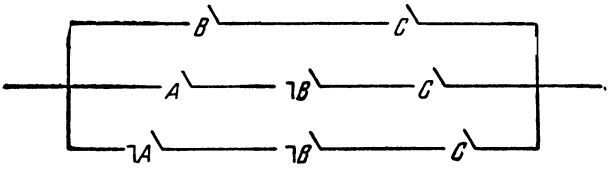


Рис. 5.

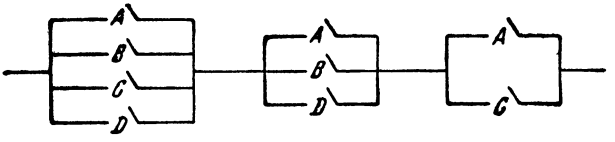


Рис. 6.

(c) Требуется, чтобы включение света в комнате осуществлялось с помощью трех различных переключателей таким образом, чтобы нажатие на любой из них приводило к включению света, если он перед этим был выключен, и к его выключению, если он был включен. Построить простую цепь, удовлетворяющую такому заданию.

11. Выяснить, являются ли следующие рассуждения логически правильными; для этого представить каждое предложение в виде пропозициональной формы и проверить, является ли заключение логическим следствием конъюнкции посылок.

(a) Если Джонс — коммунист, то Джонс — атеист. Джонс — атеист. Следовательно, Джонс — коммунист.

(b) Если строить противоатомные убежища, то другие государства будут чувствовать себя в опасности, а наш народ получит ложное представление о своей безопасности. Если другие страны будут чувствовать себя в опасности, то они смогут начать превентивную войну. Если наш народ получит ложное представление о своей безопасности, то он ослабит свои усилия, направленные на сохранение мира. Если же не строить противоатомные убежища, то мы

рискуем иметь колоссальные потери в случае войны. Следовательно, либо другие страны могут начать превентивную войну, и наш народ ослабит свои усилия, направленные на сохранение мира, либо мы рискуем иметь колоссальные потери в случае войны.

(c) Если Джонс не встречал этой ночью Смита, то либо Смит был убийцей, либо Джонс лжет. Если Смит не был убийцей, то Джонс не встречал Смита этой ночью, и убийство имело место после полуночи. Если убийство имело место после полуночи, то либо Смит был убийцей, либо Джонс лжет. Следовательно, Смит был убийцей.

(d) Если капиталовложения останутся постоянными, то возрастут правительственные расходы или возникнет безработица. Если правительственные расходы не возрастут, то налоги будут снижены. Если налоги будут снижены и капиталовложения останутся постоянными, то безработица не возникнет. Следовательно, правительственные расходы возрастут.

12. Проверить совместность каждого из множеств утверждений. Для этого представить предложения в виде пропозициональных форм и затем проверить, является ли их конъюнкция противоречием.

(a) Либо свидетель не был запуган, либо, если Генри покончил жизнь самоубийством, то записка была найдена. Если свидетель был запуган, то Генри не покончил жизнь самоубийством. Если записка была найдена, то Генри покончил жизнь самоубийством.

(b) Если вечер скучен, то или Алиса начинает плакать, или Анатоль рассказывает смешные истории. Если Сильвестр приходит на вечер, то или вечер скучен, или Алиса начинает плакать. Если Анатоль рассказывает смешные истории, то Алиса не начинает плакать. Сильвестр приходит на вечер тогда и только тогда, когда Анатоль не рассказывает смешные истории. Если Алиса начинает плакать, то Анатоль рассказывает смешные истории.

(c) Если курс ценных бумаг растет или процентная ставка снижается, то либо падает курс акций, либо налоги не повышаются. Курс акций понижается тогда и только тогда, когда растет курс ценных бумаг и налоги растут. Если процентная ставка снижается, то либо курс акций не понижается, либо курс ценных бумаг не растет. Либо повышаются налоги, либо курс акций понижается и снижается процентная ставка.

§ 3. Полные системы связок

Всякая пропозициональная форма, содержащая n пропозициональных букв, порождает соответствующую истинностную функцию от n аргументов. Значениями этих аргументов и функции являются И («истина») или Л («ложь»). Логически эквивалентные формы порождают одну и ту же функцию. Естественно возникает вопрос: все ли истинностные функции порождаются таким образом.

Предложение 1.4. *Всякая истинностная функция порождается некоторой пропозициональной формой, содержащей связки* $\neg$, $\&$ *и* $\vee$.

Доказательство. Пусть $f(x_1, \ldots, x_n)$ — данная истинностная функция. Очевидно, f может быть представлена некоторой истинностной таблицей с 2^n строками, где каждая строка содержит некоторое распределение истинностных значений для переменных $x_1, \ldots, x_n$ и соответствующее значение $f(x_1, \ldots, x_n)$. Занумеруем строки этой таблицы натуральными числами 1, 2, 3, ..., 2^n. Пусть для каждого i при $1 \leqslant i \leqslant 2^n$ C_i означает конъюнкцию $U_1^i \& \ldots \& U_n^i$, где U_j^i есть A_j, если

в i-й строке истинностной таблицы x_j принимает значение И, и U_j^i есть $\neg A_j$, если x_j принимает значение Л. Обозначим через D дизъюнкцию всех C_i таких, что функция f в i-й строке истинностной таблицы получает значение И. (Если таких строк нет, то f всегда принимает значение Л, и тогда нашей теореме удовлетворяет форма $A_1 \& \neg A_1$.) Истинностная функция, определяемая формой D, совпадает с f. В самом деле, пусть дано какое-нибудь распределение истинностных значений для пропозициональных букв $A_1, \ldots, A_n$, и предположим, что в истинностной таблице для f это распределение истинностных значений для $x_1, \ldots, x_n$ представлено в k-й строке. C_k имеет при этом распределении значение И, тогда как все остальные C_i имеют значение Л. Если для k-й строки f имеет значение И, то C_k является дизъюнктивным членом D и, следовательно, при этом распределении D тоже имеет значение И. Если для k-й строки f принимает значение Л, то C_k не является дизъюнктивным членом D и для рассматриваемого распределения все дизъюнктивные члены D принимают значение Л, а следовательно, и D принимает значение Л. Итак, порождаемая формой D истинностная функция есть f.

Примеры.

(a)

x_1	x_2	$f(x_1, x_2)$
И	И	Л
Л	И	И
И	Л	И
Л	Л	И

Искомой формой D является форма

$$(\neg A_1 \& A_2) \vee (A_1 \& \neg A_2) \vee (\neg A_1 \& \neg A_2).$$

(b)

x_1	x_2	x_3	$g(x_1, x_2, x_3)$
И	И	И	И
Л	И	И	Л
И	Л	И	И
Л	Л	И	И
И	И	Л	Л
Л	И	Л	Л
И	Л	Л	Л
Л	Л	Л	И

Искомой формой D является форма $(A_1 \& A_2 \& A_3) \vee (A_1 \& \neg A_2 \& A_3) \vee$ $\vee (\neg A_1 \& \neg A_2 \& A_3) \vee (\neg A_1 \& \neg A_2 \& \neg A_3)$.

Упражнение

Найти пропозициональную форму, содержащую только связки $\neg$, & и $\vee$, которая имеет следующую истинностную функцию $f(x_1, x_2, x_3)$:

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
И	И	И	И
Л	И	И	И
И	Л	И	Л
Л	Л	И	Л
И	И	Л	Л
Л	И	Л	Л
И	Л	Л	Л
Л	Л	Л	И

Следствие 1.5. *Для любой из следующих трех пар связок* & *и* $\neg$, $\vee$ *и* $\neg$, $\supset$ *и* $\neg$ *и для любой истинностной функции* f *существует пропозициональная форма, содержащая связки только из заданной пары и порождающая* f.

Доказательство. Заметим, что $A \vee B$ логически эквивалентно $\neg(\neg A \,\&\, \neg B)$. Следовательно, в силу второй части предложения 1.3, всякая пропозициональная форма, содержащая только связки &, $\vee$, $\neg$, логически эквивалентна некоторой пропозициональной форме, содержащей только связки & и $\neg$ (получаемой заменой всех выражений $\mathscr{A} \vee \mathscr{B}$ на $\neg(\neg\mathscr{A} \,\&\, \neg\mathscr{B})$). Остальные части доказываемого следствия подобным же образом следуют из тавтологий:

$$A \,\&\, B \equiv \neg(\neg A \vee \neg B),$$
$$A \vee B \equiv (\neg A) \supset B,$$
$$A \,\&\, B \equiv \neg(A \supset \neg B).$$

Мы только что видели, что существуют пары связок, например $\neg$ и &, через которые могут быть выражены (в смысле следствия 1.5) все истинностные функции. Оказывается, что того же эффекта можно добиться и с помощью одной связки $\downarrow$ (конъюнкция отрицаний), которая задается истинностной таблицей

A	B	$A \downarrow B$
И	И	Л
Л	И	Л
И	Л	Л
Л	Л	И

$A \downarrow B$ истинно тогда и только тогда, когда не истинно A и не истинно B. Нетрудно видеть, что формы $\neg A \equiv (A \downarrow A)$ и $(A \,\&\, B) \equiv ((A \downarrow A) \downarrow (B \downarrow B))$ суть тавтологии, и потому, в силу следствия 1.5, одной связки $\downarrow$ достаточно для построения всех истинностных функций.

Другой связкой, также достаточной для этой цели, является связка $|$ (дизъюнкция отрицаний или штрих Шеффера) с истинностной таблицей

A	B	$A\|B$
И	И	Л
Л	И	И
И	Л	И
Л	Л	И

$A|B$ истинно тогда и только тогда, когда неверно, что A и B оба истинны. Достаточность связки $|$ следует из тавтологий $\neg A \equiv (A|A)$ и $(A \vee B) \equiv ((A|A)|(B|B))$.

Предложение 1.6. *Единственными бинарными связками, каждой из которых достаточно для построения всех истинностных функций, являются связки* $\downarrow$ *и* $|$.

Доказательство. Предположим, что $\mathrm{h}(A, B)$ является достаточной в указанном смысле связкой. Если бы h (И, И) было И, то любая пропозициональная форма, построенная с помощью только лишь h, принимала бы значение И, когда все входящие в нее пропозициональные буквы принимают значение И. Следовательно, форма $\neg A$ не могла бы быть выражена только через h. Итак, h (И, И) $=$ Л. Аналогично получаем, что h (Л, Л) $=$ И. Таким образом, мы имеем таблицу

A	B	$\mathrm{h}(A, B)$
И	И	Л
Л	И	
И	Л	
Л	Л	И

Если второе и третье места в столбце значений h этой таблицы заняты соответственно значениями И, И или Л, Л, то мы получаем связку $|$ или связку $\downarrow$. Если же на этих местах стоит Л, И или И, Л, то формы $\mathrm{h}(A, B) \equiv \neg B$ и соответственно $\mathrm{h}(A, B) \equiv \neg A$ оказываются тавтологиями. В обоих случаях функция h выражена через $\neg$. Однако связка $\neg$ не является достаточной в рассматриваемом смысле, поскольку единственными истинностными функциями от одной переменной, которые могут быть выражены через $\neg$, являются функция, тождественно равная самой переменной, и отрицание переменной, а, например, функция, тождественно равная И, невыразима через отрицание.

Упражнения

1. Доказать, что каждая из пар связок $\supset$, $\vee$ и $\neg$, $\equiv$ не является достаточной для выражения любой истинностной функции.

2. Пропозициональная форма называется *дизъюнктивной нормальной формой*, если она является дизъюнкцией, состоящей из одного или более дизъюнк-

тивных членов, каждый из которых является конъюнкцией одной или нескольких пропозициональных букв или их отрицаний, например: $(A \& B) \vee (\neg A \& C)$, $A \& B$, $(A \& B \& \neg A) \vee (C \& \neg B) \vee (A \& \neg C)$, A, $A \vee (A \& B)$. Форма называется *конъюнктивной нормальной формой*, если она является конъюнкцией одного или более конъюнктивных членов, каждый из которых является дизъюнкцией одной или нескольких пропозициональных букв или их отрицаний. Заметим, что пропозициональную букву и ее отрицание мы рассматриваем как (вырожденную) дизъюнкцию или конъюнкцию. Доказательство предложения 1.4 фактически является доказательством того, что всякая пропозициональная форма логически эквивалентна некоторой дизъюнктивной нормальной форме. Применяя этот результат к $\neg \mathscr{A}$, доказать, что $\mathscr{A}$ логически эквивалентно также и некоторой конъюнктивной нормальной форме.

3. Найти конъюнктивную и дизъюнктивную нормальные формы, логически эквивалентные формам

$$(A \supset B) \vee (\neg A \& C) \text{ и } A \equiv (B \& \neg A).$$

Указание. Часто вместо того, чтобы использовать конструкцию из доказательства предложения 1.4, бывает удобнее применить упражнение 7 на стр. 28. В самом деле, пусть, например, дана форма $((A \supset \neg B) \& C) \vee (\neg A \equiv C)$. Чтобы получить конъюнктивную нормальную форму, исключим сначала $\supset$ и $\equiv$: $((\neg A \vee \neg B) \& C) \vee ((A \vee C) \& (\neg C \vee \neg A))$. Затем, в силу упражнения 7 (d), мы получаем $(\neg A \vee \neg B \vee A \vee C) \& (\neg A \vee \neg B \vee \neg C \vee \neg A) \& (C \vee A \vee C) \& (C \vee \neg C \vee \neg A)$, что логически эквивалентно конъюнктивной нормальной форме $(\neg A \vee \neg B \vee \neg C) \& (C \vee A)$. Чтобы получить дизъюнктивную нормальную форму, мы тоже сначала исключим $\supset$ и $\equiv$: $((\neg A \vee \neg B) \& C) \vee ((\neg A \& C) \vee (A \& \neg C))$, а затем, в силу упражнения 7 (c), получаем $(\neg A \& C) \vee (\neg B \& C) \vee (\neg A \& C) \vee (A \& \neg C)$, что логически эквивалентно дизъюнктивной нормальной форме $(\neg A \& C) \vee (\neg B \& C) \vee (A \& \neg C)$.

4. Пропозициональную букву A и ее отрицание $\neg A$ будем называть *литералами* буквы A. Дизъюнктивная (конъюнктивная) нормальная форма называется *совершенной*, если никакой ее дизъюнктивный член (конъюнктивный член) не содержит двух вхождений литералов одной и той же буквы и если всякая буква, входящая в один из дизъюнктивных членов (конъюнктивных членов), входит и во все остальные. Например, дизъюнктивные нормальные формы $(A \& A \& B) \vee (A \& B)$, $(A \& B) \vee A$, $(A \& \neg A \& B) \vee (A \& B)$ не являются совершенными, а формы $(A \& \neg B) \vee (A \& B)$ и $(A \& B \& \neg C) \vee (A \& B \& C) \vee (A \& \neg B \& \neg C)$ являются совершенными дизъюнктивными нормальными формами. Найти совершенные дизъюнктивную и конъюнктивную нормальные формы, логически эквивалентные формам $A \equiv (B \& \neg A)$ и $(A \supset B) \vee (\neg A \& C)$. Доказать, что всякая непротиворечивая (нетавтологическая) пропозициональная форма $\mathscr{A}$ логически эквивалентна некоторой совершенной дизъюнктивной (конъюнктивной) нормальной форме $\mathscr{F}$ и что если $\mathscr{F}$ содержит в точности n букв, то $\mathscr{A}$ является тавтологией (противоречием) тогда и только тогда, когда $\mathscr{F}$ состоит из 2^n дизъюнктивных (конъюнктивных) членов.

5. Некая страна населена жителями, каждый из которых либо всегда говорит правду, либо всегда лжет и которые отвечают на вопросы только посредством «да» или «нет». К развилке дорог, из которых одна ведет в столицу, а другая туда не приводит, приходит турист. Никаких знаков, указывающих, какую дорогу следует выбрать, при развилке нет. Зато здесь стоит местный житель, некто господин Р. Какой вопрос, требующий ответа «да» или «нет», должен задать ему турист, чтобы выбрать нужную ему дорогу?

Указание. Пусть A обозначает высказывание «господин Р всегда говорит правду», а B обозначает высказывание «дорога, идущая налево, ведет в столицу». С помощью подходящей истинностной таблицы построить такую пропозициональную форму, содержащую A и B, чтобы ответ местного жителя на вопрос, истинна ли эта пропозициональная форма, гласил «да» тогда и только тогда, когда B истинно.

§ 4. Система аксиом для исчисления высказываний

Истинностные таблицы позволяют ответить на многие важные вопросы, касающиеся истинностно-функциональных связок, в том числе такие, как вопрос о том, является ли данная пропозициональная форма тавтологией, противоречием или ни тем и ни другим, влечет ли она логически другую данную пропозициональную форму или являются ли две формы логически эквивалентными друг другу.

Более сложные вопросы логики, которыми мы в дальнейшем займемся, уже не могут быть решены с помощью истинностных таблиц или с помощью каких-либо других подобных эффективных процедур. Поэтому нами будет рассмотрен другой метод — метод формальных теорий. Хотя, как мы видели, все основные вопросы, возникающие в логике высказываний, могут быть решены методом истинностных таблиц, поучительно будет проиллюстрировать аксиоматический метод и на этой простой ветви логики.

Формальная (*аксиоматическая*) *теория* $\mathscr{S}$ считается определенной, если выполнены следующие условия:

(1) Задано некоторое счетное множество символов — символов теории $\mathscr{S}$ *). Конечные последовательности символов теории $\mathscr{S}$ называются *выражениями* теории $\mathscr{S}$.

(2) Имеется подмножество выражений теории $\mathscr{S}$, называемых *формулами* теории $\mathscr{S}$. (Обычно имеется эффективная процедура, позволяющая по данному выражению определить, является ли оно формулой.)

(3) Выделено некоторое множество формул, называемых *аксиомами* теории $\mathscr{S}$. (Чаще всего имеется возможность эффективно выяснять, является ли данная формула теории $\mathscr{S}$ аксиомой; в таком случае $\mathscr{S}$ называется эффективно *аксиоматизированной*, или *аксиоматической* теорией.)

(4) Имеется конечное множество $R_1, \ldots, R_n$ отношений между формулами, называемых правилами вывода. Для каждого R_i существует целое положительное j такое, что для каждого множества, состоящего из j формул, и для каждой формулы $\mathscr{A}$ эффективно решается вопрос о том, находятся ли данные j формул в отношении R_i с формулой $\mathscr{A}$, и если да, то $\mathscr{A}$ называется *непосредственным следствием* данных j формул по правилу R_i.

Выводом в $\mathscr{S}$ называется всякая последовательность $\mathscr{A}_1, \ldots, \mathscr{A}_n$ формул такая, что для любого i формула $\mathscr{A}_i$ есть либо аксиома теории $\mathscr{S}$, либо непосредственное следствие каких-либо предыдущих формул по одному из правил вывода.

Формула $\mathscr{A}$ теории $\mathscr{S}$ называется *теоремой* теории $\mathscr{S}$, если существует вывод в $\mathscr{S}$, в котором последней формулой является $\mathscr{A}$; такой вывод называется *выводом формулы* $\mathscr{A}$.

---

*) В качестве таких символов могут браться произвольные, а вовсе не обязательно лингвистические объекты.

Даже в случае эффективно аксиоматизированной теории $\mathscr{S}$, т. е. когда имеется эффективная процедура для определения, является ли данная формула аксиомой, понятие теоремы не обязательно эффективно, ибо, вообще говоря, может и не существовать эффективной процедуры (алгоритма), позволяющей узнавать по данной формуле, существует ли ее вывод в $\mathscr{S}$. Теория, для которой такой алгоритм существует, называется *разрешимой*, в противном случае теория называется *неразрешимой*. Грубо говоря, разрешимая теория — это такая теория, для которой можно изобрести машину, испытывающую формулы на свойство быть теоремой этой теории, в то время как для выполнения той же задачи в неразрешимой теории требуются все новые и новые независимые акты изобретательства.

Формула $\mathscr{A}$ называется *следствием* множества формул Γ в $\mathscr{S}$ тогда и только тогда, когда существует такая последовательность формул $\mathscr{A}_1, \ldots, \mathscr{A}_n$, что $\mathscr{A}_n$ есть $\mathscr{A}$, и для любого i $\mathscr{A}_i$ есть либо аксиома, либо элемент Γ, либо непосредственное следствие некоторых предыдущих формул по одному из правил вывода. Такая последовательность называется *выводом $\mathscr{A}$ из Γ*. Члены Γ называются *гипотезами* или *посылками вывода*. Для сокращения утверждения «$\mathscr{A}$ есть следствие Γ» мы будем употреблять запись $\Gamma \vdash \mathscr{A}$. Чтобы избежать путаницы там, где будут рассматриваться не одна, а несколько теорий, мы будем употреблять запись $\Gamma \vdash_{\mathscr{S}} \mathscr{A}$, указывая индексом $\mathscr{S}$ на то, о какой теории идет речь. Если множество Γ конечно: $\Gamma = \{\mathscr{B}_1, \ldots, \mathscr{B}_n\}$, то вместо $\{\mathscr{B}_1, \ldots, \mathscr{B}_n\} \vdash \mathscr{A}$ мы будем писать $\mathscr{B}_1, \ldots, \mathscr{B}_n \vdash \mathscr{A}$. Если Γ есть пустое множество 0, то $\Gamma \vdash A$ имеет место тогда и только тогда, когда $\mathscr{A}$ является теоремой. Вместо $0 \vdash \mathscr{A}$ принято писать просто $\vdash \mathscr{A}$. Таким образом, $\vdash \mathscr{A}$ служит сокращением утверждения «$\mathscr{A}$ есть теорема».

Приведем несколько простых свойств понятия выводимости из посылок.

(1) Если $\Gamma \subseteq \Delta$ и $\Gamma \vdash \mathscr{A}$, то $\Delta \vdash \mathscr{A}$.

(2) $\Gamma \vdash \mathscr{A}$ тогда и только тогда, когда в Γ существует конечное подмножество Δ, для которого $\Delta \vdash \mathscr{A}$.

(3) Если $\Delta \vdash \mathscr{A}$ и $\Gamma \vdash \mathscr{B}$ для любого $\mathscr{B}$ из множества Δ, то $\Gamma \vdash \mathscr{A}$.

Свойство (1) выражает тот факт, что если $\mathscr{A}$ выводимо из множества посылок Γ, то оно останется выводимым, если мы добавим к Γ новые посылки. Часть «тогда» утверждения (2) вытекает из (1). Часть «только тогда» этого утверждения становится очевидной, если мы вспомним, что всякий вывод $\mathscr{A}$ из Γ использует лишь конечное число посылок из Γ. Весьма прост и смысл утверждения (3): если $\mathscr{A}$ выводимо из Δ и каждая содержащаяся в Δ формула выводима из Γ, то $\mathscr{A}$ выводимо из Γ

Мы введем теперь формальную аксиоматическую теорию L для исчисления высказываний.

(1) Символами L являются $\neg$, $\supset$, (,) и буквы A_i с целыми положительными числами в качестве индексов: $A_1, A_2, A_3, \ldots$ Символы $\neg$ и $\supset$

называются *примитивными связками*, а буквы A_i — ***пропозициональными буквами.***

(2) (a) Все пропозициональные буквы суть формулы.

(b) Если $\mathscr{A}$ и $\mathscr{B}$ — формулы, то $(\neg\mathscr{A})$ и $(\mathscr{A}\supset\mathscr{B})$ — тоже формулы *). Таким образом, всякая формула теории L есть попросту пропозициональная форма, построенная из пропозициональных букв A_i с помощью связок $\neg$ и $\supset$.

(3) Каковы бы ни были формулы $\mathscr{A}$, $\mathscr{B}$ и $\mathscr{C}$ теории L, следующие формулы суть аксиомы L:

(A1) $(\mathscr{A}\supset(\mathscr{B}\supset\mathscr{A}))$;

(A2) $((\mathscr{A}\supset(\mathscr{B}\supset\mathscr{C}))\supset((\mathscr{A}\supset\mathscr{B})\supset(\mathscr{A}\supset\mathscr{C})))$;

(A3) $((\neg\mathscr{B}\supset\neg\mathscr{A})\supset((\neg\mathscr{B}\supset\mathscr{A})\supset\mathscr{B}))$.

(4) Единственным правилом вывода служит правило modus ponens: $\mathscr{B}$ есть непосредственное следствие $\mathscr{A}$ и $\mathscr{A}\supset\mathscr{B}$. Это правило будем сокращенно обозначать через MP.

Мы будем придерживаться наших соглашений относительно исключения скобок.

Отметим, что бесконечное множество аксиом теории L задано с помощью всего лишь трех *схем аксиом* (A1), (A2), (A3), каждая из которых порождает бесконечное множество аксиом. Для любой формулы легко проверить, является ли она аксиомой, и, таким образом, L есть эффективно аксиоматизированная теория. Мы ставим своей целью построить систему L таким образом, чтобы класс всех ее теорем совпадал с классом всех тавтологий.

Введем остальные связки с помощью следующих определений:

(D1) $(\mathscr{A}\,\&\,\mathscr{B})$ означает $\neg(\mathscr{A}\supset\neg\mathscr{B})$;

(D2) $(\mathscr{A}\vee\mathscr{B})$ означает $(\neg\mathscr{A})\supset\mathscr{B}$;

(D3) $(\mathscr{A}\equiv\mathscr{B})$ означает $(\mathscr{A}\supset\mathscr{B})\,\&\,(\mathscr{B}\supset\mathscr{A})$.

Смысл определения (D1), например, состоит в том, что, каковы бы ни были формулы $\mathscr{A}$ и $\mathscr{B}$, $(\mathscr{A}\,\&\,\mathscr{B})$ служит обозначением для $\neg(\mathscr{A}\supset\neg\mathscr{B})$ **).

---

*) Для большей точности мы должны были бы добавить еще так называемый заключительный пункт: (c) Выражение является формулой тогда и только тогда, когда это может быть установлено с помощью пунктов (a) и (b). Это определение можно сделать строгим, взяв за образец определение из примечания ***) на стр. 22.

**) Когда мы говорим, что $(\mathscr{A}\,\&\,\mathscr{B})$ служит обозначением для $\neg(\mathscr{A}\supset\neg\mathscr{B})$, мы под этим понимаем, что $(\mathscr{A}\,\&\,\mathscr{B})$ выбирается в качестве нового названия в русском языке (или в любом другом языке $\mathscr{L}$, на котором, быть может, случится говорить о теории L) для выражения $\neg(\mathscr{A}\supset\neg\mathscr{B})$. Заметим, что в качестве названия выражения, построенного посредством приписывания рядом каких-либо других выражений, мы употребляем выражения из русского языка (или языка $\mathscr{L}$), построенные с помощью приписывания рядом названий этих других выражений; при этом мы употребляем скобки и связки как их собст-

Лемма 1.7. $\vdash_L \mathscr{A} \supset \mathscr{A}$ *для любой формулы* $\mathscr{A}$.

Доказательство*). Построим вывод формулы $\mathscr{A} \supset \mathscr{A}$ в L.

(1) $(\mathscr{A} \supset ((\mathscr{A} \supset \mathscr{A}) \supset \mathscr{A})) \supset ((\mathscr{A} \supset (\mathscr{A} \supset \mathscr{A})) \supset (\mathscr{A} \supset \mathscr{A}))$
(подстановка в схему аксиом (A2))

(2) $\mathscr{A} \supset ((\mathscr{A} \supset \mathscr{A}) \supset \mathscr{A})$ (схема аксиом (A1))

(3) $(\mathscr{A} \supset (\mathscr{A} \supset \mathscr{A})) \supset (\mathscr{A} \supset \mathscr{A})$ (из (1), (2) по MP)

(4) $\mathscr{A} \supset (\mathscr{A} \supset \mathscr{A})$ (схема аксиом (A1))

(5) $\mathscr{A} \supset \mathscr{A}$ (из (3), (4) по MP)

венные названия, исключая, разумеется, те случаи, когда это может привести к недоразумению. Например, если $\mathscr{A}$ есть название выражения $(A_1 \supset A_2)$ и $\mathscr{B}$ есть название выражения $(\neg A_1)$, то $(\mathscr{A} \supset \mathscr{B})$ мы применяем как название выражения $((A_1 \supset A_2) \supset (\neg A_1))$. Эти соглашения представляются совершенно естественными и не замечаются большинством людей, если явно на них не указано. За дальнейшими разъяснениями по этому вопросу мы отсылаем читателя к обсуждению квазиобозначений у Куайна (Куайн [1951]) и автонимных символов у Карнапа (Карнап [1934], §§ 4 и 42); см. также Россер [1953], гл. III; Саппс [1957], глава 6; Чёрч [1956], введение и стр. 69—71.

*) Слово «proof» употребляется в двух различных смыслах. Во-первых, оно употребляется в некотором, определенном выше, точном смысле, как название для специального вида конечных последовательностей формул теории L («вывод в L»). В другом смысле оно означает последовательность предложений английского языка (дополненного различными техническими терминами), о которой предполагается, что она служит обосновывающей аргументацией в пользу того или иного утверждения о теории L (или какой-нибудь другой формальной теории). Вообще язык, который мы изучаем (в данном случае язык L), называется *языком-объектом*, а язык, на котором мы формулируем и доказываем различные результаты об этом языке-объекте, называется *метаязыком*. Этот метаязык сам мог бы быть формализован и стать предметом исследования, которое в свою очередь проводилось бы в некотором метаязыке, и т. д. Хотя для существенной части этой книги используется лишь некая математически узкая часть английского языка, мы тем не менее будем рассматривать английский язык как наш (неформализованный) метаязык. Разница между языком-объектом и метаязыком хорошо видна при изучении иностранных языков; например, на уроке немецкого языка этот последний является языком-объектом, а язык, на котором ведется преподавание, является метаязыком. Различию между «выводом в языке-объекте» и «доказательством в метаязыке» соответствует различие между теоремой языка-объекта и *метатеоремой* метаязыка. Во избежание недоразумений мы обычно вместо слова «метатеорема» употребляем слово «предложение». Слово «метаматематика» употребляется как название исследований логических и математических языков-объектов; иногда употребление этого слова ограничивается областью исследований, использующих только такие методы, которые квалифицируются метаматематиками как конструктивные (или так называемые *финитные*) методы.

[Переводя это примечание автора, мы сохранили непереведенным слово «proof» в первой фразе, а также не сделали обычной замены слов «английский язык» словами «русский язык» (в соответствующих падежах). Дело в том, что два различных смысла слова «proof», о которых говорится в этом примечании, в русской литературе выражаются обычно с помощью двух различных терминов: «вывод» и «доказательство». Такой терминологией мы и пользуемся всюду в переводе книги. (*Прим. перев.*)]

Упражнение

Доказать (построив вывод):

1. $\vdash_L (\neg \mathscr{A} \supset \mathscr{A}) \supset \mathscr{A}$.
2. $\mathscr{A} \supset \mathscr{B}, \mathscr{B} \supset \mathscr{C} \vdash_L \mathscr{A} \supset \mathscr{C}$.
3. $\mathscr{A} \supset (\mathscr{B} \supset \mathscr{C}) \vdash_L \mathscr{B} \supset (\mathscr{A} \supset \mathscr{C})$.
4. $\vdash_L (\neg \mathscr{B} \supset \neg \mathscr{A}) \supset (\mathscr{A} \supset \mathscr{B})$.

В математических рассуждениях часто какое-нибудь утверждение $\mathscr{B}$ доказывают в предположении верности другого утверждения $\mathscr{A}$, после чего заключают, что верно утверждение «если $\mathscr{A}$, то $\mathscr{B}$». Для системы L этот прием обосновывается следующей теоремой.

Предложение 1.8*). (Теорема дедукции.) *Если* Γ *— множество формул,* $\mathscr{A}$ *и* $\mathscr{B}$ *— формулы и* $\Gamma, \mathscr{A} \vdash \mathscr{B}$, *то* $\Gamma \vdash \mathscr{A} \supset \mathscr{B}$. *В частности, если* $\mathscr{A} \vdash \mathscr{B}$, *то* $\vdash \mathscr{A} \supset \mathscr{B}$ (Эрбран [1930]).

Доказательство. Пусть $\mathscr{B}_1, \ldots, \mathscr{B}_n$ есть вывод из $\Gamma \cup \{\mathscr{A}\}$, где $\mathscr{B}_n = \mathscr{B}$. Индукцией по i $(1 \leqslant i \leqslant n)$ докажем, что $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_i$. Прежде всего, $\mathscr{B}_1$ должно быть либо элементом Γ, либо быть аксиомой системы L, либо совпадать с $\mathscr{A}$. По схеме аксиом (A1), $\mathscr{B}_1 \supset (\mathscr{A} \supset \mathscr{B}_1)$ есть аксиома. Поэтому в первых двух случаях $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_1$ по MP. В третьем случае, т. е. когда $\mathscr{B}_1$ совпадает с $\mathscr{A}$, по лемме 1.7 мы имеем $\vdash \mathscr{A} \supset \mathscr{B}_1$ и, следовательно, $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_1$. Тем самым случай $i = 1$ исчерпан. Допустим теперь, что $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_k$ для любого $k < i$. Для $\mathscr{B}_i$ имеем четыре возможности: $\mathscr{B}_i$ есть аксиома, или $\mathscr{B}_i \in \Gamma$, или $\mathscr{B}_i$ есть $\mathscr{A}$, или $\mathscr{B}_i$ следует по modus ponens из некоторых $\mathscr{B}_j$ и $\mathscr{B}_m$, где $j < i$, $m < i$ и $\mathscr{B}_m$ имеет вид $\mathscr{B}_j \supset \mathscr{B}_i$. В первых трех случаях $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_i$ доказывается так же, как для $i = 1$. В последнем случае применим индуктивное предположение, согласно которому $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_j$ и $\Gamma \vdash \mathscr{A} \supset (\mathscr{B}_j \supset \mathscr{B}_i)$. По схеме аксиом (A2), $\vdash (\mathscr{A} \supset (\mathscr{B}_j \supset \mathscr{B}_i)) \supset ((\mathscr{A} \supset \mathscr{B}_j) \supset (\mathscr{A} \supset \mathscr{B}_i))$. Следовательно, по MP, $\Gamma \vdash (\mathscr{A} \supset \mathscr{B}_j) \supset (\mathscr{A} \supset \mathscr{B}_i)$ и, снова по MP, $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_i$. Таким образом, наше доказательство по индукции завершено, и для $i = n$ мы получаем требуемое утверждение. (Заметим, что проведенное доказательство позволяет по данному выводу $\mathscr{B}$ из Γ и $\mathscr{A}$ построить вывод $\mathscr{A} \supset \mathscr{B}$ из Γ и что при доказательстве теоремы дедукции мы использовали только схемы аксиом (A1) и (A2).)

Следствие 1.9.

(i) $\mathscr{A} \supset \mathscr{B}, \mathscr{B} \supset \mathscr{C} \vdash \mathscr{A} \supset \mathscr{C}$.

(ii) $\mathscr{A} \supset (\mathscr{B} \supset \mathscr{C}), \mathscr{B} \vdash \mathscr{A} \supset \mathscr{C}$.

Доказательство (i)

(a) $\mathscr{A} \supset \mathscr{B}$ гипотеза

(b) $\mathscr{B} \supset \mathscr{C}$ гипотеза

---

*) Мы пишем $\Gamma, \mathscr{A} \vdash \mathscr{B}$ вместо $\Gamma \cup \{\mathscr{A}\} \vdash \mathscr{B}$, и вообще $\Gamma, \mathscr{A}_1, \ldots, \mathscr{A}_n \vdash \mathscr{B}$ вместо $\Gamma \cup \{\mathscr{A}_1, \ldots, \mathscr{A}_n\} \vdash \mathscr{B}$.

(c) $\mathscr{A}$ гипотеза
(d) $\mathscr{B}$ (a), (c), MP
(e) $\mathscr{C}$ (b), (d), MP

Таким образом, $\mathscr{A} \supset \mathscr{B}$, $\mathscr{B} \supset \mathscr{C}$, $\mathscr{A} \vdash \mathscr{C}$ Отсюда, по теореме дедукции, $\mathscr{A} \supset \mathscr{B}$, $\mathscr{B} \supset \mathscr{C} \vdash \mathscr{A} \supset \mathscr{C}$.

Доказательство (ii) предлагается провести самостоятельно в качестве упражнения (использовать теорему дедукции).

Лемма 1.10. *Для любых формул* $\mathscr{A}$, $\mathscr{B}$ *следующие формулы являются теоремами* L:

(a) $\neg\neg\mathscr{B} \supset \mathscr{B}$;
(b) $\mathscr{B} \supset \neg\neg\mathscr{B}$;
(c) $\neg\mathscr{A} \supset (\mathscr{A} \supset \mathscr{B})$;
(d) $(\neg\mathscr{B} \supset \neg\mathscr{A}) \supset (\mathscr{A} \supset \mathscr{B})$;
(e) $(\mathscr{A} \supset \mathscr{B}) \supset (\neg\mathscr{B} \supset \neg\mathscr{A})$;
(f) $\mathscr{A} \supset (\neg\mathscr{B} \supset \neg(\mathscr{A} \supset \mathscr{B}))$;
(g) $(\mathscr{A} \supset \mathscr{B}) \supset ((\neg\mathscr{A} \supset \mathscr{B}) \supset \mathscr{B})$.

Доказательство.

(a) $\vdash \neg\neg\mathscr{B} \supset \mathscr{B}$.

1. $(\neg\mathscr{B} \supset \neg\neg\mathscr{B}) \supset ((\neg\mathscr{B} \supset \neg\mathscr{B}) \supset \mathscr{B})$ схема аксиом (A3)
2. $\neg\mathscr{B} \supset \neg\mathscr{B}$ лемма 1.7 *)
3. $(\neg\mathscr{B} \supset \neg\neg\mathscr{B}) \supset \mathscr{B}$ 1, 2, следствие 1.9 (ii)
4. $\neg\neg\mathscr{B} \supset (\neg\mathscr{B} \supset \neg\neg\mathscr{B})$ схема аксиом (A1)
5. $\neg\neg\mathscr{B} \supset \mathscr{B}$ 3, 4, следствие 1.9 (i)

(b) $\vdash \mathscr{B} \supset \neg\neg\mathscr{B}$.

1. $(\neg\neg\neg\mathscr{B} \supset \neg\mathscr{B}) \supset ((\neg\neg\neg\mathscr{B} \supset \mathscr{B}) \supset \neg\neg\mathscr{B})$ схема аксиом (A3)
2. $\neg\neg\neg\mathscr{B} \supset \neg\mathscr{B}$ пункт (a), доказанный выше
3. $(\neg\neg\neg\mathscr{B} \supset \mathscr{B}) \supset \neg\neg\mathscr{B}$ 1, 2, MP
4. $\mathscr{B} \supset (\neg\neg\neg\mathscr{B} \supset \mathscr{B})$ схема аксиом (A1)
5. $\mathscr{B} \supset \neg\neg\mathscr{B}$ 3, 4, следствие 1.9 (i)

(c) $\vdash \neg\mathscr{A} \supset (\mathscr{A} \supset \mathscr{B})$.

1. $\neg\mathscr{A}$ гипотеза
2. $\mathscr{A}$ гипотеза

*) Вместо того чтобы приводить в этом месте полный вывод для $\neg\mathscr{B} \supset \neg\mathscr{B}$, мы просто ссылаемся на лемму 1.7. Поступая таким образом, мы указываем на то, что в этом месте вывод для $\neg\mathscr{B} \supset \neg\mathscr{B}$ мог бы быть выписан, имей мы на то желание, время и место. Разумеется, это есть не что иное, как обычное применение ранее установленных теорем.

3. $\mathscr{A} \supset (\neg \mathscr{B} \supset \mathscr{A})$	схема аксиом (A1)
4. $\neg \mathscr{A} \supset (\neg \mathscr{B} \supset \neg \mathscr{A})$	схема аксиом (A1)
5. $\neg \mathscr{B} \supset \mathscr{A}$	2, 3, MP
6. $\neg \mathscr{B} \supset \neg \mathscr{A}$	1, 4, MP
7. $(\neg \mathscr{B} \supset \neg \mathscr{A}) \supset ((\neg \mathscr{B} \supset \mathscr{A}) \supset \mathscr{B})$	схема аксиом (A3)
8. $(\neg \mathscr{B} \supset \mathscr{A}) \supset \mathscr{B}$	6, 7, MP
9. $\mathscr{B}$	5, 8, MP

Итак, в силу 1—9, $\neg \mathscr{A}, \mathscr{A} \vdash \mathscr{B}$. Поэтому, по теореме дедукции, $\neg \mathscr{A} \vdash \mathscr{A} \supset \mathscr{B}$ и, снова по той же теореме, $\vdash \neg \mathscr{A} \supset (\mathscr{A} \supset \mathscr{B})$.

(d) $\vdash (\neg \mathscr{B} \supset \neg \mathscr{A}) \supset (\mathscr{A} \supset \mathscr{B})$.

1. $\neg \mathscr{B} \supset \neg \mathscr{A}$	гипотеза
2. $\mathscr{A}$	гипотеза
3. $(\neg \mathscr{B} \supset \neg \mathscr{A}) \supset ((\neg \mathscr{B} \supset \mathscr{A}) \supset \mathscr{B})$	схема аксиом (A3)
4. $\mathscr{A} \supset (\neg \mathscr{B} \supset \mathscr{A})$	схема аксиом (A1)
5. $(\neg \mathscr{B} \supset \mathscr{A}) \supset \mathscr{B}$	1, 3, MP
6. $\mathscr{A} \supset \mathscr{B}$	4, 5, следствие 1.9 (i)
7. $\mathscr{B}$	2, 6, MP

В силу 1—7, $\neg \mathscr{B} \supset \neg \mathscr{A}, \mathscr{A} \vdash \mathscr{B}$, после чего, дважды применив теорему дедукции, получим требуемый результат.

(e) $\vdash (\mathscr{A} \supset \mathscr{B}) \supset (\neg \mathscr{B} \supset \neg \mathscr{A})$.

1. $\mathscr{A} \supset \mathscr{B}$	гипотеза
2. $\neg \neg \mathscr{A} \supset \mathscr{A}$	пункт (a)
3. $\neg \neg \mathscr{A} \supset \mathscr{B}$	1, 2, следствие 1.9 (i)
4. $\mathscr{B} \supset \neg \neg \mathscr{B}$	пункт (b)
5. $\neg \neg \mathscr{A} \supset \neg \neg \mathscr{B}$	3, 4, следствие 1.9 (i)
6. $(\neg \neg \mathscr{A} \supset \neg \neg \mathscr{B}) \supset (\neg \mathscr{B} \supset \neg \mathscr{A})$	пункт (d)
7. $(\neg \mathscr{B} \supset \neg \mathscr{A})$	5, 6, MP

В силу 1—7, $\mathscr{A} \supset \mathscr{B} \vdash \neg \mathscr{B} \supset \neg \mathscr{A}$, откуда (e) получается по теореме дедукции.

(f) $\vdash \mathscr{A} \supset (\neg \mathscr{B} \supset \neg (\mathscr{A} \supset \mathscr{B}))$

Очевидно, $\mathscr{A}, \mathscr{A} \supset \mathscr{B} \vdash \mathscr{B}$. Применив дважды теорему дедукции, получаем $\vdash \mathscr{A} \supset ((\mathscr{A} \supset \mathscr{B}) \supset \mathscr{B})$. По пункту (e) имеем $\vdash ((\mathscr{A} \supset \mathscr{B}) \supset \mathscr{B}) \supset (\neg \mathscr{B} \supset \neg (\mathscr{A} \supset \mathscr{B}))$. Наконец, применив 1.9 (i), получаем

$$\vdash \mathscr{A} \supset (\neg \mathscr{B} \supset \neg (\mathscr{A} \supset \mathscr{B})).$$

(g) $\vdash (\mathscr{A} \supset \mathscr{B}) \supset ((\neg \mathscr{A} \supset \mathscr{B}) \supset \mathscr{B})$.

1. $\mathscr{A} \supset \mathscr{B}$	гипотеза
2. $\neg \mathscr{A} \supset \mathscr{B}$	гипотеза
3. $(\mathscr{A} \supset \mathscr{B}) \supset (\neg \mathscr{B} \supset \neg \mathscr{A})$	пункт (e)
4. $\neg \mathscr{B} \supset \neg \mathscr{A}$	1, 3, MP
5. $(\neg \mathscr{A} \supset \mathscr{B}) \supset (\neg \mathscr{B} \supset \neg \neg \mathscr{A})$	пункт (e)
6. $\neg \mathscr{B} \supset \neg \neg \mathscr{A}$	2, 5, MP
7. $(\neg \mathscr{B} \supset \neg \neg \mathscr{A}) \supset ((\neg \mathscr{B} \supset \neg \mathscr{A}) \supset \mathscr{B})$	схема аксиом (A3)
8. $(\neg \mathscr{B} \supset \neg \mathscr{A}) \supset \mathscr{B}$	6, 7, MP
9. $\mathscr{B}$	4, 8, MP

Итак, $\mathscr{A} \supset \mathscr{B}$, $\neg \mathscr{A} \supset \mathscr{B} \vdash \mathscr{B}$. Применив два раза теорему дедукции, получаем (g).

Упражнения

1. Показать, что следующие формулы являются теоремами теории L:

(a) $((\mathscr{A} \supset \mathscr{B}) \supset \mathscr{A}) \supset \mathscr{A}$;
(b) $\mathscr{A} \supset (\mathscr{B} \supset (\mathscr{A} \,\&\, \mathscr{B}))$.

2. Построить полное доказательство (вывод в L) для пункта (c) леммы 1.10. (Указание. Применить к приведенному выше доказательству пункта (c) леммы 1.10 построения из доказательства теоремы дедукции.) Читатель проникнется большей любовью к теореме дедукции, если он попытается провести доказательство леммы 1.10, не прибегая к помощи этой теоремы.

Наша цель — показать, что формула теории L тогда и только тогда является теоремой этой теории, когда она есть тавтология. В одну сторону это совсем просто.

Предложение 1.11. *Всякая теорема теории* L *есть тавтология.*

Доказательство. В качестве упражнения можно убедиться в том, что каждая аксиома теории L есть тавтология. В силу предложения 1.1, правило modus ponens, примененное к тавтологиям, приводит к тавтологиям. Следовательно, всякая теорема теории L есть тавтология.

Следующая лемма будет применена при доказательстве того, что каждая тавтология является теоремой теории L.

Лемма 1.12. *Пусть* $\mathscr{A}$ *есть формула, а* $B_1, \ldots, B_k$ *— пропозициональные буквы, входящие в* $\mathscr{A}$, *и пусть задано некоторое распределение истинностных значений для* $B_1, \ldots, B_k$. *Пусть тогда* B_i' *есть* B_i, *если* B_i *принимает значение* И, *и* $\neg B_i$, *если* B_i *принимает значение* Л, *и пусть, наконец,* $\mathscr{A}'$ *есть* $\mathscr{A}$, *если при этом распределении* $\mathscr{A}$ *принимает значение* И, *и* $\neg \mathscr{A}$, *если* $\mathscr{A}$ *принимает значение* Л. *Тогда* $B_1', \ldots, B_k' \vdash \mathscr{A}'$.

Если, например, $\mathscr{A}$ обозначает $\neg(\neg A_2 \supset A_5)$, то для каждой строки истинностной таблицы

A_2	A_5	$\neg(\neg A_2 \supset A_5)$
И	И	Л
Л	И	Л
И	Л	Л
Л	Л	И

лемма 1.12 утверждает факт соответствующей выводимости. Так, в частности, третьей строке соответствует утверждение $A_2, \neg A_5 \vdash \neg\neg(\neg A_2 \supset A_5)$, а четвертой строке — $\neg A_2, \neg A_5 \vdash \neg(\neg A_2 \supset A_5)$.

Доказательство. Доказательство ведется индукцией по числу n вхождений в $\mathscr{A}$ примитивных связок (предполагается, естественно, что $\mathscr{A}$ записано без сокращений). Если $n=0$, то $\mathscr{A}$ представляет собой просто пропозициональную букву B_1, и утверждение леммы сводится к $B_1 \vdash B_1$ и к $\neg B_1 \vdash \neg B_1$. Допустим теперь, что лемма верна при любом $j<n$.

Случай 1. $\mathscr{A}$ имеет вид отрицания: $\neg\mathscr{B}$. Число вхождений примитивных связок в $\mathscr{B}$, очевидно, меньше n.

Случай 1a. Пусть при заданном распределении истинностных значений $\mathscr{B}$ принимает значение И. Тогда $\mathscr{A}$ принимает значение Л. Таким образом, $\mathscr{B}'$ есть $\mathscr{B}$, а $\mathscr{A}'$ есть $\neg\mathscr{A}$. По индуктивному предположению, примененному к $\mathscr{B}$, мы имеем $B_1', \ldots, B_k' \vdash \mathscr{B}$. Следовательно, по лемме 1.10 (b) и MP, $B_1', \ldots, B_k' \vdash \neg\neg\mathscr{B}$. Но $\neg\neg\mathscr{B}$ и есть $\mathscr{A}'$.

Случай 1b. Пусть $\mathscr{B}$ принимает значение Л; тогда $\mathscr{B}'$ есть $\neg\mathscr{B}$, а $\mathscr{A}'$ совпадает с $\mathscr{A}$. По индуктивному предположению, $B_1', \ldots, B_k' \vdash \neg\mathscr{B}$, что и требовалось получить, ибо $\neg\mathscr{B}$ есть $\mathscr{A}'$.

Случай 2. $\mathscr{A}$ имеет вид $(\mathscr{B}\supset\mathscr{C})$. Тогда число вхождений примитивных связок в $\mathscr{B}$ и $\mathscr{C}$ меньше, чем в $\mathscr{A}$. Поэтому, в силу индуктивного предположения, $B_1', \ldots, B_k' \vdash \mathscr{B}'$ и $B_1', \ldots, B_k' \vdash \mathscr{C}'$.

Случай 2a. $\mathscr{B}$ принимает значение Л. Тогда $\mathscr{A}$ принимает значение И, и $\mathscr{B}'$ есть $\neg\mathscr{B}$, а $\mathscr{A}'$ есть $\mathscr{A}$. Таким образом, $B_1', \ldots, B_k' \vdash \neg\mathscr{B}$ и, по лемме 1.10 (c), $B_1', \ldots, B_k' \vdash \mathscr{B}\supset\mathscr{C}$, но $\mathscr{B}\supset\mathscr{C}$ и есть $\mathscr{A}$.

Случай 2b. $\mathscr{C}$ принимает значение И. Следовательно, $\mathscr{A}$ принимает значение И и $\mathscr{C}'$ есть $\mathscr{C}$, а $\mathscr{A}'$ есть $\mathscr{A}$. Имеем $B_1', \ldots, B_k' \vdash \mathscr{C}$, и тогда, по схеме аксиом (A1), $B_1', \ldots, B_k' \vdash \mathscr{B}\supset\mathscr{C}$, где $\mathscr{B}\supset\mathscr{C}$ совпадает с $\mathscr{A}'$.

Случай 2c. $\mathscr{B}$ принимает значение И и $\mathscr{C}$ принимает значение Л. Тогда $\mathscr{A}'$ есть $\neg\mathscr{A}$, ибо $\mathscr{A}$ принимает значение Л, $\mathscr{B}'$ есть $\mathscr{B}$ и $\mathscr{C}'$ есть $\neg\mathscr{C}$. Имеем $B_1', \ldots, B_k' \vdash \mathscr{B}$ и $B_1', \ldots, B_k' \vdash \neg\mathscr{C}$. Отсюда, по лемме 1.10 (f) получаем $B_1', \ldots, B_k' \vdash \neg(\mathscr{B}\supset\mathscr{C})$, где $\neg(\mathscr{B}\supset\mathscr{C})$ и есть $\mathscr{A}'$.

Предложение 1.13. (Теорема о полноте.) *Если формула $\mathscr{A}$ теории* L *является тавтологией, то она является теоремой теории* L.

Доказательство (Кальмар) Предположим, что $\mathscr{A}$ есть тавтология и $B_1, \ldots, B_k$ — пропозициональные буквы, входящие в $\mathscr{A}$. При каждом распределении истинностных значений для букв $B_1, \ldots, B_k$ мы имеем, в силу леммы 1.12, $B'_1, \ldots, B'_k \vdash \mathscr{A}$. ($\mathscr{A}'$ совпадает с $\mathscr{A}$, так как $\mathscr{A}$ всегда принимает значение И.) Поэтому в случае, когда B_k принимает значение И, мы, применив лемму 1.12, получим $B'_1, \ldots, B'_{k-1}, B_k \vdash \mathscr{A}$, а когда B_k принимает значение Л, мы по той же лемме получим $B'_1, \ldots, B'_{k-1}, \neg B_k \vdash \mathscr{A}$. Отсюда, по теореме дедукции, $B'_1, \ldots, B'_{k-1} \vdash B_k \supset \mathscr{A}$ и $B'_1, \ldots, B'_{k-1} \vdash \neg B_k \supset \mathscr{A}$. Применив теперь лемму 1.10 (g), получим $B'_1, \ldots, B'_{k-1} \vdash \mathscr{A}$. Точно таким же образом, рассмотрев два случая, когда B_{k-1} принимает значения И и Л, и применив лемму 1.12, теорему дедукции и лемму 1.10 (g), мы исключим B_{k-1} и так далее; после k таких шагов мы придем к $\vdash \mathscr{A}$.

Следствие 1.14. *Если выражение* $\mathscr{B}$ *содержит знаки* $\neg, \supset, \&, \vee, \equiv$ *и является сокращением* (см. определения D1 — D3) *для некоторой формулы* $\mathscr{A}$ *теории* L, *то* $\mathscr{B}$ *является тавтологией тогда и только тогда, когда* $\mathscr{A}$ *есть теорема теории* L.

Доказательство. Выражения, вводимые в определениях D1 — D3 для сокращенного обозначения формул, представляют собой пропозициональные формы, логически эквивалентные обозначаемым ими пропозициональным формам. Следовательно, в силу предложения 1.3, $\mathscr{A}$ и $\mathscr{B}$ логически эквивалентны, а потому $\mathscr{B}$ есть тавтология тогда и только тогда, когда $\mathscr{A}$ есть тавтология. Теперь остается воспользоваться предложением 1.13.

Следствие 1.15. *Система* L *непротиворечива, т. е. не существует формулы* $\mathscr{A}$ *такой, чтобы* $\mathscr{A}$ *и* $\neg\mathscr{A}$ *были теоремами в* L.

Доказательство. Согласно предложению 1.11, каждая теорема теории L является тавтологией. Отрицание тавтологии не есть тавтология. Следовательно, ни для какой формулы $\mathscr{A}$ невозможно, чтобы $\mathscr{A}$ и $\neg\mathscr{A}$ были теоремами теории L.

Из непротиворечивости L следует существование формулы, не являющейся теоремой теории L (например, отрицание любой теоремы). С другой стороны, непротиворечивость L можно было бы вывести непосредственно из факта существования формулы теории L, не являющейся теоремой. В самом деле, по лемме 1.10 (c) имеем $\vdash_L \neg\mathscr{A} \supset (\mathscr{A} \supset \mathscr{B})$, и, следовательно, если бы теория L была противоречива, т. е. если бы некоторая формула $\mathscr{A}$ была выводима в L вместе со своим отрицанием $\neg\mathscr{A}$, то, в силу $\vdash_L \neg\mathscr{A} \supset (\mathscr{A} \supset \mathscr{B})$ и MP, в L была бы выводима всякая формула $\mathscr{B}$. (Эквивалентность непротиворечивости и существования невыводимой формулы верна для всякой теории с modus ponens в качестве правила вывода, для которой доказуема лемма 1.10 (c).) Теорию, в которой не все формулы являются теоремами, часто называют *абсолютно непротиворечивой*. Это определение применимо и к теориям, не содержащим знака отрицания.

Упражнения

1. Проверить, что для любых формул $\mathscr{A}$, $\mathscr{B}$ и $\mathscr{C}$ следующие формулы являются тавтологиями и, следовательно, теоремами теории L:

(a) $((\mathscr{A} \vee \mathscr{B}) \& (\mathscr{A} \supset \mathscr{C}) \& (\mathscr{B} \supset \mathscr{C})) \supset \mathscr{C}$;

(b) $\mathscr{A} \supset (\mathscr{B} \supset \mathscr{C}) \equiv (\mathscr{A} \& \mathscr{B}) \supset \mathscr{C}$.

2. Пусть $\mathscr{A}$ — пропозициональная форма, не являющаяся тавтологией. Построим теорию L^+, добавив к L в качестве новых аксиом все формулы, которые можно получить из $\mathscr{A}$, подставляя на места пропозициональных букв в $\mathscr{A}$ произвольные формы (с тем, однако, условием, чтобы на места всех вхождений одной и той же буквы подставлялась одна и та же формула). Показать, что теория L^+ противоречива.

§ 5. Независимость. Многозначные логики

Подмножество X множества всех аксиом данной аксиоматической теории называется *независимым*, если какая-нибудь формула из X не может быть выведена с помощью правил вывода из аксиом, не входящих в X.

Предложение 1.16. *Каждая из схем аксиом* (A1) — (A3) *независима.*

Доказательство.

(a) Независимость (A1). Рассмотрим следующие таблицы:

A	$\neg A$
0	1
1	1
2	0

A	B	$A \supset B$
0	0	0
1	0	2
2	0	0
0	1	2
1	1	2
2	1	0
0	2	2
1	2	0
2	2	0

При всяком распределении значений 0, 1, 2 для букв, входящих в формулу $\mathscr{A}$, эти таблицы позволяют найти соответствующее значение формулы $\mathscr{A}$. Если формула $\mathscr{A}$ всегда принимает значение 0, то она называется *выделенной*. Modus ponens сохраняет свойство выделенности. Читателю предлагается убедиться в этом самому, показав, что если формулы $\mathscr{A} \supset \mathscr{B}$ и $\mathscr{A}$ выделенные, то и формула $\mathscr{B}$ выделенная. Нетрудно проверить также, что всякая аксиома, получающаяся по схеме (A2) или (A3), тоже выделенная. Следовательно, выделенной является и всякая формула, выводимая из (A2) — (A3) с помощью modus ponens. Однако формула $A_1 \supset (A_2 \supset A_1)$, которая представляет собой частный случай (A1),

не выделенная, ибо она принимает значение 2, когда A_1 принимает значение 1 и A_2 принимает значение 2.

(b) Независимость (A2). Рассмотрим следующие таблицы:

A	$\neg A$
0	1
1	0
2	1

A	B	$A \supset B$
0	0	0
1	0	0
2	0	0
0	1	2
1	1	2
2	1	0
0	2	1
1	2	0
2	2	0

Всякую формулу, принимающую, согласно этим таблицам, всегда значение 0, назовем *гротескной*. Modus ponens сохраняет гротескность, и все частные случаи схем (A1) и (A3) гротескны (проверьте это сами). При этом, однако, частный случай $(A_1 \supset (A_2 \supset A_3)) \supset ((A_1 \supset A_2) \supset (A_1 \supset A_3))$ схемы (A2) не является гротескным, ибо принимает значение 2, когда A_1, A_2 и A_3 получают соответственно значения 0, 0 и 1.

(c) Независимость (A3). Пусть $\mathscr{A}$ — произвольная формула и $h(\mathscr{A})$ — формула, полученная из $\mathscr{A}$ стиранием всех вхождений знака отрицания в $\mathscr{A}$. Для всякого частного случая $\mathscr{A}$ схем (A1) и (A2) $h(\mathscr{A})$ есть тавтология. Правило modus ponens сохраняет свойство $\mathscr{A}$ иметь в качестве $h(\mathscr{A})$ тавтологию, ибо если $h(\mathscr{A} \supset \mathscr{B})$ и $h(\mathscr{A})$ — тавтологии, то и $h(\mathscr{B})$ — тавтология (следует лишь заметить, что $h(\mathscr{A} \supset \mathscr{B})$ совпадает с $h(\mathscr{A}) \supset h(\mathscr{B})$). Следовательно, всякая формула $\mathscr{A}$, выводимая из (A1) — (A2) с помощью modus ponens, имеет в качестве $h(\mathscr{A})$ тавтологию. Но $h((\neg A_1 \supset \neg A_1) \supset ((\neg A_1 \supset A_1) \supset A_1))$ совпадает с $(A_1 \supset A_1) \supset ((A_1 \supset A_1) \supset A_1)$, а эта последняя формула не является тавтологией. Следовательно, $(\neg A_1 \supset \neg A_1) \supset ((\neg A_1 \supset A_1) \supset A_1)$, частный случай (A3), невыводима из (A1) и (A2) с помощью modus ponens.

Упражнение

Доказать независимость схемы аксиом (A3) построением подходящих таблиц для связок $\neg$ и $\supset$.

Обобщение идеи, использованной для доказательства независимости схем аксиом (A1) — (A3), приводит к следующему понятию многозначной логики. Назовем числа 0, 1, ..., n «истинностными значениями» и выберем какое-нибудь число m с условием $1 \leqslant m \leqslant n$. Числа 0, 1, ..., m будем называть *выделенными истинностными значениями*. Возьмем

некоторое конечное число «истинностных таблиц», представляющих функции, отображающие множество $\{0, 1, \ldots, n\}$ в себя. Для каждой таблицы введем знак, который будем называть соответствующей этой таблице связкой. С помощью этих связок и пропозициональных букв мы можем строить пропозициональные формы. Каждая такая форма определяет некоторую «истинностную функцию», отображающую множество $\{0, 1, \ldots, n\}$ в себя. Пропозициональная форма, принимающая только выделенные значения, называется *выделенной*. Говорят, что числа n, m и основные истинностные таблицы определяют некоторую (конечную) *многозначную логику* M. Аксиоматическая теория, содержащая пропозициональные буквы и связки логики M, называется *подходящей* для логики M в том и только в том случае, когда множество теорем этой теории совпадает с множеством выделенных пропозициональных форм логики M. (Очевидно, все эти понятия могут быть обобщены на случай бесконечного множества истинностных значений.)

В этой главе изучена 2-значная логика, соответствующая случаю $n=1$, $m=0$ и введенным в § 1 истинностным таблицам для связок $\neg$ и $\supset$. Выделенные формулы этой логики назывались тавтологиями. Предложения 1.11 и 1.13 устанавливают тот факт, что теория L является подходящей для этой логики аксиоматической теорией. Две трехзначные логики были использованы нами при доказательстве независимости схем аксиом (A1) — (A3).

Упражнения

1. (Мак-Кинси — Тарский.) Рассмотрим аксиоматическую систему P, в которой имеется единственная бинарная связка $*$, единственное правило вывода — modus ponens (т. е. $\mathscr{B}$ следует из $\mathscr{A} * \mathscr{B}$ и $\mathscr{A}$) и аксиомами служат все формулы вида $\mathscr{A} * \mathscr{A}$. Доказать, что теория P не является подходящей ни для какой (конечной) многозначной логики.

2. Для любой (конечной) многозначной логики M существует подходящая аксиоматическая теория.

Дальнейшие сведения о многозначных логиках можно почерпнуть из монографии Россера и Тюркетта [1952], а также из упоминаемых в этой книге работ.

§ 6. Другие аксиоматизации

Хотя система аксиом L и весьма проста, существует много других систем, работающих также хорошо.

Вместо $\neg$ и $\supset$ можно использовать и другие наборы примитивных связок, лишь бы через них можно было выразить все остальные истинностно-функциональные связки.

Примеры. L_1: Примитивные связки: $\vee$, $\neg$. $\mathscr{A} \supset \mathscr{B}$ служит сокращением для $\neg \mathscr{A} \vee \mathscr{B}$. Четыре схемы аксиом: (1) $\mathscr{A} \vee \mathscr{A} \supset \mathscr{A}$; (2) $\mathscr{A} \supset \mathscr{A} \vee \mathscr{B}$; (3) $\mathscr{A} \vee \mathscr{B} \supset \mathscr{B} \vee \mathscr{A}$; (4) $(\mathscr{B} \supset \mathscr{C}) \supset (\mathscr{A} \vee \mathscr{B} \supset$

$\supset \mathscr{A} \vee \mathscr{C}$). Единственное правило вывода — modus ponens. Эта система рассмотрена в книге Гильберта и Аккермана [1938].

L_2: Примитивные связки: & и $\neg$. $\mathscr{A} \supset \mathscr{B}$ сокращает $\neg(\mathscr{A} \& \neg \mathscr{B})$. Три схемы аксиом: (1) $\mathscr{A} \supset (\mathscr{A} \& \mathscr{A})$; (2) $(\mathscr{A} \& \mathscr{B}) \supset \mathscr{A}$; (3) $(\mathscr{A} \supset \mathscr{B}) \supset (\neg(\mathscr{B} \& \mathscr{C}) \supset \neg(\mathscr{C} \& \mathscr{A}))$. Modus ponens служит единственным правилом вывода. Система подробно изучена Россером [1953].

L_3: Эта система очень похожа на L; разница состоит в том, что вместо трех схем аксиом (A1) — (A3) здесь имеются лишь три конкретные аксиомы: (1) $A_1 \supset (A_2 \supset A_1)$; (2) $(A_1 \supset (A_2 \supset A_3)) \supset ((A_1 \supset A_2) \supset (A_1 \supset A_3))$; (3) $(\neg A_2 \supset \neg A_1) \supset ((\neg A_2 \supset A_1) \supset A_2)$, зато кроме modus ponens имеется еще одно правило вывода — правило подстановки, разрешающее подстановку любой формулы на места всех вхождений данной пропозициональной буквы в данную формулу.

L_4: Примитивными связками служат $\supset$, &, $\vee$ и $\neg$. Единственное правило вывода — modus ponens. Класс аксиом задается следующими схемами аксиом:

(1) $\mathscr{A} \supset (\mathscr{B} \supset \mathscr{A})$;
(2) $(\mathscr{A} \supset (\mathscr{B} \supset \mathscr{C})) \supset ((\mathscr{A} \supset \mathscr{B}) \supset (\mathscr{A} \supset \mathscr{C}))$;
(3) $\mathscr{A} \& \mathscr{B} \supset \mathscr{A}$;
(4) $\mathscr{A} \& \mathscr{B} \supset \mathscr{B}$;
(5) $\mathscr{A} \supset (\mathscr{B} \supset (\mathscr{A} \& \mathscr{B}))$;
(6) $\mathscr{A} \supset (\mathscr{A} \vee \mathscr{B})$;
(7) $\mathscr{B} \supset (\mathscr{A} \vee \mathscr{B})$;
(8) $(\mathscr{A} \supset \mathscr{C}) \supset ((\mathscr{B} \supset \mathscr{C}) \supset ((\mathscr{A} \vee \mathscr{B}) \supset \mathscr{C}))$;
(9) $(\mathscr{A} \supset \mathscr{B}) \supset ((\mathscr{A} \supset \neg \mathscr{B}) \supset \neg \mathscr{A})$;
(10) $\neg\neg \mathscr{A} \supset \mathscr{A}$.

Как обычно, $\mathscr{A} \equiv \mathscr{B}$ означает $(\mathscr{A} \supset \mathscr{B}) \& (\mathscr{B} \supset \mathscr{A})$. Эту систему можно найти, например, в книге Клини [1952].

Упражнения

1. (Гильберт и Аккерман [1938].) Доказать следующие теоремы о теории L_1:

(a) $\mathscr{A} \supset \mathscr{B} \vdash_{L_1} \mathscr{C} \vee \mathscr{A} \supset \mathscr{C} \vee \mathscr{B}$;
(b) $\vdash_{L_1} (\mathscr{A} \supset \mathscr{B}) \supset ((\mathscr{C} \supset \mathscr{A}) \supset (\mathscr{C} \supset \mathscr{B}))$;
(c) $\mathscr{C} \supset \mathscr{A}, \mathscr{A} \supset \mathscr{B} \vdash_{L_1} \mathscr{C} \supset \mathscr{B}$;
(d) $\vdash_{L_1} \mathscr{A} \supset \mathscr{A}$ (т. е. $\vdash_{L_1} \neg \mathscr{A} \vee \mathscr{A}$);
(e) $\vdash_{L_1} \mathscr{A} \vee \neg \mathscr{A}$;
(f) $\vdash_{L_1} \mathscr{A} \supset \neg\neg \mathscr{A}$;
(g) $\vdash_{L_1} \neg \mathscr{B} \supset (\mathscr{B} \supset \mathscr{C})$;
(h) $\vdash_{L_1} \mathscr{A} \vee (\mathscr{B} \vee \mathscr{C}) \supset ((\mathscr{B} \vee (\mathscr{A} \vee \mathscr{C})) \vee \mathscr{A})$;
(i) $\vdash_{L_1} (\mathscr{B} \vee (\mathscr{A} \vee \mathscr{C})) \vee \mathscr{A} \supset \mathscr{B} \vee (\mathscr{A} \vee \mathscr{C})$;

(j) $\vdash_{L_1} \mathscr{A} \vee (\mathscr{B} \vee \mathscr{C}) \supset \mathscr{B} \vee (\mathscr{A} \vee \mathscr{C})$;

(k) $\vdash_{L_1} (\mathscr{A} \supset (\mathscr{B} \supset \mathscr{C})) \supset (\mathscr{B} \supset (\mathscr{A} \supset \mathscr{C}))$;

(l) $\vdash_{L_1} (\mathscr{C} \supset \mathscr{A}) \supset ((\mathscr{A} \supset \mathscr{B}) \supset (\mathscr{C} \supset \mathscr{B}))$;

(m) $\mathscr{A} \supset (\mathscr{B} \supset \mathscr{C}), \mathscr{A} \supset \mathscr{B} \vdash_{L_1} \mathscr{A} \supset (\mathscr{A} \supset \mathscr{C})$;

(n) $\mathscr{A} \supset (\mathscr{B} \supset \mathscr{C}), \mathscr{A} \supset \mathscr{B} \vdash_{L_1} \mathscr{A} \supset \mathscr{C}$;

(o) если Γ, $\mathscr{A} \vdash_{L_1} \mathscr{B}$, то $\Gamma \vdash_{L_1} \mathscr{A} \supset \mathscr{B}$ (теорема дедукции);

(p) $\mathscr{B} \supset \mathscr{A}, \neg \mathscr{B} \supset \mathscr{A} \vdash_{L_1} \mathscr{A}$;

(q) $\vdash_{L_1} \mathscr{A}$ тогда и только тогда, когда $\mathscr{A}$ есть тавтология. (Указание. Доказать утверждения, аналогичные лемме 1.12 и предложению 1.13.)

2. (Россер [1953].) Доказать следующие утверждения о теории L_2:

(a) $\mathscr{A} \supset \mathscr{B}, \mathscr{B} \supset \mathscr{C} \vdash_{L_2} \neg (\neg \mathscr{C} \& \mathscr{A})$;

(b) $\vdash_{L_2} \neg (\neg \mathscr{A} \& \mathscr{A})$;

(c) $\vdash_{L_2} \neg \neg \mathscr{A} \supset \mathscr{A}$;

(d) $\vdash_{L_2} \neg (\mathscr{A} \& \mathscr{B}) \supset (\mathscr{B} \supset \neg \mathscr{A})$;

(e) $\vdash_{L_2} \mathscr{A} \supset \neg \neg \mathscr{A}$;

(f) $\vdash_{L_2} (\mathscr{A} \supset \mathscr{B}) \supset (\neg \mathscr{B} \supset \neg \mathscr{A})$;

(g) $\neg \mathscr{A} \supset \neg \mathscr{B} \vdash_{L_2} \mathscr{B} \supset \mathscr{A}$;

(h) $\mathscr{A} \supset \mathscr{B} \vdash_{L_2} \mathscr{C} \& \mathscr{A} \supset \mathscr{B} \& \mathscr{C}$;

(i) $\mathscr{A} \supset \mathscr{B}, \mathscr{B} \supset \mathscr{C}, \mathscr{C} \supset \mathscr{D} \vdash_{L_2} \mathscr{A} \supset \mathscr{D}$;

(j) $\vdash_{L_2} \mathscr{A} \supset \mathscr{A}$;

(k) $\vdash_{L_2} \mathscr{A} \& \mathscr{B} \supset \mathscr{B} \& \mathscr{A}$;

(l) $\mathscr{A} \supset \mathscr{B}, \mathscr{B} \supset \mathscr{C} \vdash_{L_2} \mathscr{A} \supset \mathscr{C}$;

(m) $\mathscr{A} \supset \mathscr{B}, \mathscr{C} \supset \mathscr{D} \vdash_{L_2} \mathscr{A} \& \mathscr{C} \supset \mathscr{B} \& \mathscr{D}$;

(n) $\mathscr{B} \supset \mathscr{C} \vdash_{L_2} \mathscr{A} \& \mathscr{B} \supset \mathscr{A} \& \mathscr{C}$;

(o) $\vdash_{L_2} (\mathscr{A} \supset (\mathscr{B} \supset \mathscr{C})) \supset ((\mathscr{A} \& \mathscr{B}) \supset \mathscr{C})$;

(p) $\vdash_{L_2} ((\mathscr{A} \& \mathscr{B}) \supset \mathscr{C}) \supset (\mathscr{A} \supset (\mathscr{B} \supset \mathscr{C}))$;

(q) $\mathscr{A} \supset \mathscr{B}, \mathscr{A} \supset (\mathscr{B} \supset \mathscr{C}) \vdash_{L_2} \mathscr{A} \supset \mathscr{C}$;

(r) $\vdash_{L_2} \mathscr{A} \supset (\mathscr{B} \supset \mathscr{A} \& \mathscr{B})$;

(s) $\vdash_{L_2} \mathscr{A} \supset (\mathscr{B} \supset \mathscr{A})$;

(t) Если Γ, $\mathscr{A} \vdash_{L_2} \mathscr{B}$, то $\Gamma \vdash_{L_2} \mathscr{A} \supset \mathscr{B}$ (теорема дедукции);

(u) $\vdash_{L_2} (\neg \mathscr{A} \supset \mathscr{A}) \supset \mathscr{A}$;

(v) $\mathscr{A} \supset \mathscr{B}, \neg \mathscr{A} \supset \mathscr{B} \vdash_{L_2} \mathscr{B}$;

(w) $\vdash_{L_2} \mathscr{A}$ тогда и только тогда, когда $\mathscr{A}$ есть тавтология. (Указание. Доказать аналоги леммы 1.12 и предложения 1.13.)

3. Доказать, что множества всех теорем теорий L и L_3 совпадают.

4. (Клини [1952].) Доказать следующие предложения о теории L_4:

(a) $\vdash_{L_4} \mathscr{A} \supset \mathscr{A}$;

(b) Если Γ, $\mathscr{A} \vdash_{L_4} \mathscr{B}$, то $\Gamma \vdash_{L_4} \mathscr{A} \supset \mathscr{B}$ (теорема дедукции);

(c) $\mathscr{A} \supset \mathscr{B}, \mathscr{B} \supset \mathscr{C} \vdash_{L_4} \mathscr{A} \supset \mathscr{C}$;
(d) $\vdash_{L_4} (\mathscr{A} \supset \mathscr{B}) \supset (\neg \mathscr{B} \supset \neg \mathscr{A})$;
(e) $\mathscr{B}, \neg \mathscr{B} \vdash_{L_4} \mathscr{C}$;
(f) $\vdash_{L_4} \mathscr{B} \supset \neg \neg \mathscr{B}$;
(g) $\vdash_{L_4} \neg \mathscr{B} \supset (\mathscr{B} \supset \mathscr{C})$;
(h) $\vdash_{L_4} \mathscr{B} \supset (\neg \mathscr{C} \supset \neg (\mathscr{B} \supset \mathscr{C}))$;
(i) $\vdash_{L_4} \neg \mathscr{B} \supset (\neg \mathscr{C} \supset \neg (\mathscr{B} \vee \mathscr{C}))$;
(j) $\vdash_{L_4} (\neg \mathscr{B} \supset \mathscr{A}) \supset ((\mathscr{B} \supset \mathscr{A}) \supset \mathscr{A})$;
(k) $\vdash_{L_4} \mathscr{A}$ тогда и только тогда, когда $\mathscr{A}$ есть тавтология.
(Доказать аналоги леммы 1.12 и предложения 1.13.)

Для исчисления высказываний могут быть построены аксиоматизации и с одной единственной схемой аксиом. Так, например, если за примитивные связки принять $\neg$ и $\supset$, то при единственном правиле вывода — modus ponens — достаточной оказывается схема аксиом:

$$[(((\mathscr{A} \supset \mathscr{B}) \supset (\neg \mathscr{C} \supset \neg \mathscr{D})) \supset \mathscr{C}) \supset \mathscr{E}] \supset [(\mathscr{E} \supset \mathscr{A}) \supset (\mathscr{D} \supset \mathscr{A})]$$

(Мередит [1953]).

Другим примером такого рода может служить система Никода [1917], в которой употребляется единственная связка $|$ (дизъюнкция отрицаний), имеется единственное правило вывода, по которому $\mathscr{C}$ следует из $\mathscr{A}$ и $\mathscr{A} \,|\, (\mathscr{B} \,|\, \mathscr{C})$, и единственная схема аксиом

$$(\mathscr{A} \,|\, (\mathscr{B} \,|\, \mathscr{C})) \,|\, \{[\mathscr{D} \,|\, (\mathscr{D} \,|\, \mathscr{D})] \,|\, [(\mathscr{E} \,|\, \mathscr{B}) \,|\, ((\mathscr{A} \,|\, \mathscr{E}) \,|\, (\mathscr{A} \,|\, \mathscr{E}))]\}.$$

Дальнейшие сведения из этой области, в том числе и исторический обзор, можно найти в книге Чёрча [1956].

Упражнения

1. Доказать, что если схему аксиом (A3) в системе L заменить схемой аксиом $(\neg \mathscr{A} \supset \neg \mathscr{B}) \supset (\mathscr{B} \supset \mathscr{A})$, то класс теорем от этого не изменится.

2. *Интуиционистским* исчислением высказываний называется система L_I, которая получается из системы L_4 заменой в ней схемы аксиом (10) схемой (10)′: $\neg \mathscr{A} \supset (\mathscr{A} \supset \mathscr{B})$.

(a) Рассмотрим $n+1$-значную логику с единственным выделенным истинностным значением 0 и связками, определяемыми следующим образом: $\neg \mathscr{A}$ есть 0, если $\mathscr{A}$ есть n, и $\neg \mathscr{A}$ есть n в остальных случаях. $\mathscr{A} \,\&\, \mathscr{B}$ всегда равно максимуму значений $\mathscr{A}$ и $\mathscr{B}$, а $\mathscr{A} \vee \mathscr{B}$ — их минимуму; $\mathscr{A} \supset \mathscr{B}$ есть 0, если значение $\mathscr{A}$ не меньше значения $\mathscr{B}$, в противном случае $\mathscr{A} \supset \mathscr{B}$ есть $\mathscr{B}$. Показать, что все теоремы L_I являются выделенными.

(b) $A_1 \vee \neg A_1$ и $\neg \neg A_1 \supset A_1$ не принадлежат к числу теорем L_I

(c) Для любого m формула

$$(A_1 \equiv A_2) \vee \ldots \vee (A_1 \equiv A_m) \vee (A_2 \equiv A_3) \vee \ldots \vee (A_2 \equiv A_m) \vee \ldots \vee (A_{m-1} \equiv A_m)$$

не является теоремой.

(d) (Гёдель [1933].) Теория L_I не является подходящей ни для какой конечной многозначной логики.

(e) (i) Если Γ, $\mathscr{A} \vdash_{L_I} \mathscr{B}$, то $\Gamma \vdash_{L_I} \mathscr{A} \supset \mathscr{B}$ (теорема дедукции);

(ii) $\mathscr{A} \supset \mathscr{B}$, $\mathscr{B} \supset \mathscr{C} \vdash_{L_I} \mathscr{A} \supset \mathscr{C}$;

(iii) $\vdash_{L_I} \mathscr{A} \supset \neg\neg\mathscr{A}$;

(iv) $\vdash_{L_I} (\mathscr{A} \supset \mathscr{B}) \supset (\neg\mathscr{B} \supset \neg\mathscr{A})$;

(v) $\vdash_{L_I} \mathscr{A} \supset (\neg\mathscr{A} \supset \mathscr{B})$;

(vi) $\vdash_{L_I} \neg\neg(\neg\neg\mathscr{A} \supset \mathscr{A})$;

(vii) $\neg\neg(\mathscr{A} \supset \mathscr{B})$, $\neg\neg\mathscr{A} \vdash_{L_I} \neg\neg\mathscr{B}$;

(viii) $\vdash_{L_I} \neg\neg\neg\mathscr{A} \supset \neg\mathscr{A}$.

[D] (f) $\vdash_{L_I} \neg\neg\mathscr{A}$ тогда и только тогда, когда $\mathscr{A}$ есть тавтология.

(g) $\vdash_{L_I} \neg\mathscr{A}$ тогда и только тогда, когда $\neg\mathscr{A}$ есть тавтология.

[D] (h) Если $\mathscr{A}$ не содержит связок, отличных от & и $\neg$, то $\vdash_{L_I} \mathscr{A}$ тогда и только тогда, когда $\mathscr{A}$ есть тавтология.

Подробнее об интуиционистской логике см. Гейтинг [1956], Клини [1945], Яськовский [1936]. В последней из названных работ доказывается, что интуиционистская система L_I является теорией, подходящей для некоторой многозначной логики с перечислимым множеством истинностных значений.

[A] **3.** Пусть $\mathscr{A}$ и $\mathscr{B}$ находятся в отношении R тогда и только тогда, когда $\vdash_L \mathscr{A} \equiv \mathscr{B}$. Доказать, что R есть отношение эквивалентности. Для произвольных классов эквивалентности $[\mathscr{A}]$ и $[\mathscr{B}]$ пусть $[\mathscr{A}] \cup [\mathscr{B}] = [\mathscr{A} \vee \mathscr{B}]$, $[\mathscr{A}] \cap [\mathscr{B}] = [\mathscr{A} \,\&\, \mathscr{B}]$ и $\overline{[\mathscr{A}]} = [\neg\mathscr{A}]$. Показать, что порожденные отношением R классы эквивалентности образуют булеву алгебру относительно операций $\cup$, $\cap$, $^-$. Эта алгебра называется *алгеброй Линденбаума*, порожденной теорией L, и обозначается через L*. Нулевым элементом 0 алгебры L* является класс всех противоречий (т. е. отрицаний тавтологий). Единицей 1 алгебры L* является класс эквивалентности, состоящий из всех тавтологий. Заметим, что $\vdash_L \mathscr{A} \supset \mathscr{B}$ тогда и только тогда, когда $[\mathscr{A}] \leqslant [\mathscr{B}]$ в L*, и что $\vdash_L \mathscr{A} \equiv \mathscr{B}$ тогда и только тогда, когда $[\mathscr{A}] = [\mathscr{B}]$. Доказать, что всякая булева функция f (построенная с помощью $\cup$, $\cap$, $^-$ из переменных, 0 и 1) тождественно равна 1 тогда и только тогда, когда $\vdash_L f\#$, где $f\#$ получается из f заменой $\cup$, $\cap$, $^-$, 0, 1 соответственно на $\vee$, &, $\neg$, A_1 & $\neg A_1$, $A_1 \vee \neg A_1$.

Глава 2

Теории первого порядка

§ 1. Кванторы

Существуют такие виды логических рассуждений, которые не могут быть обоснованы в рамках исчисления высказываний. Вот примеры таких рассуждений:

(1) Всякий друг Мартина есть друг Джона. Питер не есть друг Джона. Следовательно, Питер не есть друг Мартина.

(2) Все люди бессмертны. Сократ — человек. Следовательно, Сократ бессмертен.

(3) Все люди — животные. Следовательно, голова человека есть голова животного.

Корректность этих умозаключений покоится не только на истинностно-функциональных отношениях между входящими в них предложениями, но и на внутренней структуре самих предложений, а также и на понимании таких выражений, как «все», «всякий» и т. д.

Чтобы сделать более прозрачной структуру сложных высказываний, удобно ввести специальные обозначения для некоторых часто встречающихся выражений. Если $P(x)$ означает, что x обладает свойством P, то договоримся посредством $\forall x P(x)$ обозначать утверждение: «для всякого предмета x свойство P выполнено», или, другими словами, «все x обладают свойством P». Запись $\exists x P(x)$ будет означать, что «существует предмет x, обладающий свойством P», т. е. «существует по крайней мере один предмет x, обладающий свойством P». В выражении $\forall x P(x)$ часть $\forall x$ называется *квантором всеобщности*, а часть $\exists x$ в выражении $\exists x P(x)$ называется *квантором существования*. Изучение кванторов как логических операций и связанных с ними понятий и составляет основной предмет этой главы (отсюда и название этой главы: «Quantification Theory» в оригинале. — *Прим. перев.*).

Примеры. Пусть m, j, p, s, $F(x, y)$, $M(x)$, $I(x)$, $A(x)$, $h(x)$ обозначают соответственно «Мартин», «Джон», «Питер», «Сократ», «x есть друг y», «x есть человек», «x бессмертен», «x есть животное», «голова x». Тогда рассуждения (1) — (3) можно записать следующим образом:

(1′)
$$\frac{\forall x\,(F(x, m) \supset F(x, j))\quad \neg F(p, j)}{\neg F(p, m)};$$

(2′) $$\frac{\forall x\,(M(x) \supset I(x)) \qquad M(s)}{I(s)};$$

(3′) $$\frac{\mathbf{A}x\,(M(x) \supset A(x))}{\forall x\,(\exists y\,(x = h(y)\,\&M(y)) \supset \exists y\,(x = h(y)\,\&A(y)))}.$$

Заметим, что справедливость этих заключений не зависит от того, какой конкретный смысл имеют символы m, j, p, s, F, M, I, A и h.

Подобно тому как пропозициональные формы были использованы для выявления логической структуры, зависящей только от пропозициональных связок, можно и умозаключения (такие, как (1) — (3)), содержащие кванторы, представлять в абстрактной форме, как это было сделано в (1′) — (3′). Для этой цели мы используем запятые, скобки, символы исчисления высказываний $\neg$ и $\supset$, *предметные* (*индивидные*) *переменные* $x_1, x_2, \ldots, x_n, \ldots$, *предметные* (*индивидные*) *константы* $a_1, a_2, \ldots, a_n, \ldots$, *предикатные буквы* $A_1^1, A_1^2, \ldots, A_k^j, \ldots$ и *функциональные буквы* $f_1^1, f_1^2, \ldots, f_k^j, \ldots$ Верхний индекс предикатной или функциональной буквы указывает число аргументов, а нижний индекс служит для различения букв с одним и тем же числом аргументов. В приведенных выше примерах m, j, p, s были предметными константами, F и $=$ — двуместными предикатными буквами (т. е. буквами с двумя аргументами), M, I, A — одноместными предикатными буквами (т. е. буквами с одним аргументом), буква h играла роль функциональной буквы с одним аргументом.

Функциональные буквы, примененные к предметным переменным и константам, порождают *термы*. Точнее:

(a) всякая предметная переменная или предметная константа есть терм;

(b) если f_i^n — функциональная буква и $t_1, \ldots, t_n$ — термы, то $f_i^n(t_1, \ldots, t_n)$ есть терм;

(c) выражение является термом только в том случае, если это следует из правил (a) и (b).

Предикатные буквы, примененные к термам, порождают *элементарные формулы*, или точнее: если A_i^n — предикатная буква, а $t_1, \ldots, t_n$ — термы, то $A_i^n(t_1, \ldots, t_n)$ — элементарная формула.

Формулы исчисления предикатов определяются следующим образом:

(a) всякая элементарная формула есть формула,

(b) если $\mathscr{A}$ и $\mathscr{B}$ — формулы и y — предметная переменная, то каждое из выражений $(\neg\mathscr{A})$, $(\mathscr{A} \supset \mathscr{B})$ и $(\forall y\mathscr{A})$ есть формула,

(c) выражение является формулой только в том случае, если это следует из правил (a) и (b).

В выражении $(\forall y\mathscr{A})$ «$\mathscr{A}$» называется *областью действия квантора* $\forall y$. Заметим, что $\mathscr{A}$ может и не содержать переменной y, в таком случае мы обычно считаем, что содержательный смысл $\mathscr{A}$ и $(\forall y\mathscr{A})$ одинаков. Выражения $\mathscr{A}\,\&\mathscr{B}$, $\mathscr{A} \vee \mathscr{B}$, $\mathscr{A} \equiv \mathscr{B}$ определяются так же, как в системе L исчисления высказываний (см. стр. 38). Нет

необходимости включать в число основных символов знак $\exists$ для квантора существования, так как мы можем определить $\exists x \mathscr{A}$ как сокращенную запись для $\neg(\forall x(\neg \mathscr{A}))$. Такое определение, очевидно, правильно отражает содержательный смысл кванторов.

Оставляя в силе принятые в главе 1 соглашения об опускании скобок, договоримся дополнительно считать, что кванторы $\forall y$ и $\exists y$ располагаются по силе между связками $\equiv$, $\supset$ и связками $\vee$, $\&$, $\neg$.

Примеры. Вместо $((\forall x_1 A_1^1(x_1)) \supset A_1^3(x_1, x_2))$ пишем $\forall x_1 A_1^1(x_1) \supset \supset A_1^3(x_1, x_2)$, а вместо $(\forall x_1 (A_1^1(x_1) \vee A_1^3(x_1, x_2)))$ пишем $\forall x_1 A_1^1(x_1) \vee \vee A_1^3(x_1, x_2)$.

Упражнение

Восстановить скобки в

$$\forall x_2 \neg A_1^1(x_1) \supset A_3^3(x_1, x_2, x_3) \vee \forall x_1 A_2^1(x_1)$$

и в

$$\neg \forall x_1 A_1^1(x_1) \supset \exists x_2 A_2^1(x_2) \supset A_1^2(x_1, x_2) \vee A_1^1(x_2).$$

Договоримся также опускать скобки, в которые заключается формула $Q\mathscr{A}$ в формулах вида $Q_1(Q\mathscr{A})$, где Q и Q_1 — любые кванторы.

Пример. Вместо $(\forall x_1 (\exists x_2 (\forall x_4 A_1^3(x_1, x_2, x_4))))$ пишем формулу $\forall x_1 \exists x_2 \forall x_4 A_1^3(x_1, x_2, x_4)$.

Упражнение

Восстановить скобки в $\forall x_1 \forall x_3 \forall x_4 A_1^1(x_1) \supset A_2^1(x_3) \& \neg A_1^1(x_1)$ и в $\exists x_1 \forall x_2 \exists x_3 A_1^1(x_1) \vee \exists x_2 \neg \forall x_3 A_1^2(x_3, x_2)$.

Введем понятия *свободного* и *связанного* вхождения переменной в формулу: вхождение переменной x в данную формулу называется *связанным*, если x является переменной входящего в эту формулу квантора $\forall x$ или находится в области действия входящего в эту формулу квантора $\forall x$; в противном случае вхождение переменной x в данную формулу называется *свободным*.

Примеры

(i) $A_1^2(x_1, x_2)$;

(ii) $A_1^2(x_1, x_2) \supset \forall x_1 A_1^1(x_1)$;

(iii) $\forall x_1 (A_1^2(x_1, x_2) \supset \forall x_1 A_1^1(x_1))$.

Единственное в формуле (i) вхождение переменной x_1 свободно. Первое вхождение переменной x_1 в формулу (ii) свободно, а второе и третье — связанные. Все вхождения x_1 в формулу (iii) являются связанными. Каждое вхождение переменной x_2 во всех трех формулах свободно. Заметим, что одна и та же переменная может иметь свободные и связанные вхождения в одну и ту же формулу, как это имеет место, например, в (ii). Заметим также, что вхождение переменной может быть

связанным в той или иной формуле $\mathscr{A}$ и в то же время свободным в некоторой подформуле формулы $\mathscr{A}$; так, например, первое вхождение x_1 в формулу (ii) свободно, но (ii) является подформулой формулы (iii), где то же вхождение x_1 оказывается связанным.

Упражнения

Указать свободные и связанные вхождения переменных в следующие формулы:

1. $\forall x_3 (\forall x_1 A_1^2(x_1, x_3) \supset A_1^2(x_3, x_1))$.
2. $\forall x_2 A_1^2(x_3, x_2) \supset \forall x_3 A_1^2(x_3, x_2)$.
3. $(\forall x_2 \exists x_1 A_1^3(x_1, x_2, f_1^2(x_1, x_2))) \vee \neg \forall x_1 A_1^2(x_2, f_1^1(x_1))$.

Переменная называется *свободной* (*связанной*) *переменной* в данной формуле, если существуют свободные (связанные) ее вхождения в эту формулу. Таким образом, переменная может быть одновременно свободной и связанной в одной и той же формуле. Такова, например, переменная x_1 в примере (ii).

Пусть $x_{i_1}, \ldots, x_{i_k}$ — переменные и $\mathscr{A}$ — формула. Не обращая внимания на то, являются ли эти переменные свободными в $\mathscr{A}$ и существуют ли в $\mathscr{A}$ другие свободные переменные, мы будем иногда применять запись $\mathscr{A}(x_{i_1}, \ldots, x_{i_k})$ для обозначения формулы $\mathscr{A}$ с тем, чтобы затем через $\mathscr{A}(t_1, \ldots, t_k)$ обозначать результат подстановки термов $t_1, \ldots, t_k$ соответственно вместо свободных вхождений в $\mathscr{A}$ (если таковые имеются!) переменных $x_{i_1}, \ldots, x_{i_k}$.

Терм t называется *свободным для переменной* x_i в формуле $\mathscr{A}$, если никакое свободное вхождение x_i в $\mathscr{A}$ не лежит в области действия никакого квантора $\forall x_j$, где x_j — переменная, входящая в t.

Примеры. (a) Терм x_j свободен для x_i в $A_1^1(x_i)$, но не свободен для x_i в $\forall x_j A_1^1(x_i)$. Терм $f_1^2(x_1, x_3)$ свободен для x_1 в $\forall x_2 A_1^2(x_1, x_2) \supset \supset A_1^1(x_1)$, но не свободен для x_1 в $\exists x_3 \forall x_2 A_1^2(x_1, x_2) \supset A_1^1(x_1)$.

(b) Всякий терм, не содержащий переменных, свободен для любой переменной в любой формуле.

(c) Терм t свободен для любой переменной в формуле $\mathscr{A}$, если никакая переменная терма t не является связанной переменной в $\mathscr{A}$.

(d) x_i свободно для x_i в любой формуле.

(e) Всякий терм свободен для x_i в $\mathscr{A}$, если $\mathscr{A}$ не содержит свободных вхождений x_i.

Упражнения

1. Свободен ли терм $f_1^2(x_1, x_2)$ для x_1 в формулах $A_1^3(x_1, x_2) \supset \forall x_2 A_1^1(x_2)$, $(\forall x_2 A_1^2(x_2, a_1)) \vee \exists x_2 A_1^2(x_1, x_2)$?

2. Перевести следующие предложения на язык формул:

(a) Все рыбы, кроме акул, добры к детям.

(b) Либо всякий любитель выпивки весьма общителен, либо некий ростовщик честен и не пьет вина.

(c) Не все птицы могут летать.

(d) Либо каждый любит кого-нибудь, и ни один не любит всех; либо некто любит всех, и кто-то не любит никого.

(e) Ты можешь обманывать кое-кого все время, ты можешь обманывать всех некоторое время, но ты не можешь обманывать всех все время.

(f) Некоторые остроумны, только когда пьяны.

(g) Ни один политикан не честен.

(h) Если кто-нибудь может сделать это, то и Джон может.

(i) Всякий, в ком есть упорство, может изучить логику.

(j) Если всякий разумный философ — циник и только женщины являются разумными философами, то тогда, если существуют разумные философы, то некоторые из женщин — циники.

§ 2. Интерпретации. Выполнимость и истинность. Модели

Формулы имеют смысл только тогда, когда имеется какая-нибудь интерпретация входящих в нее символов. Под *интерпретацией* мы будем понимать всякую систему, состоящую из непустого множества D, называемого *областью* интерпретации, и какого-либо соответствия, относящего каждой предикатной букве A_j^n некоторое n-местное отношение в D, каждой функциональной букве f_j^n — некоторую n-местную операцию в D (т. е. функцию, отображающую D^n в D) и каждой предметной постоянной a_i — некоторый элемент из D. При заданной интерпретации предметные переменные мыслятся пробегающими область D этой интерпретации, а связкам $\neg$, $\supset$ и кванторам придается их обычный смысл. (Напомним, что всякое n-местное отношение в D может рассматриваться как некоторое подмножество множества D^n всех n-ок элементов из D. Например, если D есть множество человеческих существ, то отношение между двумя людьми, состоящее в том, что первый из них приходится отцом другому, можно отождествить с множеством всех упорядоченных пар (людей) (x, y) таких, что x является отцом y.)

Для данной интерпретации всякая формула без свободных переменных (или, иначе, *замкнутая формула*) представляет собой высказывание, которое истинно или ложно, а всякая формула со свободными переменными выражает некоторое отношение на области интерпретации; это отношение может быть выполнено (истинно) для одних значений переменных из области интерпретации и не выполнено (ложно) для других.

Примеры

(i) $A_1^2(x_1, x_2)$;

(ii) $\forall x_2 A_1^2(x_1, x_2)$;

(iii) $\exists x_2 \forall x_1 A_1^2(x_2, x_1)$.

Если мы берем в качестве области множество целых положительных чисел и интерпретируем $A_1^2(y, z)$ как $y \leqslant z$, то (i) представляет отношение $y \leqslant z$, которое выполнено для всех упорядоченных пар (a, b) целых положительных чисел таких, что $a \leqslant b$; (ii) представляет свойство (т. е. отношение с одним аргументом) «для каждого целого положительного y, $y \leqslant z$», которое выполнено только для числа 1; наконец, (iii)

оказывается истинным высказыванием, утверждающим существование наименьшего целого положительного числа. Если бы мы взяли в качестве области множество всех целых чисел, то (iii) оказалось бы ложным.

Упражнения

(1) $A_1^2(f_1^2(x_1, x_2), a_1)$;

(2) $A_1^2(x_1, x_2) \supset A_1^2(x_2, x_1)$;

(3) $\forall x_1 \forall x_2 \forall x_3 (A_1^2(x_1, x_2) \supset (A_1^2(x_2, x_3) \supset A_1^2(x_1, x_3)))$.

Для следующих интерпретаций и для каждой из формул (1), (2), (3) указать, при каких значениях свободных переменных эти формулы выполнены (если они имеют свободные переменные), или выяснить, являются ли они ложными или истинными высказываниями (если они не содержат свободных переменных).

(a) В качестве области берется множество всех целых положительных чисел, $A_1^2(y, z)$, $f_1^2(x, z)$ и a_1 интерпретируются соответственно как $y \geqq z$, $y \cdot z$, 1.

(b) В качестве области берется множество всех человеческих существ, $A_1^2(y, z)$, $f_1^2(y, z)$ и a_1 интерпретируются соответственно как «y любит z», «z» и «Гитлер».

(c) В качестве области берется множество всех множеств целых чисел, $A_1^2(y, z)$, $f_1^2(y, z)$ и a_1 интерпретируются соответственно как $y \supseteq z$, $y \cup z$ и 0 (пустое множество).

Понятия выполнимости и истинности интуитивно ясны, но для скептика они могут быть уточнены следующим образом (Тарский [1936]). Пусть дана некоторая интерпретация с областью D, и пусть Σ есть множество всех счетных последовательностей элементов из D. Мы сейчас определим, что значит, что формула $\mathscr{A}$ выполнена на последовательности $s = (b_1, b_2, \ldots)$ из Σ при данной интерпретации.

Предварительно мы определим одноместную функцию s* со значениями из D и определенную на множестве всех термов.

(1) Если терм t есть предметная переменная x_i, то $s^*(t) = b_i$.

(2) Если терм t есть предметная константа, то $s^*(t)$ совпадает с интерпретацией этой константы в D.

(3) Если f_j^n есть функциональная буква, интерпретируемая операцией g в D, и $t_1, \ldots, t_n$ — термы, то $s^*(f_j^n(t_1, \ldots, t_n)) = g(s^*(t_1), \ldots, s^*(t_n))$.

Таким образом, s* — это функция, определяемая последовательностью s и отображающая множество всех термов в D. Если говорить неформально, то для любой последовательности $s = (b_1, b_2, \ldots)$ и для любого терма t $s^*(t)$ есть элемент множества D, который получается в результате подстановки при каждом i элемента b_i на места всех вхождений переменной x_i в терм t и затем выполнения всех операций интерпретации, соответствующих функциональным буквам терма t. Например, если t есть $f_2^2(x_3, f_1^2(x_1, a_1))$, областью интерпретации служит множество целых чисел, f_2^2 и f_1^2 интерпретируются соответственно как обычные умножение и сложение, а a_1 — как 2; то для всякой последовательности $s^* = (b_1, b_2, \ldots)$ целых чисел $s^*(t)$ представляет собой целое число $b_3 \times (b_1 + 2)$.

Перейдем теперь к основному определению, которое сформулируем, следуя индуктивным шагам определения формулы.

(i) Если $\mathscr{A}$ есть элементарная формула $A_j^n(t_1, \ldots, t_n)$ и B_j^n есть соответствующее ей отношение в интерпретации, то формула $\mathscr{A}$ считается выполненной на последовательности s в том и только в том случае, когда $B_j^n(\mathrm{s}^*(t_1), \ldots, \mathrm{s}^*(t_n))$, то есть если n-ка $(\mathrm{s}^*(t_1), \ldots, \mathrm{s}^*(t_n))$ принадлежит отношению B_j^n *).

(ii) Формула $\neg\mathscr{A}$ выполнена на s тогда и только тогда, когда формула $\mathscr{A}$ не выполнена на s.

(iii) Формула $\mathscr{A} \supset \mathscr{B}$ выполнена на s тогда и только тогда, когда формула $\mathscr{A}$ не выполнена на s или когда формула $\mathscr{B}$ выполнена на s.

(iv) Формула $\forall x_i \mathscr{A}$ выполнена на s тогда и только тогда, когда формула $\mathscr{A}$ выполнена на любой последовательности из Σ, отличающейся от s не более чем своей i-й компонентой.

Иначе говоря, формула $\mathscr{A}$ выполнена на последовательности $\mathrm{s} = (\mathrm{b}_1, \mathrm{b}_2, \ldots)$ тогда и только тогда, когда подстановка при каждом l символа, представляющего b_i, на места всех свободных вхождений x_i в $\mathscr{A}$ приводит к истинному в данной интерпретации предложению.

Формула $\mathscr{A}$ называется *истинной* (в данной интерпретации) тогда и только тогда, когда она выполнена на всякой последовательности из Σ.

Формула $\mathscr{A}$ называется *ложной* (в данной интерпретации), если она не выполнена ни на одной последовательности из Σ.

Данная интерпретация называется *моделью* для данного множества формул Γ, если каждая формула из Γ истинна в данной интерпретации.

Читателю предоставляется самому убедиться в справедливости формулируемых ниже следствий из определений. (Следствия эти в большинстве своем тоже очевидны, если пользоваться обычными интуитивными понятиями истинности и выполнимости.)

(I) $\mathscr{A}$ ложно в данной интерпретации тогда и только тогда, когда $\neg\mathscr{A}$ истинно в той же интерпретации, и $\mathscr{A}$ истинно тогда и только тогда, когда $\neg\mathscr{A}$ ложно.

(II) Никакая формула не может быть одновременно истинной и ложной в одной и той же интерпретации.

(III) Если в данной интерпретации истинны $\mathscr{A}$ и $\mathscr{A} \supset \mathscr{B}$, то истинно и $\mathscr{B}$.

---

*) Так, например, если областью интерпретации служит множество вещественных чисел, а A_1^2 и $f_1^1(x)$ интерпретируются соответственно как $\leqslant$ и e^x, то формула $A_1^2(f_1^1(x_1), x_5)$ выполнена на последовательности $\mathrm{s} = (\mathrm{b}_1, \mathrm{b}_2, \ldots)$ тогда и только тогда, когда $e^{\mathrm{b}_1} \leqslant \mathrm{b}_5$. Если мы возьмем в качестве области множество точек плоскости, в качестве интерпретации $A_1^3(x, y, z)$ отношение «x и y равноудалены от z», а $f_1^2(x, y)$ проинтерпретируем как среднюю точку прямолинейного отрезка с концами в x и y, то формула $A_1^3(f_1^2(x_1, x_2), f_1^2(x_3, x_1), x_4)$ будет выполнена на последовательности $\mathrm{s} = (\mathrm{b}_1, \mathrm{b}_2, \ldots)$ тогда и только тогда, когда средние точки отрезков с концами b_1, b_2 и b_3, b_1 будут находиться на равном расстоянии от b_4. Если областью является множество целых чисел, а $A_1^1(x, y, u, v)$ и a_1 интерпретируются соответственно как $\mathrm{x} \cdot \mathrm{v} = \mathrm{u} \cdot \mathrm{y}$ и 2, то формула $A_1^1(x_3, a_1, x_1, x_3)$ выполнена на $\mathrm{s} = (\mathrm{b}_1, \mathrm{b}_2, \ldots)$ тогда и только тогда, когда $\mathrm{b}_3^3 = 2\mathrm{b}_1$.

(IV) $\mathscr{A} \supset \mathscr{B}$ ложно в данной интерпретации тогда и только тогда, когда $\mathscr{A}$ в этой интерпретации истинно, а $\mathscr{B}$ ложно.

(V) (i) $\mathscr{A} \,\&\, \mathscr{B}$ выполнено на последовательности $\mathfrak{s}$ тогда и только тогда, когда $\mathscr{A}$ выполнено на $\mathfrak{s}$ и $\mathscr{B}$ выполнено на $\mathfrak{s}$. $\mathscr{A} \vee \mathscr{B}$ выполнено на $\mathfrak{s}$ тогда и только тогда, когда $\mathscr{A}$ выполнено на $\mathfrak{s}$ или $\mathscr{B}$ выполнено на $\mathfrak{s}$. $\mathscr{A} \equiv \mathscr{B}$ выполнено на $\mathfrak{s}$ тогда и только тогда, когда либо $\mathscr{A}$ выполнено на $\mathfrak{s}$ и $\mathscr{B}$ выполнено на $\mathfrak{s}$, либо $\mathscr{A}$ не выполнено на $\mathfrak{s}$ и $\mathscr{B}$ не выполнено на $\mathfrak{s}$ *).

(ii) $\exists x_i \mathscr{A}$ выполнено на $\mathfrak{s}$ тогда и только тогда, когда $\mathscr{A}$ выполнено хотя бы на одной последовательности $\mathfrak{s}'$, отличающейся от $\mathfrak{s}$ не более чем одной только i-й компонентой*).

(VI) $\mathscr{A}$ истинно в данной интерпретации тогда и только тогда, когда в этой интерпретации истинно $\forall x_i \mathscr{A}$. *Замыканием* данной формулы $\mathscr{A}$ назовем формулу, которая получается приписыванием к $\mathscr{A}$ спереди знаков кванторов всеобщности, содержащих в порядке убывания индексов все свободные переменные, входящие в $\mathscr{A}$. Замыканием формулы $\mathscr{A}$, не содержащей свободных переменных, будем называть саму формулу $\mathscr{A}$. (Например, если $\mathscr{A}$ есть $A_1^2(x_2, x_5) \supset \neg \exists x_2 A_1^3(x_1, x_2, x_3)$, то замыканием $\mathscr{A}$ будет формула $\forall x_5 \forall x_3 \forall x_2 \forall x_1 \mathscr{A}$.)

(VII) Всякий частный случай всякой тавтологии истинен во всякой интерпретации. (Частным случаем данной пропозициональной формы мы называем всякую формулу, получаемую подстановкой формул в эту пропозициональную форму вместо пропозициональных букв с тем условием, чтобы вместо всех вхождений одной и той же пропозициональной буквы подставлялась одна и та же формула.) (Указание. Показать, что все частные случаи аксиом системы L истинны, а затем применить (III) и предложение 1.13.)

(VIII) Пусть свободные переменные (если таковые имеются) формулы $\mathscr{A}$ содержатся среди переменных $x_{i_1}, \ldots, x_{i_n}$. Тогда если у последовательностей $\mathfrak{s}$ и $\mathfrak{s}'$ компоненты с номерами $i_1, \ldots, i_n$ совпадают, то формула $\mathscr{A}$ выполнена на $\mathfrak{s}$ тогда и только тогда, когда она выполнена на $\mathfrak{s}'$. (Указание. Индукция по числу связок и кванторов в $\mathscr{A}$. Сначала доказать, что если переменные терма t встречаются среди $x_{i_1}, \ldots, x_{i_n}$, а члены последовательностей $\mathfrak{s}$ и $\mathfrak{s}'$ с номерами $i_1, \ldots, i_n$ совпадают, то $\mathfrak{s}^*(t) = (\mathfrak{s}')^*(t)$. В частности, если t не содержит переменных, то $\mathfrak{s}_1^*(t) = \mathfrak{s}_2^*(t)$ для любых вообще последовательностей $\mathfrak{s}_1$ и $\mathfrak{s}_2$.) (Хотя, в силу (VIII), всякая формула с n свободными переменными выполнена или не выполнена по существу только на n-ках, а не на бесконечных последовательностях, все же общую теорию выполнимости для всех формул сразу удобнее развивать в терминах не конечных, а бесконечных последовательностей.)

---

*) Напомним, что $\mathscr{A} \,\&\, \mathscr{B}$, $\mathscr{A} \vee \mathscr{B}$, $\mathscr{A} \equiv \mathscr{B}$, $\exists x_i \mathscr{A}$ являются сокращениями для $\neg(\mathscr{A} \supset \neg \mathscr{B})$, $\neg \mathscr{A} \supset \mathscr{B}$, $(\mathscr{A} \supset \mathscr{B}) \,\&\, (\mathscr{B} \supset \mathscr{A})$ и $\neg \forall x_i \neg \mathscr{A}$ соответственно.

Множество всех n-ок $(b_{i_1}, \ldots, b_{i_n})$ элементов области D таких, что формула $\mathscr{A}$ выполнена на всякой последовательности s, у которой i_1-я, ..., i_n-я компоненты совпадают соответственно с $b_{i_1}, \ldots, b_{i_n}$, называется отношением (или свойством) интерпретации, соответствующим формуле $\mathscr{A}$*). Пусть, например, областью D служит множество всех человеческих существ, $A_1^2(x, y)$ и $A_2^2(x, y)$ интерпретируются соответственно как «x есть брат y» и «x есть родитель y»; тогда бинарное отношение в D, соответствующее формуле $\exists x_3(A_1^2(x_1, x_3) \& A_2^2(x_3, x_2))$, представляет собой отношение родства, связывающее дядю и племянника. Если в качестве области D взять множество целых положительных чисел, а A_1^2, f_1^2 и a_1 интерпретировать соответственно как $=$, умножение и 1, то формуле

$$\neg A_1^2(x_1, a_1) \& \forall x_2(\exists x_3 A_1^2(x_1, f_1^2(x_2, x_3)) \supset A_1^2(x_2, x_1) \vee A_1^2(x_2, a_1))$$

будет соответствовать в указанном смысле свойство числа быть простым.

(IX) Если формула $\mathscr{A}$ замкнута, то в любой данной интерпретации либо истинно $\mathscr{A}$, либо истинно $\neg\mathscr{A}$ (т. е. ложно $\mathscr{A}$). (Указание. Следует из (VIII).) При этом, разумеется, $\mathscr{A}$ может быть истинно в одних интерпретациях и ложно в других (например, $A_1^1(a_1)$).

Незамкнутая, т. е. содержащая свободные переменные, формула $\mathscr{A}$ может в некоторых интерпретациях быть и не истинной и не ложной. Пусть, например, $\mathscr{A}$ есть $A_1^2(x_1, x_2)$. Рассмотрим интерпретацию, областью которой служит множество целых чисел и в которой $A_1^2(x_1, x_2)$ интерпретируется как $x < y$. В этой интерпретации $\mathscr{A}$ выполнено только на последовательностях $s = (b_1, b_2, \ldots)$, удовлетворяющих условию $b_1 < b_2$. Следовательно, в этой интерпретации рассматриваемая формула $\mathscr{A}$ не истинна и не ложна.

(X) Лемма. *Пусть t и v — термы, s — последовательность из Σ, t' получается из t подстановкой v вместо всех вхождений x_i и s' получается из s заменой в ней ее i-й компоненты на $s^*(v)$; тогда $s^*(t') = (s')^*(t)$.* (Указание. Индукция по длине t**).)

Пусть теперь $\mathscr{A}(x_i)$ — формула, t — терм, свободный для x_i в $\mathscr{A}(x_i)$, и $\mathscr{A}(t)$ — формула, полученная подстановкой t вместо всех свободных вхождений x_i в $\mathscr{A}(x_i)$. Утверждается, что формула $\mathscr{A}(t)$ выполнена на последовательности $s = (b_1, b_2, \ldots)$ тогда и только тогда, когда $\mathscr{A}(x_i)$ выполнена на последовательности s', полученной из s подстановкой $s^*(t)$ в s вместо b_i. (Указание. Индукция по числу связок и кванторов в $\mathscr{A}(x_i)$ с применением леммы.)

Следствие. *Если на последовательности s выполнена формула $\forall x_i \mathscr{A}(x_i)$ и терм t свободен для x_i в $\mathscr{A}(x_i)$, то выполнена и формула $\mathscr{A}(t)$. Следовательно, формула $\forall x_i \mathscr{A}(x_i) \supset \mathscr{A}(t)$ истинна в каждой интерпретации.*

---

*) Здесь предполагается, что $x_{i_1}, \ldots, x_{i_n}$ — все свободные переменные формулы $\mathscr{A}$.

**) Длиной данного выражения называется число всех вхождений символов в это выражение.

(XI) Если формула $\mathscr{A}$ не содержит x_i в качестве свободной переменной, то формула

$$\forall x_i (\mathscr{A} \supset \mathscr{B}) \supset (\mathscr{A} \supset \forall x_i \mathscr{B})$$

истинна во всякой интерпретации.

Упражнение

Доказать (I) — (XI). В качестве примера докажем (XI). Допустим, что (XI) неверно. Это значит, что при некоторых $\mathscr{A}$ и $\mathscr{B}$ формула $\forall x_i (\mathscr{A} \supset \mathscr{B}) \supset (\mathscr{A} \supset \forall x_i \mathscr{B})$ не истинна в некоторой интерпретации. Согласно пункту (iii) последнего определения, должна существовать последовательность s, на которой $\forall x_i (\mathscr{A} \supset \mathscr{B})$ выполнено, а $(\mathscr{A} \supset \forall x_i \mathscr{B})$ не выполнено. Тогда опять по тому же пункту (iii) на этой последовательности s выполнено $\mathscr{A}$ и не выполнено $\forall x_i \mathscr{B}$. Следовательно, в силу пункта (iv) того же определения, существует последовательность s′, быть может, отличающаяся от s одной лишь i-й компонентой, на которой не выполнено $\mathscr{B}$. Поскольку x_i не является свободной переменной ни в $\forall x_i (\mathscr{A} \supset \mathscr{B})$, ни в $\mathscr{A}$, а сами эти формулы выполнены на s, то, в силу (VIII), они выполнены и на s′. Из того, что $\forall x_i (\mathscr{A} \supset \mathscr{B})$ выполнено на s′, согласно (iv) вытекает, что и $\mathscr{A} \supset \mathscr{B}$ выполнено на s′. Таким образом, $\mathscr{A} \supset \mathscr{B}$ и $\mathscr{A}$ выполнены на s′, откуда, по пункту (iii) определения, следует, что и $\mathscr{B}$ выполнено на s′. Мы пришли к противоречию с тем, что $\mathscr{B}$ не выполнено на s′. (XI) доказано.

Формула $\mathscr{A}$ называется *логически общезначимой* (в исчислении предикатов), если она истинна в каждой интерпретации.

Формула $\mathscr{A}$ называется *выполнимой* (в исчислении предикатов), если существует интерпретация, в которой $\mathscr{A}$ выполнима хотя бы на одной последовательности из Σ.

Очевидно, что формула $\mathscr{A}$ логически общезначима тогда и только тогда, когда формула $\neg\mathscr{A}$ не является выполнимой, и формула $\mathscr{A}$ выполнима тогда и только тогда, когда формула $\neg\mathscr{A}$ не является логически общезначимой. Как мы знаем, во всякой интерпретации всякая замкнутая формула $\mathscr{A}$ или истинна или ложна, т. е. выполнима либо на каждой последовательности, либо ни на одной. Следовательно, всякая замкнутая формула $\mathscr{A}$ выполнима тогда и только тогда, когда она истинна в какой-нибудь интерпретации.

Будем называть формулу $\mathscr{A}$ *противоречием* (в исчислении предикатов), если формула $\neg\mathscr{A}$ является логически общезначимой или, что то же самое, если формула $\mathscr{A}$ ложна во всякой интерпретации.

Говорят, что *формула $\mathscr{A}$ логически влечет формулу $\mathscr{B}$* (в исчислении предикатов), если в любой интерпретации формула $\mathscr{B}$ выполнена на всякой последовательности, на которой выполнена формула $\mathscr{A}$. (Более общо́ говорят, что формула $\mathscr{B}$ является *логическим следствием* (в исчислении предикатов) множества Γ формул, если во всякой интерпретации формула $\mathscr{B}$ выполнена на каждой последовательности, на которой выполнены все формулы из Γ.)

Формулы называются *логически эквивалентными* (в исчислении предикатов), если каждая из них логически влечет другую.

Из этих определений непосредственно вытекают следующие утверждения:

(a) Формула $\mathscr{A}$ логически влечет формулу $\mathscr{B}$ тогда и только тогда, когда формула $\mathscr{A} \supset \mathscr{B}$ логически общезначима.

(b) Формулы $\mathscr{A}$ и $\mathscr{B}$ логически эквивалентны тогда и только тогда, когда формула $\mathscr{A} \equiv \mathscr{B}$ логически общезначима.

(c) Если формула $\mathscr{A}$ логически влечет формулу $\mathscr{B}$ и $\mathscr{A}$ истинно в данной интерпретации, то в этой же интерпретации истинно и $\mathscr{B}$.

(d) Если формула $\mathscr{B}$ является логическим следствием некоторого множества Γ формул, истинных в данной интерпретации, то в этой интерпретации истинна и формула $\mathscr{B}$.

Всякое предложение какого-нибудь формального или естественного языка называется *логически истинным* (в исчислении предикатов), если оно является частным случаем некоторой логически общезначимой формулы, и называется *логически ложным* (в исчислении предикатов), если оно есть частный случай некоторого противоречия (в исчислении предикатов) *).

Примеры. 1. Всякий частный случай тавтологии логически общезначим (VII).

2. Если $\mathscr{A}$ не содержит x свободно, то $\forall x(\mathscr{A} \supset \mathscr{B}) \supset (\mathscr{A} \supset \supset \forall x\mathscr{B})$ логически общезначимо (XI).

3. Если t свободен для x в $\mathscr{A}$, то $\forall x\mathscr{A}(x) \supset \mathscr{A}(t)$ логически общезначимо (X).

4. Формула $\forall x_2\exists x_1 A_1^2(x_1, x_2) \supset \exists x_1\forall x_2 A_1^2(x_1, x_2)$ не является логически общезначимой. В качестве контрпримера рассмотрим область D, состоящую из всех целых чисел, и интерпретацию $A_1^2(y, z)$ посредством $y < z$. Тогда $\forall x_2\exists x_1 A_1^2(x_1, x_2)$ истинно, а $\exists x_1\forall x_2 A_1^2(x_1, x_2)$ ложно.

Упражнения

1. Показать, что следующие формулы не являются логически общезначимыми:

(a) $[\forall x_1 A_1^1(x_1) \supset \forall x_1 A_2^1(x_1)] \supset [(\forall x_1 (A_1^1(x_1) \supset A_2^1(x_1))]$;
(b) $[\forall x_1 (A_1^1(x_1) \vee A_2^1(x_1))] \supset [(\forall x_1 A_1^1(x_1)) \vee (\forall x_1 A_2^1(x_1))]$.

2. Показать, что следующие формулы логически общезначимы:

(a) $\mathscr{A}(t) \supset \exists x_i\mathscr{A}(x_i)$, если t свободен для x_i в $\mathscr{A}$;
(b) $\forall x_i\mathscr{A} \supset \exists x_i\mathscr{A}$;
(c) $\forall x_i\forall x_j\mathscr{A} \equiv \forall x_j\forall x_i\mathscr{A}$;
(d) $\forall x_i\mathscr{A} \equiv \neg\exists x_i\neg\mathscr{A}$;
(e) $\forall x_i(\mathscr{A} \supset \mathscr{B}) \supset (\forall x_i\mathscr{A} \supset \forall x_i\mathscr{B})$;
(f) $(\forall x_i\mathscr{A} \,\&\, \forall x_i\mathscr{B}) \equiv \forall x_i(\mathscr{A} \,\&\, \mathscr{B})$;
(g) $(\forall x_i\mathscr{A} \vee \forall x_i\mathscr{B}) \supset \forall x_i(\mathscr{A} \vee \mathscr{B})$;
(h) $\exists x_i\exists x_j\mathscr{A} \equiv \exists x_j\exists x_i\mathscr{A}$;
(i) $\exists x_i\forall x_j\mathscr{A} \supset \forall x_j\exists x_i\mathscr{A}$.

*) В дальнейшем слова «в исчислении предикатов» мы будем опускать.

3. Доказать, что замкнутая формула $\mathscr{A}$ логически влечет формулу $\mathscr{B}$ тогда и только тогда, когда $\mathscr{B}$ истинна во всякой интерпретации, в которой истинна $\mathscr{A}$. (Это, вообще говоря, неверно, если $\mathscr{A}$ содержит свободные переменные. Например, пусть $\mathscr{A}$ есть $A_1^1(x_1)$ и $\mathscr{B}$ есть $\forall x_1 A_1^1(x_1)$. Тогда, в силу (VI), $\mathscr{B}$ истинна, если истинна $\mathscr{A}$. Предлагается построить интерпретацию, показывающую, что $\mathscr{A}$ не влечет логически $\mathscr{B}$.)

4. Показать, что формулы

(a) $\exists x \forall y (A_1^2(x, y) \& \neg A_1^2(y, x) \supset [A_1^2(x, x) \equiv A_1^2(y, y)])$;

(b) $\forall x \forall y \forall z (A_1^2(x, y) \& A_1^2(y, z) \supset A_1^2(x, z)) \&$
$\& \forall x \neg A_1^2(x, x) \supset \exists x \forall y \neg A_1^2(x, y)$;

(c) $\forall x \forall y \forall z (A_1^2(x, x) \& (A_1^2(x, z) \supset A_1^2(x, y) \vee A_1^2(y, z))) \supset \exists y \forall z A_1^2(y, z)$

не являются логически общезначимыми.

5. Доказать, что всякая формула $\mathscr{A}$ со свободными переменными $y_1, \ldots, y_n$ выполнима тогда и только тогда, когда выполнима формула $\exists y_1 \ldots \exists y_n \mathscr{A}$.

6. Введя подходящие обозначения, записать предложения, участвующие в нижеследующих выводах, в виде формул и выяснить, в каких случаях конъюнкция посылок логически влечет заключение.

(a) Всякий, кто находится в здравом уме, может понимать математику. Ни один из сыновей Гегеля не может понимать математику. Сумасшедшие не допускаются к голосованию. Следовательно, никто из сыновей Гегеля не допускается к голосованию.

(b) Для любого множества x существует множество y такое, что мощность y больше мощности x. Если x включено в y, то мощность x не больше мощности y. Всякое множество включено в V. Следовательно, V не множество.

(c) Если всякий предок предка данного индивидуума есть также предок того же индивидуума и никакой индивидуум не есть предок самого себя, то должен существовать некто, не имеющий предков.

(d) Всякий парикмахер в Джонсвилле бреет всех тех и только тех, кто не бреется сам. Следовательно, в Джонсвилле нет ни одного парикмахера.

7. Привести пример логически общезначимой формулы, которая не является частным случаем тавтологии. Показать, однако, что всякая логически общезначимая открытая формула (т. е. формула без кванторов) является частным случаем некоторой тавтологии.

§ 3. Теории первого порядка

В случае пропозиционального исчисления метод истинностных таблиц дает нам эффективный способ проверки, является ли данная пропозициональная форма тавтологией. Однако представляется сомнительным существование эффективного процесса, позволяющего для любой данной формулы решать вопрос о том, является ли она логически общезначимой, поскольку теперь уже для каждой формулы приходится иметь дело с проверкой ее истинности в интерпретациях с областями, вообще говоря, сколь угодно большими конечными, а также и бесконечными. И в самом деле, в дальнейшем мы увидим, что, в соответствии с некоторым совершенно естественным определением понятия «эффективности», действительно может быть доказана невозможность эффективного способа распознавать логическую общезначимость. Аксиоматический метод, который был, пожалуй, излишней роскошью при изучении пропозиционального исчисления, предстаёляется, таким образом, необходимым при изучении

формул, содержащих кванторы *), и поэтому мы теперь обращаемся к рассмотрению *теорий первого порядка* **) (или, иначе, *элементарных теорий*).

Символами всякой теории K первого порядка служат по существу те же символы, которые мы ввели ранее в этой главе: пропозициональные связки $\neg$, $\supset$; знаки пунктуации (,), , (строго говоря, запятая не является необходимой, но удобна для облегчения чтения формул); счетное множество предметных переменных $x_1, x_2, \ldots$; непустое, конечное или счетное, множество предикатных букв A_j^n $(n, j \geqslant 1)$; конечное (возможно, и пустое) или счетное множество функциональных букв f_j^n $(n, j \geqslant 1)$; и, наконец, конечное (тоже, возможно, пустое) или счетное множество предметных констант a_i $(i \geqslant 1)$. Таким образом, в теории K могут отсутствовать некоторые или даже все функциональные буквы и предметные константы, а также некоторые — но не все! — предикатные буквы. Различные теории могут отличаться друг от друга по составу символов.

Сформулированные в § 1 определения терма, формулы и пропозициональных связок &, $\vee$, $\equiv$ остаются в силе для любой теории первого порядка. Разумеется, в случае каждой конкретной теории K в построении термов и формул участвуют только те символы, которые принадлежат теории K.

Аксиомы теории K разбиваются на два класса: логические аксиомы и собственные (или нелогические) аксиомы.

Логические аксиомы: каковы бы ни были формулы $\mathscr{A}$, $\mathscr{B}$ и $\mathscr{C}$ теории K, следующие формулы являются логическими аксиомами теории K

(1) $\mathscr{A} \supset (\mathscr{B} \supset \mathscr{A})$;

(2) $(\mathscr{A} \supset (\mathscr{B} \supset \mathscr{C})) \supset ((\mathscr{A} \supset \mathscr{B}) \supset (\mathscr{A} \supset \mathscr{C}))$;

*) Имеются еще и другие доводы в пользу аксиоматического подхода. Концепции и построения, включающие в себя понятие интерпретации и связанные с ним понятия истины, модели и т. п., часто называются *семантическими* в отличие от так называемых *синтаксических* концепций, восходящих к простым отношениям между символами и выражениями точных формальных языков. Поскольку семантические понятия носят теоретико-множественный характер, а теория множеств, по причине парадоксов, представляется в известной степени шаткой основой для исследований в области математической логики, то многие логики считают более надежным синтаксический подход, состоящий в изучении формальных аксиоматических теорий с применением лишь довольно слабых арифметических методов. Подробнее об этом см. в первоначальных исследованиях в области семантики Тарского [1936], Клини [1952], Чёрча [1956] и Гильберта и Бернайса [1934].

**) Слова «первого порядка» указывают на отличие теорий, которые мы будем изучать, от таких теорий, в которых либо допускаются предикаты, имеющие в качестве возможных значений своих аргументов другие предикаты и функции, либо допускаются кванторы по предикатам или кванторы по функциям. Теорий первого порядка хватает для выражения известных математических теорий, и, во всяком случае, большинство теорий высших порядков может быть подходящим образом «переведено» на язык первого порядка. Примеры теорий высших порядков можно найти у Чёрча [1940], Гёделя [1931], Тарского [1933], Хазенъегера и Шольца [1961; §§ 200—219].

(3) $(\neg \mathscr{B} \supset \neg \mathscr{A}) \supset ((\neg \mathscr{B} \supset \mathscr{A}) \supset \mathscr{B})$;

(4) $\forall x_i \mathscr{A}(x_i) \supset \mathscr{A}(t)$, где $\mathscr{A}(x_i)$ есть формула теории K и t есть терм теории K, свободный для x_i в $\mathscr{A}(x_i)$. Заметим, что t может совпадать с x_i, и тогда мы получаем аксиому $\forall x_i \mathscr{A}(x_i) \supset \mathscr{A}(x_i)$.

(5) $\forall x_i(\mathscr{A} \supset \mathscr{B}) \supset (\mathscr{A} \supset \forall x_i \mathscr{B})$, если формула $\mathscr{A}$ не содержит свободных вхождений x_i.

Собственные аксиомы: таковые не могут быть сформулированы в общем случае, ибо меняются от теории к теории. Теория первого порядка, не содержащая собственных аксиом, называется *исчислением предикатов первого порядка.*

Правилами вывода во всякой теории первого порядка являются

(i) Modus ponens: *из* $\mathscr{A}$ *и* $\mathscr{A} \supset \mathscr{B}$ *следует* $\mathscr{B}$.

(ii) Правило *обобщения* (или связывания квантором всеобщности): *из* $\mathscr{A}$ *следует* $\forall x_i \mathscr{A}$.

(В дальнейшем применение этих правил будет сокращенно отмечаться соответственно посредством MP и Gen (от английского слова «Generalization»).)

Моделью теории первого порядка K называется всякая интерпретация, в которой истинны все аксиомы теории K. В силу (III) и (VI) на стр. 59 — 60, если правила modus ponens и обобщения применяются к истинным в данной интерпретации формулам, то результатом являются формулы, также истинные в той же интерпретации. Следовательно, и всякая теорема теории K истинна во всякой ее модели.

Как мы увидим позже, логические аксиомы выбраны таким образом, что множество логических следствий (в семантическом смысле, см. стр. 62) аксиом теории K в точности совпадает с множеством теорем теории K. В частности, для исчисления предикатов первого порядка оказывается, что множество его теорем совпадает с множеством логически общезначимых формул.

Ограничения, содержащиеся в формулировках схем аксиом (4) и (5), требуют некоторых пояснений. Если бы, в случае схемы (4), терм t мог не быть свободным для x_i в $\mathscr{A}$, то стал бы возможным следующий неприятный результат. Пусть $\mathscr{A}(x_1)$ есть $\neg \forall x_2 A_1^2(x_1, x_2)$ и t есть x_2. Заметим, что тогда терм t не свободен для x_1 в $\mathscr{A}(x_1)$. Рассмотрим такой частный случай схемы аксиом (4):

$$\forall x_1 (\neg \forall x_2 A_1^2(x_1, x_2)) \supset \neg \forall x_2 A_1^2(x_2, x_2), \qquad (*)$$

и возьмем в качестве интерпретации любую область, содержащую не менее двух элементов, а в качестве A_1^2 — отношение тождества. Тогда посылка в (*) истинна, а заключение ложно.

Для схемы (5) отказ от требования, чтобы x_i не входило свободно в $\mathscr{A}$, также приводит к неприятностям. Пусть, например, $\mathscr{A}$ и $\mathscr{B}$ представляют собой $A_1^1(x_1)$. Таким образом, сейчас x_1 свободно входит в $\mathscr{A}$. Рассмотрим частный случай схемы (5):

$$\forall x_1 (A_1^1(x_1) \supset A_1^1(x_1)) \supset (A_1^1(x_1) \supset \forall x_1 A_1^1(x_1)). \qquad (**)$$

Антецедент в (**), очевидно, логически общезначим. Однако если мы возьмем какую-нибудь интерпретацию, в которой A_1^1 выполнено для некоторых, но не для всех элементов области, то обнаружим, что консеквент не является истинным.

Примеры теорий первого порядка.

(i) Теория частичного упорядочения. Пусть K содержит единственную предикатную букву A_1^2 и не содержит функциональных букв и предметных констант. Вместо $A_1^2(x_1, x_2)$ и $\neg A_1^2(x_1, x_2)$ будем соответственно писать $x_1 < x_2$ и $x_1 \not< x_2$. Пусть, наконец, K содержит две собственные аксиомы:

(a) $\forall x_1 (x_1 \not< x_1)$ (иррефлексивность);

(b) $\forall x_1 \forall x_2 \forall x_3 (x_1 < x_2 \,\&\, x_2 < x_3 \supset x_1 < x_3)$ (транзитивность).

Всякая модель этой теории называется частично упорядоченной структурой.

(ii) Теория групп. Пусть K имеет одну предикатную букву A_1^2, одну функциональную букву f_1^2 и одну предметную константу a_1. (В соответствии с обычными обозначениями, мы будем писать: $t = s$ вместо $A_1^2(t, s)$, $t + s$ вместо $f_1^2(t, s)$ и 0 вместо a_1.) Собственными аксиомами теории K являются формулы:

(a) $\forall x_1 \forall x_2 \forall x_3 (x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3)$ (ассоциативность);

(b) $\forall x_1 (0 + x_1 = x_1)$;

(c) $\forall x_1 \exists x_2 (x_2 + x_1 = 0)$ (существование обратного элемента);

(d) $\forall x_1 (x_1 = x_1)$ (рефлексивность равенства);

(e) $\forall x_1 \forall x_2 (x_1 = x_2 \supset x_2 = x_1)$ (симметричность равенства);

(f) $\forall x_1 \forall x_2 \forall x_3 (x_1 = x_2 \supset (x_2 = x_3 \supset x_1 = x_3))$ (транзитивность равенства);

(g) $\forall x_1 \forall x_2 \forall x_3 (x_2 = x_3 \supset (x_1 + x_2 = x_1 + x_3 \,\&\, x_2 + x_1 = x_3 + x_1))$ (подстановочность равенства).

Всякая модель этой теории называется группой.

Если в группе истинна формула $\forall x_1 \forall x_2 (x_1 + x_2 = x_2 + x_1)$, то группа называется абелевой, или коммутативной.

Теория частичного упорядочения и теория групп обе являются эффективно аксиоматизированными. Вообще всякая теория с конечным числом собственных аксиом является эффективно аксиоматизированной, ибо, как нетрудно видеть, имеется возможность для любой данной формулы эффективно решать вопрос, принадлежит ли она к числу логических аксиом (см. стр. 65—66).

§ 4. Свойства теорий первого порядка

Все результаты этого параграфа относятся (если нет специальной оговорки) к произвольной теории первого порядка K. Заметим, что всякая теория первого порядка является формальной теорией (см. стр. 36).

Предложение 2.1. *Если формула* $\mathscr{A}$ *теории* K *есть частный случай тавтологии, то* $\mathscr{A}$ *есть теорема в* K *и может быть выведена с употреблением одних только схем аксиом* (1) — (3) *и правила* modus ponens.

Доказательство. Пусть $\mathscr{A}$ получена из некоторой тавтологии W с помощью подстановок. Согласно предложению 1.13, существует вывод W в L. Сделаем теперь всюду в этом выводе подстановки по следующему правилу: (i) если какая-нибудь пропозициональная буква входит в W, то на места всех ее вхождений в каждую формулу вывода подставляем ту формулу теории K, которая подставлялась в W на места вхождений той же буквы при построении $\mathscr{A}$, (ii) если данная пропозициональная буква не входит в W, то на места всех ее вхождений в формулы вывода подставляем произвольную (одну и ту же для данной буквы) формулу теории K. Полученная таким образом последовательность формул и будет выводом формулы $\mathscr{A}$ в K, причем выводом, использующим только схемы аксиом (1) — (3) и MP.

Предложение 2.2. *Всякое исчисление предикатов первого порядка* K *непротиворечиво.*

Доказательство. Для произвольной формулы $\mathscr{A}$ обозначим через $\mathrm{h}(\mathscr{A})$ выражение, получающееся в результате следующего преобразования формулы $\mathscr{A}$: в $\mathscr{A}$ опускаются все кванторы и термы (вместе с соответствующими скобками и запятыми). Например, $\mathrm{h}(\forall x_1 A_1^2(x_1, x_2) \supset A_1^1(x_3))$ есть $A_1^2 \supset A_1^1$, $\mathrm{h}(\neg \forall x_7 A_2^3(x_4, a_1, x_7) \supset A_3^1(x_4))$ есть $\neg A_2^3 \supset A_3^1$. По существу $\mathrm{h}(\mathscr{A})$ всегда является пропозициональной формой, в которой роль пропозициональных букв играют символы A_j^k. Очевидно, $\mathrm{h}(\neg \mathscr{A}) = \neg \mathrm{h}(\mathscr{A})$ и $\mathrm{h}(\mathscr{A} \supset \mathscr{B}) = \mathrm{h}(\mathscr{A}) \supset \mathrm{h}(\mathscr{B})$. Для всякой аксиомы $\mathscr{A}$, получаемой по какой-нибудь из схем аксиом (1) — (5), $\mathrm{h}(\mathscr{A})$ является тавтологией. Это очевидно для (1) — (3). Всякий частный случай $\forall x_i \mathscr{A}(x_i) \supset \mathscr{A}(t)$ схемы (4) преобразуется операцией h в тавтологию вида $\mathscr{B} \supset \mathscr{B}$, а всякий частный случай $\forall x_i(\mathscr{A} \supset \mathscr{B}) \supset (\mathscr{A} \supset \forall x_i \mathscr{B})$ схемы (5) преобразуется в тавтологию вида $(\mathscr{D} \supset \mathscr{E}) \supset (\mathscr{D} \supset \mathscr{E})$. Наконец, если $\mathrm{h}(\mathscr{A})$ и $\mathrm{h}(\mathscr{A} \supset \mathscr{B})$ — тавтологии, то, в силу предложения 1.1, и $\mathrm{h}(\mathscr{B})$ — тавтология; и если $\mathrm{h}(\mathscr{A})$ тавтология, то и $\mathrm{h}(\forall x_i \mathscr{A})$ — тавтология, ибо результаты применения операции h к $\mathscr{A}$ и $\forall x_i \mathscr{A}$ совпадают. Следовательно, если $\mathscr{A}$ есть теорема в K, то $\mathrm{h}(\mathscr{A})$ есть тавтология. Если бы существовала формула $\mathscr{B}$ в K такая, что $\vdash_K \mathscr{B}$ и $\vdash_K \neg \mathscr{B}$, то оба выражения $\mathrm{h}(\mathscr{B})$ и $\mathrm{h}(\neg \mathscr{B})$ были бы тавтологиями, что невозможно. Таким образом, K непротиворечиво. (Операция h равносильна интерпретации K в области, состоящей из одного элемента. Все теоремы K истинны в такой интерпретации, однако ни в какой интерпретации никакая формула не может быть истинной вместе со своим отрицанием.)

Теорема дедукции для пропозиционального исчисления (предложение 1.8) без соответствующей модификации не может быть проведена для произвольных теорий первого порядка K. Например, $\mathscr{A} \vdash_K \forall x_1 \mathscr{A}$

для любой формулы $\mathscr{A}$, однако отнюдь не всегда $\vdash_K \mathscr{A} \supset \forall x_1 \mathscr{A}$. В самом деле, рассмотрим область, содержащую по меньшей мере два элемента c и d. Пусть K есть некоторое исчисление предикатов, и пусть $\mathscr{A}$ есть $A_1^1(x_1)$. Проинтерпретируем A_1^1 каким-нибудь свойством, которым обладает только элемент c. Тогда $A_1^1(x_1)$ выполнено на всякой последовательности $s = (b_1, b_2, \ldots)$, где $b_1 = c$, однако $\forall x_1 A(x_1)$ не выполнено вообще ни на какой последовательности. Следовательно, формула $A_1^1(x_1) \supset \forall x_1 A_1^1(x_1)$ не истинна в этой интерпретации и потому не является логически общезначимой. Легко, однако, видеть (предложение 2.7), что всякая теорема всякого исчисления предикатов является логически общезначимой.

Однако некоторая ослабленная, но все же полезная форма теоремы дедукции и здесь может быть доказана.

Пусть $\mathscr{A}$ — какая-нибудь формула, принадлежащая заданному множеству Γ формул, и пусть $\mathscr{B}_1, \ldots, \mathscr{B}_n$ — какой-нибудь вывод из Γ, снабженный обоснованием каждого в нем шага. Мы будем говорить, что $\mathscr{B}_i$ *зависит от* $\mathscr{A}$ в этом выводе, если

(i) $\mathscr{B}_i$ есть $\mathscr{A}$ и обоснованием $\mathscr{B}_i$ служит принадлежность $\mathscr{B}_i$ к Γ, или

(ii) $\mathscr{B}_i$ обосновано как непосредственное следствие по MP или Gen некоторых предшествующих в этом выводе формул, из которых по крайней мере одна зависит от $\mathscr{A}$.

Пример. $\mathscr{A}, \forall x_1 \mathscr{A} \supset \mathscr{C} \vdash \forall x_1 \mathscr{C}$.

$(\mathscr{B}_1)$	$\mathscr{A}$	гипотеза
$(\mathscr{B}_2)$	$\forall x_1 \mathscr{A}$	$(\mathscr{B}_1)$, Gen
$(\mathscr{B}_3)$	$\forall x_1 \mathscr{A} \supset \mathscr{C}$	гипотеза
$(\mathscr{B}_4)$	$\mathscr{C}$	$(\mathscr{B}_2)$, $(\mathscr{B}_3)$, MP
$(\mathscr{B}_5)$	$\forall x_1 \mathscr{C}$	$(\mathscr{B}_4)$, Gen

Здесь $(\mathscr{B}_1)$ зависит от $\mathscr{A}$, $(\mathscr{B}_2)$ зависит от $\mathscr{A}$, $(\mathscr{B}_3)$ зависит от $\forall x_1 \mathscr{A} \supset \mathscr{C}$, $(\mathscr{B}_4)$ зависит от $\mathscr{A}$ и от $\forall x_1 \mathscr{A} \supset \mathscr{C}$ и $(\mathscr{B}_5)$ зависит от $\mathscr{A}$ и от $\forall x_1 \mathscr{A} \supset \mathscr{C}$.

Предложение 2.3. *Если* $\mathscr{B}$ *не зависит от* $\mathscr{A}$ *в выводе* Γ, $\mathscr{A} \vdash \mathscr{B}$, *то* $\Gamma \vdash \mathscr{B}$.

Доказательство. Пусть $\mathscr{B}_1, \ldots, \mathscr{B}_n = \mathscr{B}$ — вывод $\mathscr{B}$ из Γ и $\mathscr{A}$, в котором $\mathscr{B}$ не зависит от $\mathscr{A}$. В качестве индуктивного предположения допустим, что доказываемое предложение справедливо для всех выводов, длина которых меньше n. Если $\mathscr{B}$ принадлежит Γ или есть аксиома, то $\Gamma \vdash \mathscr{B}$. Если $\mathscr{B}$ является непосредственным следствием каких-то (одной или двух) предшествующих формул, то, поскольку $\mathscr{B}$ не зависит от $\mathscr{A}$, не зависит от $\mathscr{A}$ и ни одна из этих формул. Следовательно, по индуктивному предположению, из Γ выводимы эти (одна или две) формулы, а вместе с ними и $\mathscr{B}$.

Предложение 2.4. (Теорема дедукции.) *Пусть* $\Gamma, \mathscr{A} \vdash \mathscr{B}$, *и при этом пусть существует такой вывод* $\mathscr{B}$ *из* $\{\Gamma, \mathscr{A}\}$, *в котором ни при каком применении правила обобщения к формулам, зависящим в этом выводе от* $\mathscr{A}$, *не связывается квантором никакая свободная переменная формулы* $\mathscr{A}$. *Тогда* $\Gamma \vdash \mathscr{A} \supset \mathscr{B}$.

Доказательство. Пусть $\mathscr{B}_1, \ldots, \mathscr{B}_n = \mathscr{B}$ — удовлетворяющий условию теоремы вывод $\mathscr{B}$ из $\{\Gamma, \mathscr{A}\}$. Докажем по индукции, что $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_i$ для любого i, $i \leqslant n$. Если $\mathscr{B}_i$ есть аксиома или принадлежит Γ, то $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_i$, поскольку $\mathscr{B}_i \supset (\mathscr{A} \supset \mathscr{B}_i)$ — аксиома. Если $\mathscr{B}_i$ совпадает с $\mathscr{A}$, то $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_i$ в силу $\vdash \mathscr{A} \supset \mathscr{A}$ (предложение 2.1). Если существуют j и k, меньшие i, такие, что $\mathscr{B}_k$ есть $\mathscr{B}_j \supset \mathscr{B}_i$, то, согласно индуктивному предположению, $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_j$ и $\Gamma \vdash \mathscr{A} \supset (\mathscr{B}_j \supset \mathscr{B}_i)$. Следовательно, по схеме аксиом (2) и MP, $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_i$. Предположим, наконец, что существует j, $j < i$, такое, что $\mathscr{B}_i$ есть $\forall x_k \mathscr{B}_j$. По предположению, $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_j$, и либо $\mathscr{B}_j$ не зависит от $\mathscr{A}$, либо x_k не является свободной переменной формулы $\mathscr{A}$. Если $\mathscr{B}_j$ не зависит от $\mathscr{A}$, то, в силу предложения 2.3, $\Gamma \vdash \mathscr{B}_j$, и тогда, применяя Gen, получаем $\Gamma \vdash \forall x_k \mathscr{B}_j$, т. е. $\Gamma \vdash \mathscr{B}_i$. По схеме аксиом (1), $\vdash \mathscr{B}_i \supset (\mathscr{A} \supset \mathscr{B}_i)$. Отсюда, по правилу MP, получаем: $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_i$. Если x_k не является свободной переменной формулы $\mathscr{A}$, то, по схеме аксиом (5), $\vdash \forall x_k (\mathscr{A} \supset \mathscr{B}_j) \supset (\mathscr{A} \supset \forall x_k \mathscr{B}_j)$. Так как $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_j$, то, по правилу Gen, получаем $\Gamma \vdash \forall x_k (\mathscr{A} \supset \mathscr{B}_j)$ и, наконец, с помощью MP: $\Gamma \vdash \mathscr{A} \supset \forall x_k \mathscr{B}_j$, т. е. $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_i$. Этим и завершается индукция. Доказываемое предложение мы получаем при $i = n$.

Условия предложения 2.4 слишком громоздки, и часто полезнее оказываются его более слабые следствия:

Следствие 2.5. *Если* $\Gamma, \mathscr{A} \vdash \mathscr{B}$ *и существует вывод, построенный без применения правила обобщения к свободным переменным формулы* $\mathscr{A}$, *то* $\Gamma \vdash \mathscr{A} \supset \mathscr{B}$.

Следствие 2.6. *Если формула* $\mathscr{A}$ *замкнута и* $\Gamma, \mathscr{A} \vdash \mathscr{B}$, *то* $\Gamma \vdash \mathscr{A} \supset \mathscr{B}$.

Следующее дополнительное заключение можно извлечь из доказательств предложений 2.3 — 2.6. При построении нового вывода, т. е. вывода $\Gamma \vdash \mathscr{A} \supset \mathscr{B}$ ($\Gamma \vdash \mathscr{B}$, в случае предложения 2.3), применение Gen к какой-нибудь формуле, зависящей от некоторой формулы $\mathscr{C}$ из Γ, требуется только в том случае, когда и в данном выводе, т. е. в выводе $\mathscr{B}$ из $\{\Gamma, \mathscr{A}\}$, имеется применение Gen (с той же связываемой переменной) к некоторой формуле, зависящей от $\mathscr{C}$. (Нетрудно видеть, что $\mathscr{B}_j$ из доказательства предложения 2.4 зависит от той или иной посылки $\mathscr{C}$ из Γ в первоначальном выводе тогда и только тогда, когда $\mathscr{A} \supset \mathscr{B}_j$ зависит от $\mathscr{C}$ в новом выводе.)

Это дополнительное замечание бывает полезно, когда мы хотим применить теорему дедукции несколько раз подряд в процессе доказательства какого-либо утверждения о выводимости, например, чтобы получить $\Gamma \vdash \mathscr{D} \supset (\mathscr{A} \supset \mathscr{B})$ из $\Gamma, \mathscr{D}, \mathscr{A} \vdash \mathscr{B}$. Поэтому в дальнейшем

мы будем рассматривать это замечание как часть заключения предложений 2.3 — 2.6.

Пример. $\vdash \forall x_1 \forall x_2 \mathscr{A} \supset \forall x_2 \forall x_1 \mathscr{A}$.

Доказательство.

1. $\forall x_1 \forall x_2 \mathscr{A}$	гипотеза
2. $\forall x_1 \forall x_2 \mathscr{A} \supset \forall x_2 \mathscr{A}$	схема аксиом (4)
3. $\forall x_2 \mathscr{A}$	1, 2, MP
4. $\forall x_2 \mathscr{A} \supset \mathscr{A}$	схема аксиом (4)
5. $\mathscr{A}$	3, 4, MP
6. $\forall x_1 \mathscr{A}$	5, Gen
7. $\forall x_2 \forall x_1 \mathscr{A}$	6, Gen

Таким образом, в силу 1 — 7, мы имеем $\forall x_1 \forall x_2 \mathscr{A} \vdash \forall x_2 \forall x_1 \mathscr{A}$, причем в построенном выводе ни при одном применении Gen не связывается свободная переменная формулы $\forall x_1 \forall x_2 \mathscr{A}$. Поэтому, на основании следствия 2.5, $\vdash \forall x_1 \forall x_2 \mathscr{A} \supset \forall x_2 \forall x_1 \mathscr{A}$.

Упражнения

1. Показать, что

(a) $\vdash \forall x_1 (\mathscr{A} \supset \mathscr{B}) \supset (\forall x_1 \mathscr{A} \supset \forall x_1 \mathscr{B})$;
(b) $\vdash \forall x (\mathscr{A} \supset \mathscr{B}) \supset (\exists x \mathscr{A} \supset \exists x \mathscr{B})$;
(c) $\vdash \forall x (\mathscr{A} \,\&\, \mathscr{B}) \equiv \forall x \mathscr{A} \,\&\, \forall x \mathscr{B}$;
(d) $\vdash \forall y_1 \ldots \forall y_n \mathscr{A} \supset \mathscr{A}$.

2. Пусть K — теория первого порядка, и пусть K# — теория со следующими аксиомами:
(1) $\forall y_1 \ldots \forall y_n \mathscr{A}$, где $\mathscr{A}$ — произвольная аксиома теории K, а $y_1, \ldots, y_n$ $(n \geqslant 0)$ — произвольные предметные переменные;
(2) $\forall y_1 \ldots \forall y_n (\mathscr{A} \supset \mathscr{B}) \supset [\forall y_1 \ldots \forall y_n \mathscr{A} \supset \forall y_1 \ldots \forall y_n \mathscr{B}]$,
где $\mathscr{A}$ и $\mathscr{B}$ — произвольные формулы, а $y_1, \ldots, y_n$ — произвольные предметные переменные. Единственным правилом вывода в K# служит modus ponens. Доказать, что множества всех теорем теорий K и K# совпадают.

§ 5. Теоремы о полноте

Предложение 2.7. *Во всяком исчислении предикатов первого порядка всякая теорема является логически общезначимой.*

Доказательство. В силу свойства (VII) понятия истинной формулы (см. стр. 60), аксиомы, задаваемые схемами (1) — (3), логически общезначимы. В силу свойств (X) (следствие) и (XI), логически верны аксиомы, порождаемые схемами (4) — (5). В силу (III) и (VI), правила вывода MP и Gen сохраняют свойство логической общезначимости. Таким образом, всякая теорема любого исчисления предикатов логически общезначима.

Упражнения

1. Для любой теории первого порядка K, если $\Gamma \vdash_K \mathscr{A}$ и каждая формула из Γ истинна в данной модели M, то и формула $\mathscr{A}$ истинна в модели M.

2. Если формула $\mathscr{A}$ не содержит кванторов и доказуема в исчислении предикатов, то она является частным случаем тавтологии, и потому, согласно предложению 2.1, для этой формулы существует бескванторный вывод (т. е. вывод, члены которого суть формулы, не содержащие кванторов), использующий только схемы аксиом (1) — (3) и MP. (Указание. Если бы формула $\mathscr{A}$ не была тавтологией, то можно было бы построить интерпретацию с областью, состоящей из термов, входящих в $\mathscr{A}$, в которой, в противоречие с предложением 2.7, формула $\mathscr{A}$ была бы ложна.) Заметим, что этот результат влечет непротиворечивость исчисления предикатов, а также приводит к разрешающей процедуре для проблемы выводимости бескванторных формул.

Предложение 2.7 представляет собой половину той теоремы о полноте, которую мы теперь хотим доказать. Другая ее половина будет следовать из гораздо более общих предложений, устанавливаемых ниже. Предварительно мы докажем несколько лемм.

Пусть переменные x_i и x_j не совпадают и формула $\mathscr{A}(x_j)$ получается из формулы $\mathscr{A}(x_i)$ подстановкой x_j вместо всех свободных вхождений x_i, тогда $\mathscr{A}(x_i)$ и $\mathscr{A}(x_j)$ называются *подобными*, если x_j свободна для x_i в $\mathscr{A}(x_i)$ и $\mathscr{A}(x_i)$ не имеет свободных вхождений x_j. Если $\mathscr{A}(x_i)$ и $\mathscr{A}(x_j)$ подобны, то x_i свободно для x_j в $\mathscr{A}(x_j)$ и $\mathscr{A}(x_j)$ не имеет свободных вхождений x_i. Таким образом, подобие оказывается симметричным отношением. Иначе говоря, $\mathscr{A}(x_i)$ и $\mathscr{A}(x_j)$ подобны тогда и только тогда, когда $\mathscr{A}(x_j)$ имеет свободные вхождения x_j в точности в тех местах, в которых $\mathscr{A}(x_i)$ имеет свободные вхождения x_i.

Лемма 2.8. *Если формулы* $\mathscr{A}(x_i)$ *и* $\mathscr{A}(x_j)$ *подобны, то* $\vdash \forall x_i \mathscr{A}(x_i) \equiv \forall x_j \mathscr{A}(x_j)$.

Доказательство. По схеме аксиом (4), $\vdash \forall x_i \mathscr{A}(x_i) \supset \mathscr{A}(x_j)$. Применим правило Gen: $\vdash \forall x_j (\forall x_i \mathscr{A}(x_i) \supset \mathscr{A}(x_j))$ и, по схеме аксиом (5), получим $\vdash \forall x_i \mathscr{A}(x_i) \supset \forall x_j \mathscr{A}(x_j)$. Точно так же докажем, что $\vdash \forall x_j \mathscr{A}(x_j) \supset \forall x_i \mathscr{A}(x_i)$. Применяя тавтологию $A_1 \supset (A_2 \supset (A_1 \& A_2))$ и предложение 2.1, получаем наконец $\vdash \forall x_i \mathscr{A}(x_i) \equiv \equiv \forall x_j \mathscr{A}(x_j)$.

Упражнение

Если $\mathscr{A}(x_i)$ и $\mathscr{A}(x_j)$ подобны, то $\vdash \exists x_i \mathscr{A}(x_i) \equiv \exists x_j \mathscr{A}(x_j)$.

Лемма 2.9. *Если замкнутая формула* $\neg \mathscr{A}$ *теории* K *невыводима в* K, *то теория* K′, *полученная из* K *добавлением* $\mathscr{A}$ *в качестве аксиомы, непротиворечива.*

Доказательство. Допустим, что теория K′ противоречива. Это значит, что имеется формула $\mathscr{B}$, для которой $\vdash_{K'} \mathscr{B}$ и $\vdash_{K'} \neg \mathscr{B}$. В силу предложения 2.1, имеем: $\vdash_{K'} \mathscr{B} \supset (\neg \mathscr{B} \supset \neg \mathscr{A})$. Следовательно, $\vdash_{K'} \neg \mathscr{A}$ и $\mathscr{A} \vdash_K \neg \mathscr{A}$. Поскольку формула $\mathscr{A}$ замкнута, го, в силу

следствия 2.6 теоремы дедукции, имеем $\vdash_K \mathscr{A} \supset \neg\mathscr{A}$. С другой стороны, в силу предложения 2.1, $\vdash_K (\mathscr{A} \supset \neg\mathscr{A}) \supset \neg\mathscr{A}$. Поэтому $\vdash_K \neg\mathscr{A}$, что противоречит условию. (Подобным же образом, если формула $\mathscr{A}$ невыводима в K, то добавление к K формулы $\neg\mathscr{A}$ в качестве новой аксиомы к противоречию не приводит.)

Лемма 2.10. *Множество всех выражений всякой теории первого порядка счетно (следовательно, счетны в частности: множество всех термов, множество всех формул, множество всех замкнутых формул).*

Доказательство. Отнесем каждому символу u нечетное число $g(u)$ по следующему правилу: $g(\,(\,) = 3$, $g(\,)\,) = 5$, $g(,) = 7$, $g(\neg) = 9$, $g(\supset) = 11$, $g(x_k) = 5 + 8k$, $g(a_k) = 7 + 8k$, $g\left(f_k^n\right) = 9 + 8 \cdot (2^n \cdot 3^k)$, $g\left(A_k^n\right) = 11 + 8 \cdot (2^n \cdot 3^k)$; при этом полагаем $g(\forall x_i) = g((x_i))$. Теперь выражению $u_0 u_1 \ldots u_r$ отнесем число $2^{g(u_0)} 3^{g(u_1)} \ldots p_r^{g(u_r)}$, где p_i — i-е простое число. При такой нумерации, очевидно, разные выражения получают разные номера, и мы можем пересчитать все выражения в порядке возрастания отнесенных им чисел.

Более того, если мы умеем эффективно распознавать символы теории K, то тогда не только может быть осуществлена эффективная нумерация выражений этой теории, но оказывается возможным и по любому числу узнавать, является оно в этой нумерации номером какого-нибудь выражения теории K или нет. Сказанное верно, в частности, и для термов, формул, замкнутых формул и т. д. Если теория K является к тому же эффективно аксиоматизированной, т. е. если имеется эффективная процедура, позволяющая для любой данной формулы решать вопрос о том, является ли она аксиомой, то мы можем следующим образом перенумеровать все теоремы теории K: имея соответствующую произведенной нумерации выражений в K нумерацию всех аксиом, начнем с первой в этой нумерации аксиомы, добавив к ней все ее непосредственные следствия по правилу MP и по правилу Gen, примененного только к переменной x_1; затем добавим к полученному списку вторую аксиому (если ее еще там нет) и все непосредственные следствия формул этого расширенного за счет второй аксиомы списка, на этот раз с применением правила Gen уже по двум переменным x_1 и x_2. Если, поступая подобным же образом далее, мы на k-м шаге добавим к уже полученному списку формул k-ю аксиому и ограничим действие Gen переменными $x_1, \ldots, x_k$, то при этом мы получим в конечном счете все теоремы теории K. Однако в отличие от случая выражений, формул, термов и т. д. оказывается, что существуют такие теории K, для которых мы не можем по любой наперед заданной формуле заранее сказать, встретится ли в конце концов эта формула в списке теорем.

Назовем теорию K первого порядка *полной*, если для любой замкнутой формулы $\mathscr{A}$ теории K либо $\vdash_K \mathscr{A}$, либо $\vdash_K \neg\mathscr{A}$.

Теория K′ первого порядка, имеющая те же символы, что и теория K первого порядка, называется *расширением* теории K, если всякая теорема теории K является также теоремой теории K′. (Очевидно, чтобы доказать, что теория K′ является расширением теории K, достаточно доказать, что все собственные аксиомы теории K являются теоремами теории K′.)

Лемма 2.11. (Лемма Линденбаума.) *Если теория* K *первого порядка непротиворечива, то существует непротиворечивое полное ее расширение.*

Доказательство. Пусть $\mathscr{B}_1$, $\mathscr{B}_2$, ... — какой-нибудь пересчет всех замкнутых формул теории K (лемма 2.10). Следующим образом определим последовательность теорий J_0, J_1, J_2, ... Пусть J_0 есть K. Предположим, что теория J_n ($n \geqslant 0$) определена. Если неверно $\vdash_{J_n} \neg \mathscr{B}_{n+1}$, то J_{n+1} определим как теорию, получающуюся добавлением $\mathscr{B}_{n+1}$ к J_n в качестве новой аксиомы. Если же $\vdash_{J_n} \neg \mathscr{B}_{n+1}$, то полагаем $J_{n+1} = J_n$. Пусть J есть теория первого порядка, получающаяся, если в качестве аксиом взять все аксиомы всех теорий J_i. Очевидно, J_{n+1} служит расширением для J_n, а J является расширением каждой из теорий J_i, в том числе и теории $J_0 = K$. Для доказательства непротиворечивости теории J достаточно доказать непротиворечивость каждой из теорий J_i, так как всякий вывод противоречия в J использует лишь конечное число аксиом и, следовательно, является выводом противоречия уже в некоторой теории J_n. Докажем непротиворечивость теорий J_i индукцией по номеру i. По условию, теория $J_0 = K$ непротиворечива. Допустим, что теория J_i непротиворечива. Тогда, если $J_{i+1} = J_i$, то и теория J_{i+1} непротиворечива. Если же $J_{i+1} \neq J_i$ и, следовательно, согласно определению J_{i+1}, формула $\neg \mathscr{B}_{i+1}$ невыводима в J_i, то, по лемме 2.9, теория J_{i+1} тоже непротиворечива. Итак, непротиворечивость J_i влечет непротиворечивость J_{i+1}, и мы доказали, что все теории J_i непротиворечивы; непротиворечива, следовательно, и теория J. Для доказательства полноты теории J рассмотрим произвольную замкнутую формулу $\mathscr{A}$ теории K. Очевидно, $\mathscr{A} = \mathscr{B}_{j+1}$ при некотором j ($j \geqslant 0$). Согласно определению теорий J_i, либо $\vdash_{J_j} \neg \mathscr{B}_{j+1}$, либо $\vdash_{J_{j+1}} \mathscr{B}_{j+1}$, так как если не $\vdash_{J_j} \neg \mathscr{B}_{j+1}$, то $\mathscr{B}_{j+1}$ объявляется аксиомой в J_{j+1}. Следовательно, имеем $\vdash_J \neg \mathscr{B}_{j+1}$ или $\vdash_J \mathscr{B}_{j+1}$.

Таким образом, теория J является непротиворечивым полным расширением теории K.

Заметим, что если даже мы умеем эффективно распознавать аксиомы теории K, может тем не менее не существовать никакого эффективного способа распознавать (или даже перечислять) аксиомы теории J, т. е. J может не быть эффективно аксиоматизированной теорией, даже если K такова. Причиной этого может быть невозможность эффективного способа узнавать для любого n выводима или нет формула $\neg \mathscr{B}_{n+1}$ в J_n.

Упражнение

[D]Доказать, что всякая непротиворечивая разрешимая теория первого порядка имеет непротиворечивое разрешимое полное расширение.

Предложение 2.12 *). *Всякая непротиворечивая теория первого порядка имеет счетную модель (т. е. модель со счетной областью).*

Доказательство. Добавим к символам теории K счетное множество $\{b_1, b_2, \ldots\}$ новых предметных констант. Новую, полученную таким образом теорию назовем теорией K_0. Ее аксиомами являются все аксиомы теории K, а также все частные случаи схем логических аксиом, содержащие новые предметные константы. Теория K_0 непротиворечива. В самом деле, допустим, что для некоторой формулы $\mathscr{A}$ существует вывод в K_0 формулы $\mathscr{A} \& \neg \mathscr{A}$. Заменим всюду в этом выводе каждую встречающуюся в нем предметную константу b_i какой-нибудь предметной переменной, которая в этом выводе отсутствует. При такой замене участвующие в этом выводе аксиомы останутся аксиомами и сохранится свойство формул быть непосредственным следствием предыдущих формул по правилам вывода. Таким образом, после этой замены мы снова получим вывод, но теперь уже это будет вывод в K, поскольку ни одна из формул нового вывода не содержит предметных констант $b_1, b_2, \ldots$ Последняя формула этого вывода тоже является противоречием, что противоречит условию непротиворечивости теории K. Итак, теория K_0 непротиворечива.

Пусть $F_1(x_{i_1}), F_2(x_{i_2}), \ldots, F_k(x_{i_k}), \ldots$ — какой-нибудь пересчет всех формул теории K_0, содержащих не более одной свободной переменной (лемма 2.10). (Здесь x_{i_k} — свободная переменная формулы F_k, если же на самом деле F_k не содержит свободной переменной, то x_{i_k} есть x_1.)

Выберем какую-нибудь последовательность $b_{j_1}, b_{j_2}, \ldots, b_{j_k}, \ldots$, составленную из элементов множества $\{b_1, b_2, \ldots\}$, таким образом, чтобы постоянная b_{j_k} не содержалась в $F_1(x_{i_1}), \ldots, F_k(x_{i_k})$ и была отлична от $b_{j_1}, \ldots, b_{j_{k-1}}$. Рассмотрим формулу

$$(S_k) \qquad \neg \forall x_{i_k} F_k(x_{i_k}) \supset \neg F_k(b_{j_k}).$$

Определим теорию K_n как теорию первого порядка, получающуюся из теории K_0 в результате присоединения к аксиомам последней формул $(S_1), \ldots, (S_n)$ в качестве новых аксиом, а теорию K_ω — как теорию, получающуюся аналогичным образом присоединением всех формул (S_i) к аксиомам K_0. Всякий вывод в теории K_ω содержит лишь конечное

*) Мы здесь предлагаем упрощенное Хазенъегером [1953] доказательство Генкина [1949]. Впервые этот результат был установлен Гёделем [1930]. Расёва и Сикорский [1951, 1952] и Бет [1951] опубликовали доказательства, использующие соответственно алгебраические и топологические методы. Другие доказательства можно найти у Хинтикки [1955a, b] и Бета [1959].

множество формул (S_i) и потому является также выводом и в некоторой теории K_n. Следовательно, если все теории K_n непротиворечивы, то непротиворечива и теория K_ω. Индукцией по i докажем непротиворечивость теорий K_i. Непротиворечивость K_0 уже доказана. Допустим, что при некотором n $(n \geqslant 1)$ теория K_{n-1} непротиворечива, а теория K_n противоречива. Тогда, как мы знаем (в силу тавтологии $A_1 \supset (\neg A_1 \supset A_2)$ и предложения 2.1), в K_n выводима любая формула. В частности, $\vdash_{K_n} \neg(S_n)$. Поэтому $(S_n) \vdash_{K_{n-1}} \neg(S_n)$. Так как формула (S_n) замкнута, то, по следствию 2.6, $\vdash_{K_{n-1}} (S_n) \supset \neg(S_n)$. Теперь, принимая во внимание тавтологию $(A_1 \supset \neg A_1) \supset \neg A_1$ и предложение 2.1, мы получаем $\vdash_{K_{n-1}} \neg(S_n)$, т. е.

$$\vdash_{K_{n-1}} \neg(\neg \forall x_{i_n} F_n(x_{i_n}) \supset \neg F_n(b_{j_n})).$$

Используя затем тавтологии $\neg(A_1 \supset A_2) \supset (A_1 \,\&\, \neg A_2)$, $(A_1 \,\&\, A_2) \supset A_1$, $(A_1 \,\&\, A_2) \supset A_2$ и $\neg\neg A_1 \supset A_1$, мы получаем $\vdash_{K_{n-1}} \neg \forall x_{i_n} F_n(x_{i_n})$ и $\vdash_{K_{n-1}} F_n(b_{j_n})$.

Рассмотрим какой-нибудь вывод формулы $F_n(b_{j_n})$ в K_{n-1}. Пусть x_p — переменная, не встречающаяся в этом выводе. Тогда если всюду в этом выводе заменить b_{j_n} на x_p, то получим вывод $F_n(x_p)$ в K_{n-1}, т. е. $\vdash_{K_{n-1}} F_n(x_p)$. Теперь, по правилу Gen, получаем $\vdash_{K_{n-1}} \forall x_p F_n(x_p)$ и, наконец, по лемме 2.8, $\vdash_{K_{n-1}} \forall x_{i_n} F(x_{i_n})$. (Мы здесь используем тот факт, что формулы $F_n(x_{i_n})$ и $F_n(x_p)$ подобны.) Но, с другой стороны, выше мы установили, что $\vdash_{K_{n-1}} \neg \forall x_{i_n} F_n(x_{i_n})$. Таким образом, налицо противоречие с предположением о непротиворечивости K_{n-1}. Поэтому и теория K_n должна также быть непротиворечива. Итак, мы доказали, что все теории K_i, а с ними вместе и теория K_ω непротиворечивы. Заметим, что K_ω есть непротиворечивое расширение K_0. По лемме 2.11, K_ω имеет некоторое непротиворечивое полное расширение J.

Назовем *замкнутым термом* всякий терм, не содержащий переменных. Счетная интерпретация M теории K_0 будет иметь своей областью множество замкнутых термов теории K_0. (По лемме 2.10, это множество счетно.) Если c есть предметная константа в K_0, то она сама и будет своей интерпретацией. Функциональная буква f_j^n теории K будет интерпретироваться операцией f_j^{n*} в M, имеющей своими аргументами замкнутые термы $t_1, \ldots, t_n$ теории K_0 а значением — замкнутый терм $f_j^n(t_1, \ldots, t_n)$ той же теории. Отношение $(A_j^n)^*$, интерпретирующее предикатную букву A_j^n теории K, будет считаться выполненным в M для аргументов $t_1, \ldots, t_n$ тогда и только тогда, когда $\vdash_J A_j^n(t_1, \ldots, t_n)$. Чтобы доказать, что M является моделью K_0, достаточно доказать, что произвольная замкнутая формула $\mathscr{A}$ теории K_0 истинна в M тогда и только тогда, когда $\vdash_J \mathscr{A}$, так как все теоремы теории K_0 являются

также и теоремами теории J. Мы докажем это индукцией по числу связок и кванторов в $\mathscr{A}$. Пусть сначала $\mathscr{A}$ есть замкнутая элементарная формула. В этом случае формула $\mathscr{A}$, согласно определению, истинна в M тогда и только тогда, когда $\vdash_J \mathscr{A}$. Допустим теперь, что всякая замкнутая формула $\mathscr{B}$ с меньшим, чем у $\mathscr{A}$, числом связок и кванторов истинна в M тогда и только тогда, когда $\vdash_J \mathscr{B}$.

Случай 1. $\mathscr{A}$ имеет вид $\neg\mathscr{B}$. Если $\mathscr{A}$ истинна в M, то $\mathscr{B}$ ложна в M и, следовательно, в силу индуктивного предположения, не $\vdash_J \mathscr{B}$. Так как теория J полна, а формула $\mathscr{B}$ замкнута, то $\vdash_J \neg\mathscr{B}$, т. е. $\vdash_J \mathscr{A}$. С другой стороны, если $\mathscr{A}$ не истинна в M, то $\mathscr{B}$ истинна в M, и тогда $\vdash_J \mathscr{B}$, а так как теория J непротиворечива, то не $\vdash_J \neg\mathscr{B}$, т. е. не $\vdash_J \mathscr{A}$.

Случай 2. $\mathscr{A}$ есть $(\mathscr{B} \supset \mathscr{C})$. Из замкнутости $\mathscr{A}$ вытекает замкнутость $\mathscr{B}$ и $\mathscr{C}$. Если $\mathscr{A}$ ложна в M, то $\mathscr{B}$ истинна и $\mathscr{C}$ ложна в M. В силу полноты J, $\vdash_J \neg\mathscr{C}$. Тогда, согласно тавтологии $A_1 \supset (\neg A_2 \supset \supset \neg(A_1 \supset A_2))$, имеем $\vdash_J \neg(\mathscr{B} \supset \mathscr{C})$, т. е. $\vdash_J \neg\mathscr{A}$ и, в силу непротиворечивости J, не $\vdash_J \mathscr{A}$. С другой стороны, если не $\vdash_J \mathscr{A}$, то, в силу полноты J, $\vdash_J \neg\mathscr{A}$. Принимая во внимание тавтологии $\neg(A_1 \supset A_2) \supset A_1$ и $\neg(A_1 \supset A_2) \supset \neg A_2$, получаем тогда $\vdash_J \mathscr{B}$ и $\vdash_J \neg\mathscr{C}$. Следовательно, формула $\mathscr{B}$ истинна в M. В силу же непротиворечивости J, имеем не $\vdash_J \mathscr{C}$, и, следовательно, формула $\mathscr{C}$ ложна в M. Таким образом, $\mathscr{A}$ ложна в M.

Случай 3. $\mathscr{A}$ есть $\forall x_n \mathscr{B}$. Тогда, при некотором k, $\mathscr{B}$ есть $F_k(x_{i_k})$ и x_n есть x_{i_k}. (Здесь есть еще возможность того, что $\mathscr{B}$ замкнута и не содержит x_n свободно. Но в таком случае $\mathscr{A}$ истинна тогда и только тогда, когда $\mathscr{B}$ истинна (см. (VI) на стр. 60), и поэтому $\vdash_J \mathscr{A}$ тогда и только тогда, когда $\vdash_J \mathscr{B}$. Таким образом, интересующее нас утверждение для $\mathscr{A}$ следует из соответствующего утверждения о $\mathscr{B}$.) Предположим, что $\mathscr{A}$ истинна в M, но не $\vdash_J \mathscr{A}$. В силу полноты J, имеем $\vdash_J \neg\mathscr{A}$, т. е. $\vdash_J \neg \forall x_{i_k} F_k(x_{i_k})$. Однако, как мы знаем, $\vdash_J (S_k)$. Следовательно, $\vdash_J \neg F_k(b_{j_k})$. Так как формула $\mathscr{A} = \forall x_{i_k} F_k(x_{i_k})$ истинна в M, то истинна в M и формула $F_k(b_{i_k})$ (см. (X), следствие, стр. 61). По индуктивному предположению, получаем $\vdash_J F_k(b_{i_k})$ и приходим, таким образом, к противоречию с фактом непротиворечивости теории J. Допустим теперь, что $\mathscr{A}$ ложна в M, но $\vdash_J \mathscr{A}$. Из ложности формулы $\forall x_{i_k} F_k(x_{i_k})$ в M и из определения M как множества всех замкнутых термов теории K_0 вытекает (на основании (IV) и второй части (X) на стр. 60 и 61 *)), что для некоторого замкнутого терма t теории K_0 $F_k(t)$ ложно. Однако, по предположению, имеем $\vdash_J \forall x_{i_k} F_k(x_{i_k})$. Следова-

*) Здесь следует обратить внимание на то, что $s^*(t) = t$ для любой последовательности s элементов области M и для любого замкнутого терма t.

тельно, по аксиоме (4), $\vdash_J F_k(t)$ и, далее, по индуктивному предположению, формула $F_k(t)$ истинна в M. Мы снова пришли к противоречию.

Итак, M является счетной моделью для J, а следовательно, и для K_0. Так как всякая теорема теории K является также теоремой и теории K_0, то M и для теории K тоже служит счетной моделью. (Заметим, что модель M не всегда может быть эффективно построена. Интерпретация предикатных букв зависит от понятия выводимости в J, а это последнее, как было отмечено непосредственно после доказательства леммы 2.11 (стр. 74), может не быть эффективно разрешимым.)

Следствие 2.13. *Всякая логически общезначимая формула теории* K *первого порядка является теоремой теории* K.

Доказательство. Достаточно рассмотреть лишь замкнутые формулы $\mathscr{A}$, поскольку всякая формула $\mathscr{B}$ логически общезначима тогда и только тогда, когда логически общезначимо ее замыкание, и выводима в K тогда и только тогда, когда в K выводимо ее замыкание. Итак, пусть $\mathscr{A}$ — логически общезначимая замкнутая формула теории K. Допустим, что $\mathscr{A}$ не есть теорема в K. Тогда если мы добавим формулу $\neg\mathscr{A}$ в качестве новой аксиомы к теории K, то получим новую теорию K′, непротиворечивую в силу леммы 2.9. Теория K′ имеет, согласно предложению 2.12, модель M. Так как формула $\neg\mathscr{A}$ является аксиомой в K′, то $\neg\mathscr{A}$ истинна в M, а так как формула $\mathscr{A}$ логически общезначима, то и она истинна в M. Итак, мы пришли к тому, что формула $\mathscr{A}$ одновременно истинна и ложна в M, что невозможно (см. (II), стр. 59). Таким образом, формула $\mathscr{A}$ должна быть теоремой теории K.

Следствие 2.14. (Теорема Гёделя [1930] о полноте.) *Во всяком исчислении предикатов первого порядка теоремами являются все те и только те формулы, которые логически общезначимы.*

Доказательство. Следует из предложения 2.7 и следствия 2.13. (Первоначальное доказательство самого Гёделя следовало совсем другими путями. Конструктивное доказательство родственного результата см. у Эрбрана [1930], целый ряд других доказательств теоремы Гёделя о полноте можно найти у Дребена [1952], Хинтикка [1955 a, b], Бета [1951], Расёвой и Сикорского [1951], [1952].)

Следствие 2.15. (a) *Формула $\mathscr{A}$ истинна в каждой счетной модели теории* K *тогда и только тогда, когда $\vdash_K \mathscr{A}$. Следовательно, $\mathscr{A}$ истинна в каждой модели теории* K *тогда и только тогда, когда $\vdash_K \mathscr{A}$.*

(b) *Если во всякой модели теории* K *формула $\mathscr{B}$ выполнена на каждой последовательности, на которой выполнены все формулы некоторого множества формул* Γ, *то* $\Gamma \vdash_K \mathscr{B}$.

(c) *Если формула $\mathscr{B}$ теории* K *является логическим следствием* (см. стр. 62) *данного множества* Γ *формул теории* K, *то* $\Gamma \vdash_K \mathscr{B}$.

(d) *Если формула $\mathscr{B}$ теории* K *является логическим следствием формулы $\mathscr{A}$ той же теории, то* $\mathscr{A} \vdash_K \mathscr{B}$.

Доказательство. (a) Мы можем считать, что формула $\mathscr{A}$ замкнута. Допустим, что формула $\mathscr{A}$ истинна в любой счетной модели теории K. Если не $\vdash_K \mathscr{A}$, то теория $K' = K + \{\neg \mathscr{A}\}$ непротиворечива *). Следовательно, K′ имеет счетную модель M. Формула $\neg \mathscr{A}$, как аксиома теории K′, истинна в M. Но M является также моделью и для K, и потому $\mathscr{A}$ истинна в M. Таким образом, формула $\mathscr{A}$ одновременно истинна и ложна в M, и мы пришли к противоречию.

(b) Рассмотрим теорию $K + \Gamma$. Формула $\mathscr{B}$ истинна в каждой модели этой теории. Тогда, в силу утверждения (a), $\vdash_{K+\Gamma} \mathscr{B}$, и, следовательно, $\Gamma \vdash_K \mathscr{B}$.

Пункт (c), очевидно, следует из (b), а (d) является частным случаем (c).

Упражнение

Доказать, что $\vdash_K \mathscr{A}$ имеет место тогда и только тогда, когда существует формула $\mathscr{C}$, являющаяся замыканием конъюнкции некоторых аксиом теории K и такая, что формула $\mathscr{C} \supset \mathscr{A}$ логически общезначима.

Следствия 2.13—2.15 показывают, что для логики предикатов синтаксический метод теорий первого порядка равносилен семантическому методу, использующему понятия интерпретации, модели, логической общезначимости и т. п. Для исчисления высказываний аналогичная эквивалентность семантических (тавтология и др.) и синтаксических (теорема системы L и др.) понятий выражается следствием 1.14. Отметим также, что для исчисления высказываний теорема о полноте системы L (предложение 1.13) приводит к решению проблемы разрешения. Однако для теорий первого порядка мы не можем получить разрешающую процедуру для логической общезначимости или, что то же самое, для выводимости в любом исчислении предикатов первого порядка. Этот результат, а также некоторые родственные ему результаты будут доказаны ниже (гл. V).

Из предложения 2.12 вытекает еще один важный классический результат:

Следствие 2.16. (Теорема Сколема—Лёвенгейма [1919, 1915].) *Если теория* K *первого порядка имеет какую-нибудь модель, то она имеет и счетную модель.*

Доказательство. Если K имеет модель, то K непротиворечива (см. (II), стр. 59). Следовательно, в силу предложения 2.12, K имеет счетную модель.

Справедливо, однако, и следующее более сильное следствие предложения 2.12.

[A]Следствие 2.17. *Для любого кардинального числа* $\alpha \geqslant \aleph_0$ *всякая непротиворечивая теория* K *первого порядка имеет модель мощности* α.

*) Если K — теория и Δ — множество формул K, то через $K + \Delta$ обозначается теория, получающаяся из K добавлением формул Δ в качестве дополнительных аксиом.

Доказательство. Как мы знаем, согласно предложению 2.12, теория K имеет счетную модель. Поэтому для наших целей теперь достаточно доказать следующую лемму.

Лемма. *Если* α *и* β *— кардинальные числа, причем* $\alpha \leqslant \beta$, *и если* K *имеет модель мощности* α, *то* K *имеет модель и мощности* β.

Доказательство. Пусть M есть модель K с областью D мощности α, и пусть D′ — какое-нибудь множество мощности β, содержащее D. Расширим модель M до некоторой интерпретации M′ с областью D′ следующим образом. Пусть c — некоторый фиксированный элемент D. Условимся считать, что элементы множества D′ — D ведут себя, как c. Например, если B_j^n есть интерпретация в M предикатной буквы A_j^n, а $(B_j^n)'$ — новая интерпретация в M′, то для любых $d_1, \ldots, d_n$ из D′ $(B_j^n)'$ считается выполненным для $(d_1, \ldots, d_n)$ в том и только в том случае, когда B_j^n выполнено для $(u_1, \ldots, u_n)$, где $u_i = d_i$, если $d_i \in D$, и $u_i = c$, если $d_i \in D' - D$. Аналогично распространяется интерпретация функциональных букв, а интерпретации для предметных констант остаются прежними, т. е. берутся из M. Индукцией по числу связок и кванторов в формуле $\mathscr{A}$ нетрудно теперь доказать, что $\mathscr{A}$ истинна в M′ тогда и только тогда, когда $\mathscr{A}$ истинна в M. Следовательно, M′ является моделью K мощности β.

Упражнения

[A] **1.** Если для некоторой мощности $\alpha \geqslant \aleph_0$ формула $\mathscr{A}$ истинна в каждой интерпретации мощности α, то $\mathscr{A}$ логически общезначима.

[A] **2.** Если формула $\mathscr{A}$ истинна во всех интерпретациях мощности α, то $\mathscr{A}$ истинна во всех интерпретациях мощности $\leqslant \alpha$.

3. (a) Для всякой формулы $\mathscr{A}$ существует лишь конечное множество интерпретаций $\mathscr{A}$ на данной области, имеющей конечную мощность k.

(b) Для любой формулы $\mathscr{A}$ существует эффективный способ узнавать, является ли $\mathscr{A}$ истинной во всех интерпретациях с областью, имеющей некоторую фиксированную конечную мощность k. (Указание. Ввести новые предметные постоянные константы $b_1, \ldots, b_k$ и всякую формулу вида $\forall x \mathscr{B}(x)$ заменить на $\mathscr{B}(b_1)$ & ... & $\mathscr{B}(b_k)$.)

4. Показать, что следующая формула истинна во всех конечных областях, но в некоторой бесконечной области ложна:

$$\{\forall x \forall y \forall z [A_1^2(x, x) \& (A_1^2(x, y) \& A_1^2(y, z) \supset A_1^2(x, z)) \&$$

$$\& (A_1^2(x, y) \vee A_1^2(y, x))]\} \supset \exists y \forall x A_1^2(y, x).$$

5. (a) Замкнутая формула $\forall x_1 \ldots \forall x_n \exists y_1 \ldots \exists y_m \mathscr{A}$, где $m \geqslant 0$, $n \geqslant 1$ и $\mathscr{A}$ не содержит кванторов, функциональных букв или предметных постоянных, логически общезначима тогда и только тогда, когда она истинна во всякой интерпретации с областью, состоящей из n объектов.

(b) Замкнутая формула $\exists y_1 \ldots \exists y_m \mathscr{A}$ (где $\mathscr{A}$ удовлетворяет условию пункта (a)) логически общезначима тогда и только тогда, когда она истинна в каждой области, состоящей из одного элемента.

(c) Существует эффективная процедура для распознавания логической верности формул вида, описанного в (a) и (b).

§ 6. Некоторые дополнительные метатеоремы

Для облегчения дальнейшей работы с конкретными теориями первого порядка полезно доказать несколько дополнительных фактов об этих теориях. В этом параграфе мы всюду будем предполагать, что имеем дело с некоторой произвольной теорией K первого порядка.

Во многих случаях бывает желательно, доказав $\forall x \mathscr{A}(x)$, иметь также доказанным и $\mathscr{A}(t)$, где t — какой-нибудь терм, свободный для x в $\mathscr{A}(x)$. Это оказывается возможным, причем обосновывается следующим правилом.

Правило индивидуализации A4. *Если терм t свободен для x в $\mathscr{A}(x)$, то $\forall x \mathscr{A}(x) \vdash \mathscr{A}(t)$.*

Доказательство. Из $\forall x \mathscr{A}(x)$ и из частного случая $\forall x \mathscr{A}(x) \supset \mathscr{A}(t)$ аксиомы (4) мы получаем $\mathscr{A}(t)$ с помощью modus ponens.

Предложение 2.18. *Если $\mathscr{A}$ и $\mathscr{B}$ — формулы и предметная переменная x не является свободной в $\mathscr{A}$, то следующие формулы суть теоремы в* K:

(a) $\mathscr{A} \supset \forall x \mathscr{A}$ (следовательно, по аксиоме (4), $\vdash \mathscr{A} \equiv \forall x \mathscr{A}$);

(b) $\exists x \mathscr{A} \supset \mathscr{A}$ (следовательно, по нижеследующему правилу E4, $\vdash \exists x \mathscr{A} \equiv \mathscr{A}$);

(c) $\forall x (\mathscr{A} \supset \mathscr{B}) \equiv (\mathscr{A} \supset \forall x \mathscr{B})$;

(d) $\forall x (\mathscr{B} \supset \mathscr{A}) \equiv (\exists x \mathscr{B} \supset \mathscr{A})$.

Доказательство предоставляется читателю в качестве упражнения.

Полезно также следующее производное правило, которое является контрапозицией правила A4.

Правило существования E4. *Если терм t свободен для x в $\mathscr{A}(x)$, то $\vdash \mathscr{A}(t) \supset \exists x \mathscr{A}(x)$ и, следовательно, $\mathscr{A}(t) \vdash \exists x \mathscr{A}(x)$.*

Доказательство. По аксиоме (4) имеем $\vdash \forall x \neg \mathscr{A}(x) \supset \neg \mathscr{A}(t)$. С помощью тавтологии $(A \supset \neg B) \supset (B \supset \neg A)$ и MP получаем $\vdash \mathscr{A}(t) \supset \neg \forall x \neg \mathscr{A}(x)$, т. е. $\vdash \mathscr{A}(t) \supset \exists x \mathscr{A}(x)$. Следовательно, $\mathscr{A}(t) \vdash \exists x \mathscr{A}(x)$.

Упражнения

1. Вывести следующие производные правила:
Правило конъюнкции: $\mathscr{A}, \mathscr{B} \vdash \mathscr{A} \,\&\, \mathscr{B}$.
Правило дизъюнкции: $\mathscr{A} \supset \mathscr{C}, \mathscr{B} \supset \mathscr{D}, \mathscr{A} \vee \mathscr{B} \vdash \mathscr{C} \vee \mathscr{D}$.

2. Если формула $\mathscr{B}$ получена из $\mathscr{A}$ стиранием всех кванторов $\forall x$ или $\exists x$, области действия которых не содержат x свободно, то $\vdash \mathscr{A} \equiv \mathscr{B}$.

Предложение 2.19. *Для любых формул $\mathscr{A}$ и $\mathscr{B}$*

$$\vdash \forall x (\mathscr{A} \equiv \mathscr{B}) \supset (\forall x \mathscr{A} \equiv \forall x \mathscr{B}).$$

Доказательство.

1. $\forall x (\mathscr{A} \equiv \mathscr{B})$	гипотеза
2. $\forall x \mathscr{A}$	гипотеза
3. $\mathscr{A} \equiv \mathscr{B}$	1, правило A4
4. $\mathscr{A}$	2, правило A4

5. $\mathscr{B}$	3, 4, тавтология $(\mathscr{A} \equiv \mathscr{B}) \supset (\mathscr{A} \supset \mathscr{B})$, MP
6. $\forall x \mathscr{B}$	5, Gen
7. $\forall x (\mathscr{A} \equiv \mathscr{B}), \forall x \mathscr{A}(x) \vdash \forall x \mathscr{B}$	1—6
8. $\forall x (\mathscr{A} \equiv \mathscr{B}) \vdash \forall x \mathscr{A} \supset \forall x \mathscr{B}$	1—7, предложение 2.4
9. $\forall x (\mathscr{A} \equiv \mathscr{B}) \vdash \forall x \mathscr{B} \supset \forall x \mathscr{A}$	доказывается аналогично 8
10. $\forall x (\mathscr{A} \equiv \mathscr{B}) \vdash \forall x \mathscr{A} \equiv \forall x \mathscr{B}$	8,9, правило коньюнкции
11. $\vdash \forall x (\mathscr{A} \equiv \mathscr{B}) \supset (\forall x \mathscr{A} \equiv \forall x \mathscr{B})$	1—10, предложение 2.4

Предложение 2.20. (Теорема эквивалентности.) *Если $\mathscr{B}$ есть подформула $\mathscr{A}$ и $\mathscr{A}'$ есть результат замены в $\mathscr{A}$ каких-нибудь (быть может, также и ни одного) вхождений $\mathscr{B}$ формулой $\mathscr{C}$ и если всякая свободная переменная формулы $\mathscr{B}$ или формулы $\mathscr{C}$, которая одновременно является связанной переменной формулы $\mathscr{A}$, встречается в списке $y_1, \ldots, y_k$, то*

$$\vdash [\forall y_1 \ldots \forall y_k (\mathscr{B} \equiv \mathscr{C})] \supset (\mathscr{A} \equiv \mathscr{A}').$$

Доказательство. Применим индукцию по числу связок и кванторов в $\mathscr{A}$. Заметим сперва, что если ни одно вхождение $\mathscr{B}$ на самом деле не заменяется, то $\mathscr{A}$ совпадает с $\mathscr{A}'$, и формула, которую требуется вывести, является частным случаем тавтологии $B \supset (A \equiv A)$. Если $\mathscr{B}$ совпадает с $\mathscr{A}$ и это единственное вхождение заменяется на $\mathscr{C}$, то формула, которую требуется вывести, выводима из аксиомы (4) (см. упражнение 1 (d) на стр. 71). Итак, в дальнейшем мы можем считать, что $\mathscr{B}$ есть собственная подформула $\mathscr{A}$ и что по крайней мере одно вхождение $\mathscr{B}$ подлежит замене. Предположим, что теорема верна для всякой формулы с меньшим числом связок и кванторов, чем у $\mathscr{A}$.

Случай 1. $\mathscr{A}$ есть элементарная формула. Тогда $\mathscr{B}$ не может быть собственной подформулой $\mathscr{A}$.

Случай 2. $\mathscr{A}$ есть $\neg \mathscr{D}$. Пусть тогда $\mathscr{A}'$ есть $\neg \mathscr{D}'$. По индуктивному предположению, $\vdash \forall y_1 \ldots \forall y_k (\mathscr{B} \equiv \mathscr{C}) \supset (\mathscr{D} \equiv \mathscr{D}')$. Отсюда с помощью тавтологии $(A \equiv B) \supset (\neg A \equiv \neg B)$ получаем $\vdash \forall y_1 \ldots \forall y_k (\mathscr{B} \equiv \mathscr{C}) \supset (\mathscr{A} \equiv \mathscr{A}')$.

Случай 3. $\mathscr{A}$ есть $\mathscr{D} \supset \mathscr{E}$. Пусть тогда $\mathscr{A}'$ есть $\mathscr{D}' \supset \mathscr{E}'$. Согласно индуктивному предположению, $\vdash \forall y_1 \ldots \forall y_k (\mathscr{B} \equiv \mathscr{C}) \supset (\mathscr{D} \equiv \mathscr{D}')$ и $\forall y_1 \ldots \forall y_k (\mathscr{B} \equiv \mathscr{C}) \supset (\mathscr{E} \equiv \mathscr{E}')$. Применяя тавтологию $((A \equiv B) \& (C \equiv D)) \supset ((A \supset C) \equiv (B \supset D))$, получаем $\vdash \forall y_1 \ldots \forall y_k (\mathscr{B} \equiv \mathscr{C}) \supset (\mathscr{A} \equiv \mathscr{A}')$.

Случай 4. $\mathscr{A}$ есть $\forall x \mathscr{D}$. Тогда для некоторой формулы $\mathscr{D}'$ $\mathscr{A}$ совпадает с $\forall x \mathscr{D}'$. По индуктивному предположению, $\vdash \forall y_1 \ldots \forall y_k (\mathscr{B} \equiv \mathscr{C}) \supset (\mathscr{D} \equiv \mathscr{D}')$. Переменная x не встречается свободно в $\forall y_1 \ldots \forall y_k (\mathscr{B} \equiv \mathscr{C})$; в самом деле, если бы x входила свободно

в эту последнюю формулу, то x входила бы свободно в $\mathscr{B}$ или в $\mathscr{C}$, а поскольку x связана в $\mathscr{A}$, x входила бы в перечень $y_1, \ldots, y_k$ и была бы связанной переменной в $\forall y_1 \ldots \forall y_k (\mathscr{B} \equiv \mathscr{C})$, что приводит нас к противоречию. Применяя теперь аксиому (5), мы получаем $\vdash \forall y_1 \ldots \forall y_k (\mathscr{B} \equiv \mathscr{C}) \supset \forall x (\mathscr{D} \equiv \mathscr{D}')$. В то же время, в силу предложения 2.19, имеем $\forall x (\mathscr{D} \supset \mathscr{D}') \supset (\forall x \mathscr{D} \equiv \forall x \mathscr{D}')$. Сопоставляя последние два утверждения о выводимости, получаем $\vdash \forall y_1 \ldots \forall y_k (\mathscr{B} \equiv \mathscr{C}) \supset \supset (\mathscr{A} \equiv \mathscr{A}')$.

Следствие 2.21. (Теорема о замене.) *Пусть* $\mathscr{A}$, $\mathscr{B}$, $\mathscr{A}'$ *и* $\mathscr{C}$ *удовлетворяют условиям предложения* 2.20. *Если* $\vdash \mathscr{B} \equiv \mathscr{C}$, *то* $\vdash \mathscr{A} \equiv \mathscr{A}'$, *а если* $\vdash \mathscr{B} \equiv \mathscr{C}$ *и* $\vdash \mathscr{A}$, *то* $\vdash \mathscr{A}'$.

Следствие 2.22. (Переименование связанных переменных.) *Если* $\forall x \mathscr{B}(x)$ *есть подформула формулы* $\mathscr{A}$, *формула* $\mathscr{B}(y)$ *подобна формуле* $\mathscr{B}(x)$ *и* $\mathscr{A}'$ *есть результат замены по крайней мере одного вхождения* $\forall x \mathscr{B}(x)$ *в* $\mathscr{A}$ *на* $\forall y \mathscr{B}(y)$, *то* $\vdash \mathscr{A} \equiv \mathscr{A}'$.

Доказательство. Применить лемму 2.8 и следствие 2.21.

Упражнения

1. Доказать, что $\vdash \exists x \neg \mathscr{A} \equiv \neg \forall x \mathscr{A}$ и $\vdash \forall x \mathscr{A} \equiv \neg \exists x \neg \mathscr{A}$.

2. Пусть $\mathscr{A}$ — формула, содержащая, быть может, кванторы и связки $\&$, $\vee$, $\neg$, но не содержащая связок $\supset$, $\equiv$. Всюду в $\mathscr{A}$ поменяем взаимно кванторы существования и всеобщности, а также связки $\&$ и $\vee$. Полученная в результате формула $\mathscr{A}^*$ называется *двойственной* к $\mathscr{A}$*). Доказать, что (a) $\vdash \mathscr{A}$ тогда и только тогда, когда $\vdash \neg \mathscr{A}^*$; (b) $\vdash \mathscr{A} \supset \mathscr{B}$ тогда и только тогда, когда $\vdash \mathscr{B}^* \supset \mathscr{A}^*$; (c) $\vdash \mathscr{A} \equiv \mathscr{B}$ тогда и только тогда, когда $\vdash \mathscr{A}^* \equiv \mathscr{B}^*$; (d) применяя $\vdash \forall x (\mathscr{A} \,\&\, \mathscr{B}) \equiv \forall x \mathscr{A} \,\&\, \forall x \mathscr{B}$ (см. упражнение 1 (c), стр. 71), доказать, что $\vdash \exists x (\mathscr{A} \vee \mathscr{B}) \equiv \exists x \mathscr{A} \vee \exists x \mathscr{B}$.

§ 7. Правило C

В математике весьма распространены умозаключения следующего типа. Допустим, что мы вывели формулу вида $\exists x \mathscr{A}(x)$. Затем мы говорим: «Пусть b — объект такой, что $\mathscr{A}(b)$», и продолжаем наше рассуждение или доказательство, приходя в конце концов к формуле, которая не содержит произвольно выбранного элемента b.

Пусть, скажем, мы хотим доказать, что

$$\exists x (\mathscr{B}(x) \supset \mathscr{C}(x)),\ \forall x \mathscr{B}(x) \vdash \exists x \mathscr{C}(x):$$

1. $\exists x (\mathscr{B}(x) \supset \mathscr{C}(x))$	гипотеза
2. $\forall x \mathscr{B}(x)$	гипотеза
3. $\mathscr{B}(b) \supset \mathscr{C}(b)$ при некотором b	1

*) Вот точное определение операции *: 1) если $\mathscr{A}$ — элементарная формула, то $\mathscr{A}^*$ есть $\mathscr{A}$; 2) $(\mathscr{A} \,\&\, \mathscr{B})^*$ есть $\mathscr{A}^* \vee \mathscr{B}^*$; 3) $(\mathscr{A} \vee \mathscr{B})^*$ есть $\mathscr{A}^* \,\&\, \mathscr{B}^*$; 4) $(\neg \mathscr{A})^*$ есть $\neg \mathscr{A}^*$; 5) $(\forall x \mathscr{A})^*$ есть $\exists x \mathscr{A}^*$; 6) $(\exists x \mathscr{A})^*$ есть $\forall x \mathscr{A}^*$. (*Прим. перев.*)

4. $\mathscr{B}(b)$ — 2, правило A4
5. $\mathscr{C}(b)$ — 3, 4, MP
6. $\exists x \mathscr{C}(x)$ — 5, правило E4
7. $\exists x(\mathscr{B}(x) \supset \mathscr{C}(x)),\ \forall x \mathscr{B}(x) \vdash \exists x \mathscr{C}(x)$ — 1—6

Такой вывод представляется с интуитивной точки зрения совершенно законным. На самом же деле мы можем получить тот же результат, не прибегая к произвольному выбору некоторого элемента на шаге 3. Это может быть сделано следующим образом:

1. $\forall x \mathscr{B}(x)$ — гипотеза
2. $\forall x \neg \mathscr{C}(x)$ — гипотеза
3. $\mathscr{B}(x)$ — 1, правило A4
4. $\neg \mathscr{C}(x)$ — 2, правило A4
5. $\neg(\mathscr{B}(x) \supset \mathscr{C}(x))$ — 3, 4, тавтология $(A \& \neg B) \supset \supset \neg(A \supset B)$
6. $\forall x \neg(\mathscr{B}(x) \supset \mathscr{C}(x))$ — 5. Gen
7. $\forall x \mathscr{B}(x),\ \forall x \neg \mathscr{C}(x) \vdash \forall x \neg(\mathscr{B}(x) \supset \mathscr{C}(x))$ — 1—6
8. $\forall x \mathscr{B}(x) \vdash \forall x \neg \mathscr{C}(x) \supset \forall x \neg(\mathscr{B}(x) \supset \mathscr{C}(x))$ — 7, предложение 2.4
9. $\forall x \mathscr{B}(x) \vdash \neg \forall x \neg(\mathscr{B}(x) \supset \mathscr{C}(x)) \supset \neg \forall x \neg \mathscr{C}(x)$ — 8, тавтология $(A \supset B) \supset \supset (\neg B \supset \neg A)$
10. $\forall x \mathscr{B}(x) \vdash \exists x(\mathscr{B}(x) \supset \mathscr{C}(x)) \supset \exists x \mathscr{C}(x)$ — сокращение для 9
11. $\exists x(\mathscr{B}(x) \supset \mathscr{C}(x)),\ \forall x \mathscr{B}(x) \vdash \exists x \mathscr{C}(x)$ — 10, MP

Вообще всякая формула, которая может быть выведена с применением подобных произвольных актов выбора, может быть также выведена и без помощи таких актов выбора. Правило, позволяющее переходить от $\exists x \mathscr{A}(x)$ к $\mathscr{A}(b)$, будем называть *Правилом* C (C — первая буква английского слова choice — выбор). Для большей точности следовало бы говорить о понятии «вывода с правилом C» в теории первого порядка K. Это правило можно определить следующим образом:

$\Gamma \vdash_C \mathscr{A}$ тогда и только тогда, когда существует последовательность формул $\mathscr{B}_1, \ldots, \mathscr{B}_n = \mathscr{A}$ такая, что выполняются следующие условия:

(l) для любого i либо

(i) $\mathscr{B}_i$ есть аксиома K, либо

(ii) $\mathscr{B}_i$ принадлежит Γ, либо

(iii) $\mathscr{B}_i$ следует по MP или Gen из формул, предшествующих в этой последовательности формуле $\mathscr{B}_i$, либо

(iv) формуле $\mathscr{B}_i$ предшествует формула $\exists x \mathscr{C}(x)$, а сама формула $\mathscr{B}_i$ есть $\mathscr{C}(b)$, где b — новая предметная постоянная. (Правило C.)

(II) В качестве аксиом в (I) (i) разрешаются также всевозможные логические аксиомы, включающие новые предметные постоянные, уже ранее введенные по правилу С, т. е. по (I) (iv).

(III) Не допускается применение правила Gen по переменным, свободным хотя бы в одной формуле вида $\exists x \mathscr{C}(x)$, к которой ранее было применено правило С.

(IV) $\mathscr{A}$ не содержит новых предметных постоянных, введенных с помощью правила С.

Следует обратить внимание на то, что пункт (III) определения действительно необходим, ибо без ограничений, накладываемых этим пунктом, становится возможным, например, такой вывод:

1. $\forall x \exists y A_1^2(x, y)$	гипотеза
2. $\exists y A_1^2(x, y)$	1, правило А4
3. $A_1^2(x, b)$	2, правило С
4. $\forall x A_1^2(x, b)$	3, Gen
5. $\exists y \forall x A_1^2(x, y)$	4, правило Е4
6. $\forall x \exists y A_1^2(x, y) \vdash_C \exists y \forall x A_1^2(x, y)$	1—5

А между тем мы знаем (см. пример 4 на стр. 63), что существует интерпретация, для которой формула $\forall x \exists y A_1^2(x, y)$ истинна, а формула $\exists y \forall x A_1^2(x, y)$ ложна.

Предложение 2.23. *Если* $\Gamma \vdash_C \mathscr{A}$, *то* $\Gamma \vdash \mathscr{A}$. Более того, из нижеследующего доказательства легко усмотреть, что если в новом выводе имеется применение правила Gen по некоторой переменной к формуле, зависящей от некоторой формулы из Γ, то такое же применение Gen было и в первоначальном выводе *).

Доказательство. Пусть дан какой-нибудь С-вывод формулы $\mathscr{A}$ из Γ, и пусть $\exists y_1 \mathscr{C}_1(y_1), \ldots, \exists y_k \mathscr{C}_k(y_k)$ — формулы (в порядке их появления), к которым в этом С-выводе применяется правило С, а $c_1, \ldots, c_k$ — вводимые при этом новые предметные константы. Тогда, очевидно, $\Gamma, \mathscr{C}_1(c_1), \ldots, \mathscr{C}_k(c_k) \vdash \mathscr{A}$, а в силу ограничения на применение правила Gen в первоначальном С-выводе, мы можем применить теорему дедукции 2.4 и, следовательно, $\Gamma, \mathscr{C}_1(c_1), \ldots, \mathscr{C}_{k-1}(c_{k-1}) \vdash \vdash \mathscr{C}_k(c_k) \supset \mathscr{A}$. Заменив всюду в соответствующем выводе константу c_k на переменную z, не встречающуюся в этом выводе, мы получим

$$\Gamma, \mathscr{C}_1(c_1), \ldots, \mathscr{C}_{k-1}(c_{k-1}) \vdash \mathscr{C}_k(z) \supset \mathscr{A}$$

и, следовательно, по правилу Gen,

$$\Gamma, \mathscr{C}_1(c_1), \ldots, \mathscr{C}_{k-1}(c_{k-1}) \vdash \forall z (\mathscr{C}_k(z) \supset \mathscr{A}),$$

отсюда, на основании предложения 2.18 (d), получаем

$$\Gamma, \mathscr{C}_1(c_1), \ldots, \mathscr{C}_{k-1}(c_{k-1}) \vdash \exists y_k \mathscr{C}_k(y_k) \supset \mathscr{A}.$$

*) По-видимому, впервые правило С в схожей форме сформулировал Россер [1953].

Но так как

$$\Gamma, \mathscr{C}_1(c_1), \ldots, \mathscr{C}_{k-1}(c_{k-1}) \vdash \exists y_k \mathscr{C}_k(y_k),$$

то

$$\Gamma, \mathscr{C}_1(c_1), \ldots, \mathscr{C}_{k-1}(c_{k-1}) \vdash \mathscr{A}.$$

Повторяя эту же схему рассуждений, мы теперь исключим по очереди $\mathscr{C}_{k-1}(c_{k-1})$, $\mathscr{C}_{k-2}(c_{k-2})$ и т. д. вплоть до $\mathscr{C}_1(c_1)$, в результате чего получим $\Gamma \vdash \mathscr{A}$.

Пример. $\vdash \forall x(\mathscr{A}(x) \supset \mathscr{B}(x)) \supset (\exists x \mathscr{A}(x) \supset \exists x \mathscr{B}(x))$.

1. $\forall x(\mathscr{A}(x) \supset \mathscr{B}(x))$	гипотеза
2. $\exists x \mathscr{A}(x)$	гипотеза
3. $\mathscr{A}(b)$	2, правило С
4. $\mathscr{A}(b) \supset \mathscr{B}(b)$	1, правило А4
5. $\mathscr{B}(b)$	3, 4, MP
6. $\exists x \mathscr{B}(x)$	5, правило Е4
7. $\forall x(\mathscr{A}(x) \supset \mathscr{B}(x)), \exists x \mathscr{A}(x) \vdash_C \exists x \mathscr{B}(x)$	1—6
8. $\forall x(\mathscr{A}(x) \supset \mathscr{B}(x)), \exists x \mathscr{A}(x) \vdash \exists x \mathscr{B}(x)$	7, предложение 2.23
9. $\forall x(\mathscr{A}(x) \supset \mathscr{B}(x)) \vdash \exists x \mathscr{A}(x) \supset \exists x \mathscr{B}(x)$	8, предложение 2.24
10. $\vdash \forall x(\mathscr{A}(x) \supset \mathscr{B}(x)) \supset (\exists x \mathscr{A}(x) \supset \exists x \mathscr{B}(x))$	9, предложение 2.24

Упражнения

С помощью правила С и предложения 2.23 доказать:

(1) $\vdash \exists x(\mathscr{A}(x) \supset \mathscr{B}(x)) \supset (\forall x \mathscr{A}(x) \supset \exists x \mathscr{B}(x))$;

(2) $\vdash (\forall x \mathscr{A}(x) \vee \forall x \mathscr{B}(x)) \supset \forall x(\mathscr{A}(x) \vee \mathscr{B}(x))$.

§ 8. Теории первого порядка с равенством

Пусть K — теория первого порядка, в числе предикатных букв которой имеется A_1^2. Будем для сокращения писать $t = s$ вместо $A_1^2(t, s)$ и $t \neq s$ вместо $\neg A_1^2(t, s)$. Теория K называется *теорией первого порядка с равенством*, если следующие формулы являются теоремами K:

(6*) $\forall x_1(x_1 = x_1)$ (рефлексивность равенства);

(7) $(x = y) \supset (\mathscr{A}(x, x) \supset \mathscr{A}(x, y))$ (подстановочность равенства),

где x и y — предметные переменные, $\mathscr{A}(x, x)$ — произвольная формула, а $\mathscr{A}(x, y)$ получается из $\mathscr{A}(x, x)$ заменой каких-нибудь (не обязательно всех) свободных вхождений x вхождениями y, с соблюдением условия, чтобы y было свободно для тех вхождений x, которые заменяются.

*) Мы здесь продолжаем нумерацию логических аксиом на стр. 65—66.

Таким образом, в одних случаях $\mathscr{A}(x, y)$ может иметь свободные вхождения x, в других случаях таких вхождений может уже не быть.

Предложение 2.24. *Во всякой теории первого порядка с равенством*

(a) $\vdash t = t$ *для любого терма* t;

(b) $\vdash x = y \supset y = x$;

(c) $\vdash x = y \supset (y = z \supset x = z)$.

Доказательство. (a) В силу (6), $\vdash \forall x_1 (x_1 = x_1)$, следовательно, по правилу A4 $\vdash t = t$.

(b) Пусть $\mathscr{A}(x, x)$ есть $x = x$ и $\mathscr{A}(x, y)$ есть $y = x$. Тогда, согласно (7), $\vdash (x = y) \supset (x = x \supset y = x)$. Но, как только что доказано, $\vdash x = x$. Теперь $\vdash x = y \supset y = x$ мы получим с помощью тавтологии $B \supset ((A \supset (B \supset C)) \supset (A \supset C))$.

(c) Пусть $\mathscr{A}(y, y)$ есть $y = z$ и $\mathscr{A}(y, x)$ есть $x = z$. Тогда, в силу (7) с взаимной заменой x и y, $\vdash y = x \supset (y = z \supset x = z)$. Но в силу (b), $\vdash x = y \supset y = x$. Следовательно, используя тавтологию $(A \supset B) \supset \supset ((B \supset C) \supset (A \supset C))$, мы имеем $\vdash x = y \supset (y = z \supset x = z)$.

Упражнения

Доказать:

(1) $\vdash \forall x (\mathscr{B}(x) \equiv \exists y (x = y \,\&\, \mathscr{B}(y)))$;

(2) $\vdash \forall x (\mathscr{B}(x) \equiv \forall y (x = y \supset \mathscr{B}(y)))$;

(3) $\vdash \forall x \exists y (x = y)$.

Условие (7) для равенства может быть сведено к нескольким более простым случаям.

Предложение 2.25. *Если теоремами теории первого порядка* K *являются формула* (6) *и, для любой элементарной формулы* $\mathscr{A}(x, x)$, *формула* (7), *то* K *есть теория первого порядка с равенством, т. е. в* K *всякая формула вида* (7) *является теоремой.*

Доказательство. Итак, мы должны доказать, что всякая формула вида (7) является теоремой в K. Для элементарных формул это верно по условию. Заметим, что для рассматриваемой теории K предложение 2.24 верно, ибо в его доказательстве используется (7) только для элементарных формул. Следуя индукции по числу n всех связок и кванторов в $\mathscr{A}$, предположим, что для всех $k < n$ все формулы вида (7) являются теоремами в K.

Случай 1. $\mathscr{A}(x, x)$ есть $\neg\mathscr{B}(x, x)$. По индуктивному предположению мы имеем $\vdash y = x \supset (\mathscr{B}(x, y) \supset \mathscr{B}(x, x))$, так как $\mathscr{B}(x, x)$ получается из $\mathscr{B}(x, y)$ заменой некоторых вхождений y на x. Отсюда, применяя предложение 2.24(b) и тавтологии $(A \supset B) \supset (\neg B \supset \neg A)$ и $(A \supset B) \supset ((B \supset C) \supset (A \supset C))$, получаем $\vdash x = y \supset (\mathscr{A}(x, x) \supset \supset \mathscr{A}(x, y))$.

Случай 2. $\mathscr{A}(x, x)$ есть $\mathscr{B}(x, x) \supset \mathscr{C}(x, x)$. В силу индуктивного предположения и предложения 2.24(b), $\vdash x = y \supset (\mathscr{B}(x, y) \supset \mathscr{B}(x, x))$ и $\vdash x = y \supset (\mathscr{C}(x, x) \supset \mathscr{C}(x, y))$. Отсюда с помощью тавтологии $(A \supset (B_1 \supset B)) \supset [(A \supset (C \supset C_1)) \supset (A \supset ((B \supset C) \supset (B_1 \supset C_1)))]$ получаем $\vdash x = y \supset (\mathscr{A}(x, x) \supset \mathscr{A}(x, y))$.

Случай 3. $\mathscr{A}(x, x)$ есть $\forall z \mathscr{B}(x, x, z)$. По индуктивному предположению, $\vdash x = y \supset (\mathscr{B}(x, x, z) \supset \mathscr{B}(x, y, z))$. Применяя правило Gen и аксиому (5), получаем $\vdash x = y \supset \forall z (\mathscr{B}(x, x, z) \supset \mathscr{B}(x, y, z))$. В силу упражнения 1 (a) на стр. 71 имеем $\forall z (\mathscr{B}(x, x, z) \supset \mathscr{B}(x, y, z)) \supset [\forall z \mathscr{B}(x, x, z) \supset \forall z \mathscr{B}(x, y, z)]$ и теперь с помощью тавтологии $(A \supset B) \supset ((B \supset C) \supset (A \supset C))$ получаем окончательно $\vdash x = y \supset (\mathscr{A}(x, x) \supset \mathscr{A}(x, y))$.

Сужение класса формул $\mathscr{A}(x, x)$ в (7) может быть продолжено еще дальше.

Предложение 2.26. *Пусть* K — *теория первого порядка, в которой к числу теорем принадлежит формула* (6), *а также все формулы вида* (7), *в которых формула* $\mathscr{A}(x, x)$ *элементарна, не содержит вхождений функциональных букв и* $\mathscr{A}(x, y)$ *получается из* $\mathscr{A}(x, x)$ *замещением на* y *в точности одного вхождения* x. *Пусть, кроме того*: (*) *для всякой функциональной буквы* f_j^n *и для всякого набора переменных* $z_1, \ldots, z_n$ *выполнено* $\vdash x = y \supset f_j^n(z_1, \ldots, z_n) = f_j^n(w_1, \ldots, w_n)$, *где* $f_j^n(w_1, \ldots, w_n)$ *получено из* $f_j^n(z_1, \ldots, z_n)$ *заменой какого-нибудь одного вхождения* x *на* y. *Тогда* K *есть теория первого порядка с равенством.*

Доказательство. Отметим сразу, что случаи замены многих вхождений x на y сводятся, очевидно, к последовательным актам замещения одного вхождения x на y. Легко видеть, что и предложение 2.24 все еще доказуемо и в условиях настоящей теоремы. В силу предложения 2.25, достаточно доказать, что теоремами в K являются все формулы вида (7) с элементарными $\mathscr{A}$. При этом не составляет труда доказать, что $\vdash y_1 = z_1 \,\&\, \ldots \,\&\, y_n = z_n \supset (\mathscr{A}(y_1, \ldots, y_n) \supset \mathscr{A}(z_1, \ldots, z_n))$ для любого набора переменных $y_1, \ldots, y_n, z_1, \ldots, z_n$ и для любой элементарной формулы $\mathscr{A}$ без вхождений функциональных букв. Применяя правило A4, мы теперь можем свести доказательство к установлению факта $\vdash x = y \supset t(x, x) = t(x, y)$, где $t(x, x)$ — терм и $t(x, y)$ получен из $t(x, x)$ замещением на y некоторых вхождений x. Но это без труда может быть доказано с использованием условия (*) индукцией по числу функциональных букв, входящих в t, и мы предоставляем читателю проделать это самому в качестве упражнения.

Упражнения

1. Пусть K_1 — теория первого порядка с единственной предикатной буквой $=$, без функциональных букв и предметных констант и с собственными аксиомами: $\forall x_1 (x_1 = x_1)$, $\forall x_1 \forall x_2 (x_1 = x_2 \supset x_2 = x_1)$ и $\forall x_1 \forall x_2 \forall x_3 (x_1 = x_2 \supset (x_2 = x_3 \supset x_1 = x_3))$. Доказать, что K_1 есть теория первого порядка с равенством.

Указание. В силу предложения 2.26, достаточно вывести следующие формулы:

$$x=y \supset (x=x \supset y=x),$$
$$x=y \supset (x=x \supset x=y),$$
$$x=y \supset (x=y \supset y=y),$$
$$x=y \supset (y=x \supset y=y),$$
$$x=y \supset (x=z \supset y=z),$$
$$x=y \supset (z=x \supset z=y).$$

Теория K_1 называется элементарной теорией равенства.

2. Пусть K_2 — теория первого порядка с двумя предикатными буквами $=$ и $<$, без функциональных букв и предметных констант и со следующими собственными аксиомами:

(a) $\forall x_1\,(x_1=x_1)$;
(b) $\forall x_1 \forall x_2\,(x_1=x_2 \supset x_2=x_1)$;
(c) $\forall x_1 \forall x_2 \forall x_3\,(x_1=x_2 \supset (x_2=x_3 \supset x_1=x_3))$;
(d) $\forall x_1 \exists x_2 \exists x_3\,(x_1<x_2 \,\&\, x_3<x_1)$;
(e) $\forall x_1 \forall x_2 \forall x_3\,(x_1<x_2 \,\&\, x_2<x_3 \supset x_1<x_3)$;
(f) $\forall x_1 \forall x_2\,(x_1=x_2 \supset \neg\, x_1<x_2)$;
(g) $\forall x_1 \forall x_2\,(x_1<x_2 \vee x_1=x_2 \vee x_2<x_1)$;
(h) $\forall x_1 \forall x_2\,(x_1<x_2 \supset \exists x_3\,(x_1<x_3 \,\&\, x_3<x_2))$.

Опираясь на предложение 2.26, показать, что K_2 есть теория первого порядка с равенством. (K_2 есть элементарная теория плотно упорядоченных множеств без первого и последнего элементов.)

3. Пусть K — произвольная теория первого порядка с равенством. (a) Доказать, что $\vdash_K x_1=y_1 \,\&\, \ldots \,\&\, x_n=y_n \supset t(x_1, \ldots, x_n)=t(y_1, \ldots, y_n)$, где $t(y_1, \ldots, y_n)$ получено из терма $t(x_1, \ldots, x_n)$ заменой $x_1, \ldots, x_n$ соответственно на $y_1, \ldots, y_n$. (b) Доказать, что $\vdash_K x_1=y_1 \,\&\, \ldots \,\&\, x_n=y_n \supset (\mathscr{A}(x_1, \ldots, x_n) \equiv \mathscr{A}(y_1, \ldots, y_n))$, где $\mathscr{A}(y_1, \ldots, y_n)$ получено заменой одного или более вхождений x_i на y_i, $i=1, 2, \ldots, n$, причем $y_1, \ldots, y_n$ свободны в $\mathscr{A}(x_1, \ldots, x_n)$ для $x_1, \ldots, x_n$ соответственно.

Примеры:

1. Элементарная теория групп G: предикатная буква $=$, функциональная буква f_1^2, предметная константа a_1. Для сокращения в дальнейшем мы будем вместо $f_1^2(t, s)$ писать $t+s$ и 0 вместо a_1. Собственные аксиомы:

(a) $x_1+(x_2+x_3)=(x_1+x_2)+x_3$;
(b) $x_1+0=x_1$;
(c) $\forall x_1 \exists x_2\,(x_1+x_2=0)$;
(d) $x_1=x_1$;
(e) $x_1=x_2 \supset x_2=x_1$;
(f) $x_1=x_2 \supset (x_2=x_3 \supset x_1=x_3)$;
(g) $x_1=x_2 \supset (x_1+x_3=x_2+x_3 \,\&\, x_3+x_1=x_3+x_2)$.

Опираясь на предложение 2.26, легко доказать, что G есть теория первого порядка с равенством. Если мы добавим еще одну аксиому:

(h) $x_1+x_2=x_2+x_1$,

то получим теорию G_C, называемую элементарной теорией абелевых групп.

2. Элементарная теория полей F: предикатная буква $=$, функциональные буквы f_1^2 и f_2^2, предметные константы a_1 и a_2. Сокращениями служат: $t+s$ для $f_1^2(t, s)$, $t \cdot s$ для $f_2^2(t, s)$, 0 и 1 для a_1 и a_2 соответственно. Собственными аксиомами являются аксиомы (a) — (h) теории G_C из предыдущего примера 1, а также следующие формулы:

(i) $x_1 = x_2 \supset (x_1 \cdot x_3 = x_2 \cdot x_3 \,\&\, x_3 \cdot x_1 = x_3 \cdot x_2)$;
(j) $(x_1 \cdot x_2) \cdot x_3 = x_1 \cdot (x_2 \cdot x_3)$;
(k) $x_1 \cdot (x_2 + x_3) = (x_1 \cdot x_2) + (x_1 \cdot x_3)$;
(l) $x_1 \cdot x_2 = x_2 \cdot x_1$;
(m) $x_1 \cdot 1 = x$;
(n) $x_1 \neq 0 \supset \exists x_2 (x_1 \cdot x_2 = 1)$.

F является теорией первого порядка с равенством. Аксиомы (a) — (m) определяют элементарную теорию R_C коммутативных колец с единицей. Добавив к F новую предикативную букву A_2^2, которую будем обозначать знаком $<$, аксиомы (e), (f), (g) из предыдущего упражнения 2 и еще две аксиомы: $x_1 < x_2 \supset x_1 + x_3 < x_2 + x_3$, $x_1 < x_2 \,\&\, 0 < x_3 \supset \supset x_1 \cdot x_3 < x_2 \cdot x_3$, мы получим элементарную теорию $F_<$ упорядоченных полей.

Упражнение

Показать, что аксиомы равенства (d) — (f) в двух последних примерах могут быть заменены парой аксиом, из которых одна есть снова (d), а другая — формула $x = y \supset (z = y \supset x = z)$.

Часто встречаются теории первого порядка, в которых равенство $=$ может быть определено. Это значит, что в такой теории K имеется формула $\mathscr{E}(x, y)$, для которой, если $\mathscr{E}(t, s)$ обозначить через $t = s$, формулы (6), (7) выводимы в K. При этом только следует условиться считать, что если t и s — термы, не свободные соответственно для x и y в $\mathscr{E}(x, y)$, то $t = s$ служит сокращенным обозначением не для $\mathscr{E}(t, s)$, а для некоторой формулы $\mathscr{E}^*(t, s)$, которая получена из $\mathscr{E}(t, s)$ подходящим переименованием связанных переменных (см. следствие 2.22) таким образом, чтобы t и s оказались свободными соответственно для x и y в $\mathscr{E}^*(x, y)$. Для таких теорий K могут быть доказаны предложения, аналогичные предложениям 2.25 и 2.26, в предположении, что (7) является теоремой в K для соответствующих типов формул $\mathscr{E}^*(x, y)$. (Предоставляется читателю в качестве упражнения.)

В теориях первого порядка с равенством для выражений вида «существует один и только один предмет x такой, что ...» можно использовать следующее

Определение. $\exists_1 x \mathscr{A}(x)$ означает $\exists x \mathscr{A}(x) \,\&\, \forall x \forall y (\mathscr{A}(x) \,\&\, \mathscr{A}(y) \supset x = y)$.

Упражнения

1. $\vdash \forall x \exists_1 y\,(x = y)$.
2. $\vdash \exists_1 x \mathscr{A}(x) \equiv \exists x \forall y\,(x = y \equiv \mathscr{A}(y))$.
3. $\vdash \forall x\,(\mathscr{A}(x) \equiv \mathscr{B}(x)) \supset [\exists_1 x \mathscr{A}(x) \equiv \exists_1 x \mathscr{B}(x)]$.

Для всякой модели теории первого порядка K с равенством отношение E, соответствующее в этой модели предикатной букве $=$, является отношением эквивалентности (в силу предложения 2.24). Если в области некоторой модели это отношение E оказывается отношением тождества, то эта модель называется *нормальной*.

Всякая модель M теории K может быть *сужена* до некоторой нормальной модели M′ теории K. Для этого в качестве области D′ новой модели M′ возьмем множество классов эквивалентности, определяемых отношением E в области D модели M. Затем для каждой предикатной буквы A_j^n с интерпретацией $(A_j^n)^*$ в M определим новую интерпретацию $(A_j^n)'$ в M′ условием: для любых классов эквивалентности $[b_1], \ldots, [b_n]$, определяемых элементами $b_1, \ldots, b_n$ из D, $(A_j^n)'$ выполнено тогда и только тогда, когда в M для $b_1, \ldots, b_n$ выполнено $(A_j^n)^*$. Это определение не зависит от выбора представителей $b_1, \ldots, b_n$ соответствующих классов эквивалентности, так как, на основании (7), $\vdash x_1 = y_1 \& \ldots \& x_n = y_n \supset \supset (A_j^n(x_1, \ldots, x_n) \supset A_j^n(y_1, \ldots, y_n))$. Аналогично, новую интерпретацию $(f_j^n)'$ в M′ для функциональной буквы f_j^n с интерпретацией $(f_j^n)^*$ в M зададим условием: $(f_j^n)'([b_1], \ldots, [b_n]) = [(f_j^n)^*(b_1, \ldots, b_n)]$. Нетрудно видеть, что и это определение не зависит от выбора представителей классов эквивалентности, так как, на основании (7), $\vdash x_1 = y_1 \& \ldots \& x_n = y_n \supset \supset f_j^n(x_1, \ldots, x_n) = f_j^n(y_1, \ldots, y_n)$. Наконец, всякая предметная константа a_i с интерпретацией c в M будет теперь интерпретироваться в M′ классом $[c]$. Отношение E′, соответствующее в M′ предикатной букве $=$, является отношением тождества в D′: $E'([b_1], [b_2])$ имеет место тогда и только тогда, когда выполнено $E(b_1, b_2)$, т. е. когда $[b_1] = [b_2]$. Следующая лемма легко может быть теперь доказана по индукции: если $s = (b_1, b_2, \ldots)$ — счетная последовательность элементов из D, $[b_i]$ — класс эквивалентности, порождаемый элементом b_i, и $s' = ([b_1], [b_2], \ldots)$, то формула $\mathscr{A}$ выполнена в M на s тогда и только тогда, когда $\mathscr{A}$ выполнена в M′ на s′. Отсюда следует, что всякая формула $\mathscr{A}$ истинна в M тогда и только тогда, когда она истинна в M′, а так как M есть модель K, то, следовательно, M′ есть нормальная модель теории K.

Предложение 2.27. (Продолжение предложения 2.12; Гёдель [1930].) *Всякая непротиворечивая теория первого порядка* K *с равенством имеет конечную или счетную нормальную модель.*

Доказательство. Согласно предложению 2.12, K имеет счетную модель M. Следовательно, сужение модели M описанным только что выше способом приводит к нормальной конечной или счетной модели M′, так как множество классов эквивалентности, на которые разбивается D, имеет мощность не бо́льшую, чем само D.

Следствие 2.28. (Продолжение теоремы Сколема — Лёвенгейма.) *Всякая теория первого порядка* K *с равенством, имеющая бесконечную нормальную модель* M, *имеет счетную нормальную модель.*

Доказательство. Добавим к K новые предметные константы $b_1, b_2, \ldots$ вместе с аксиомами $b_i \neq b_j$ для $i \neq j$. Новая теория K′ непротиворечива. Если бы теория K′ была противоречива, то существовал бы вывод в K′ некоторого противоречия $\mathscr{C} \& \neg \mathscr{C}$, причем можно считать, что $\mathscr{C}$ есть формула теории K. Такой вывод использовал бы, очевидно, лишь конечное число новых аксиом: $b_{i_1} \neq b_{j_1}, \ldots, b_{i_n} \neq b_{j_n}$, и модель M могла бы быть расширена до некоторой модели теории, получающейся из K добавлением аксиом $b_{i_1} \neq b_{j_1}, \ldots, b_{i_n} \neq b_{j_n}$. В самом деле, так как M есть бесконечная нормальная модель, то мы можем так выбрать интерпретации предметных постоянных $b_{i_1}, b_{j_1}, \ldots, b_{i_n}, b_{j_n}$, чтобы формулы $b_{i_1} \neq b_{j_1}, \ldots, b_{i_n} \neq b_{j_n}$ были истинны в M. Поэтоту выводимость $\mathscr{C} \& \neg \mathscr{C}$ из этих формул и аксиом K повлекла бы за собой истинность $\mathscr{C} \& \neg \mathscr{C}$ в M, что невозможно ввиду (II) на стр. 59. Итак, теория K′ должна быть непротиворечивой. В силу предложения 2.27, K′ имеет конечную или счетную нормальную модель N. Формулы $b_i \neq b_j$ для $i \neq j$ истинны в N, как аксиомы теории K′. Следовательно, элементы области модели N, интерпретирующие соответственно $b_1, b_2, \ldots$, должны быть попарно различны, откуда следует, что область N бесконечна и, следовательно, счетна.

Упражнения

1. Определим $\exists_n x_{\mathscr{A}}(x)$ для $n \geqslant 1$ индукцией по n. Для случая $n = 1$ используем определение $\exists_1 x_{\mathscr{A}}(x)$ на стр. 90. Пусть теперь для произвольного n $\exists_{n+1} x_{\mathscr{A}}(x)$ обозначает $\exists y\,(\mathscr{A}(y) \& \exists_n x\,(x \neq y \& \mathscr{A}(x)))$. Показать, что $\exists_n x_{\mathscr{A}}(x)$ выражает собой утверждение существования в точности n объектов, для которых $\mathscr{A}$ выполнено, в том смысле, что во всякой нормальной модели формулы $\exists_n x_{\mathscr{A}}(x)$ имеется в точности n объектов, которые обладают свойством, интерпретирующим $\mathscr{A}(x)$.

2. Если теория первого порядка K с равенством имеет конечные нормальные модели со сколь угодно большим числом элементов, то она имеет и счетную модель. (Указание. Доказательство аналогично доказательству следствия 2.28.)

3. Всякое исчисление предикатов с равенством непротиворечиво. (Указание. Пусть $\mathscr{A}$ — произвольная формула; опустить в ней все знаки кванторов, заменить всякую элементарную формулу $t = s$ на $\mathscr{B} \vee \neg \mathscr{B}$ с некоторой фиксированной формулой $\mathscr{B}$, стереть все термы и все связанные с ними скобки. Показать, что если $\mathscr{A}$ — теорема, то описанная процедура над $\mathscr{A}$ приводит к частному случаю тавтологии. Однако при этом формула $x_1 \neq x_1$ преобразуется в $\neg(\mathscr{B} \vee \neg \mathscr{B})$.)

4. Доказать независимость аксиом (1) — (7) во всяком исчислении предикатов с равенством. (Указание. Для доказательства независимости аксиом (1) — (3) заменить все формулы $t = s$ пропозициональной формой $A \supset A$, затем стереть все кванторы, термы и связанные с ними запятые и скобки; аксиомы (4) — (6) переходят при этом в пропозициональные формы вида $P \supset P$, а аксиома (7) — в $(P \supset P) \supset (Q \supset Q)$. После этого для аксиом (2), (3) использовать то же доказательство, что и для независимости аксиом (A2) — (A3) пропозиционального исчисления (стр. 47). Что касается аксиомы (1), то трехзначная

истинностная таблица, использованная на стр. 46 для доказательства независимости аксиомы (A1), не дает значения 0 для $P \supset P$; предлагается взамен этого воспользоваться следующими четырехзначными истинностными таблицами:

A	$\neg A$
0	1
1	0
2	3
3	2

A	B	$A \supset B$
0	0	0
1	0	0
2	0	0
3	0	0
0	1	1
1	1	0
2	1	1
3	1	1

A	B	$A \supset P$
0	2	1
1	2	0
2	2	0
3	2	0
0	3	1
1	3	0
2	3	1
3	3	0

Для доказательства независимости аксиомы (4) заменить все кванторы всеобщности $\forall x$ кванторами существования $\exists x$. Вопрос с аксиомой (5) решается заменой всех термов t на x_1, а всех кванторов всеобщности на $\forall x_1$. Для аксиомы (6) воспользоваться заменой всех формул вида $t = s$ отрицанием какой-нибудь фиксированной теоремы. Наконец, заменив все формулы вида $t = s$ какой-нибудь фиксированной теоремой, можно получить доказательство независимости аксиомы (7).) Во всяком исчислении предикатов с равенством формулы (6) и (7) предполагаются аксиомами.

5. Для правил вывода MP и Gen доказать их независимость в том смысле, что если мы опустим любое из них в определении исчисления предикатов с равенством, то его нельзя уже будет потом получить в качестве производного правила. (Указание. Для доказательства независимости MP достаточно заметить, что применение Gen увеличивает число кванторов, не меняя числа связок; замена всякой формулы $\forall x \mathscr{A}$ на $\forall x \neg (\mathscr{A} \supset \mathscr{A})$ поможет доказать независимость Gen.)

6. Назовем формулу $\mathscr{A}$ k-общезначимой, если она истинна во всех интерпретациях с k элементами. Назовем $\mathscr{A}$ в точности k-общезначимой, если она k-общезначима, но не является $k+1$-общезначимой. Заметим, что $k+1$-общезначимость влечет k-общезначимость. Построить пример в точности k-общезначимой формулы. (Подробнее об этом см. Гильберт — Бернайс [1934, §§ 4 — 5]; Вайсберг [1933].)

§ 9. Введение новых функциональных букв и предметных констант

В математике часто после того, как удается доказать, что для любых $y_1, \ldots, y_n$ существует и притом единственный объект u, обладающий свойством $\mathscr{A}(u, y_1, \ldots, y_n)$, вводят новую функцию $f(y_1, \ldots, y_n)$ такую, что $\mathscr{A}(f(y_1, \ldots, y_n), y_1, \ldots, y_n)$ выполнено при любых $y_1, \ldots, y_n$. Аналогично, если доказано существование единственного объекта u, удовлетворяющего условию $\mathscr{A}(u)$, где $\mathscr{A}(u)$ имеет u своей единственной свободной переменной, то вводят новую предметную константу b. Общеизвестно, что такие определения хотя и удобны, но ничего действительно нового к теории не добавляют. Этот факт может быть точно выражен в следующей форме.

Предложение 2.29. *Пусть* K — *теория первого порядка с равенством. Предположим, что* $\vdash_K \exists_1 u \mathscr{A}(u, y_1, \ldots, y_n)$. *Пусть* K′ — *теория первого порядка с равенством, полученная добавлением к* K

новой n-местной функциональной буквы f, собственной аксиомы $\mathscr{A}(f(y_1, \ldots, y_n), y_1, \ldots, y_n)$ и всех содержащих f частных случаев аксиом (1)—(7). Тогда существует эффективное отображение, преобразующее всякую формулу $\mathscr{B}$ теории K′ в некоторую формулу $\mathscr{B}'$ теории K таким образом, что

(1) *если f не входит в $\mathscr{B}$, то $\mathscr{B}'$ совпадает с $\mathscr{B}$,*
(2) *$(\neg\mathscr{B})'$ совпадает с $\neg(\mathscr{B}')$,*
(3) *$(\mathscr{B}\supset\mathscr{C})'$ совпадает с $\mathscr{B}'\supset\mathscr{C}'$,*
(4) *$(\forall x\mathscr{B})'$ совпадает с $\forall x(\mathscr{B})'$,*
(5) *$\vdash_{K'}\mathscr{B}\equiv\mathscr{B}'$,*
(6) *если $\vdash_{K'}\mathscr{B}$, то $\vdash_K\mathscr{B}'$.*

Следовательно, если $\mathscr{B}$ не содержит f и $\vdash_{K'}\mathscr{B}$, то $\vdash_K\mathscr{B}$.

Доказательство. Назовем простым f-термом всякий терм $f(t_1, \ldots, t_n)$, где термы $t_1, \ldots, t_n$ не содержит f. Пусть дана элементарная формула $\mathscr{B}$ теории K′, и пусть $\mathscr{B}^*$ обозначает результат замещения самого левого вхождения какого-либо простого f-терма $f(t_1, \ldots, t_n)$ в $\mathscr{B}$ первой переменной u, не встречающейся в $\mathscr{B}$. Назовем формулу $\exists u(\mathscr{A}(u, t_1, \ldots, t_n)\&\mathscr{B}^*)$ f-образом $\mathscr{B}$. Если формула $\mathscr{B}$ не содержит f, то пусть она сама будет своим f-образом. Очевидно, что $\vdash_{K'}\exists u(\mathscr{A}(u, t_1, \ldots, t_n)\&\mathscr{B}^*)\equiv\mathscr{B}$. (Здесь следует принять во внимание условие $\vdash_K\exists_1 u\mathscr{A}(u, y_1, \ldots, y_n)$ и аксиому $\mathscr{A}(f(y_1, \ldots, y_n), y_1, \ldots, y_n)$ теории K′.) Число вхождений функциональной буквы f в $\mathscr{B}^*$ на единицу меньше, чем в $\mathscr{B}$, и $\vdash_{K'}\exists u(\mathscr{A}(u, t_1, \ldots, t_n)\&\mathscr{B}^*)\equiv\mathscr{B}$, поэтому, строя последовательные f-образы, мы в конце концов получим формулу $\mathscr{B}'$, которая не содержит f, и такую, что $\vdash_{K'}\mathscr{B}'\equiv\mathscr{B}$. Назовем $\mathscr{B}'$ f-свободным образом $\mathscr{B}$. Распространим теперь операцию $'$ на все формулы теории K′, определив $(\neg\mathscr{B})'$ как $\neg(\mathscr{B}')$, $(\mathscr{B}\supset\mathscr{C})'$ как $\mathscr{B}'\supset\mathscr{C}'$ и $(\forall x\mathscr{B})'$ как $\forall x(\mathscr{B})'$. Легко видеть, что утверждения (1)—(5) выполнены. Чтобы доказать (6), достаточно, используя (1) и (5), показать, что если $\mathscr{B}$ не содержит f и $\vdash_{K'}\mathscr{B}$, то $\vdash_K\mathscr{B}$. При этом мы можем считать, что формула $\mathscr{B}$ замкнута, так как всякая формула выводима из своего замыкания и обратно.

Пусть M — произвольная модель теории K и M_1 — соответствующая ей нормальная модель той же теории (см. стр. 91). Как мы знаем, всякая формула истинна в M тогда и только тогда, когда она истинна в M_1. Так как $\vdash_K\exists_1 u\mathscr{A}(u, y_1, \ldots, y_n)$, то для любых $b_1, \ldots, b_n$ из области модели M_1 существует единственный элемент c в этой области, для которого $\mathscr{A}(c, b_1, \ldots, b_n)$ истинно в M_1. Исходя из модели M_1, мы получим теперь модель M′ теории K′, если возьмем в качестве интерпретации функциональной буквы f функцию f′, определенную условием $f'(b_1, \ldots, b_n) = c$. В самом деле, логические аксиомы (включая аксиомы равенства для K′) истинны в любой интерпретации, а аксиома $A(f(y_1, \ldots, y_n), y_1, \ldots, y_n)$ верна в M′ в силу определения функции f′. Так как собственные аксиомы теории K не содержат f и

истинны в M_1, то они истинны и в M′. Пусть теперь $\vdash_{K'} \mathscr{B}$ и $\mathscr{B}$ не содержит f. Тогда формула $\mathscr{B}$ истинна в M′, а следовательно (так как она не содержит f), она истинна в M_1 и в M. Итак, формула $\mathscr{B}$ истинна в любой модели теории K. Отсюда, в силу следствия 2.15 (а) теоремы о полноте, следует $\vdash_K \mathscr{B}$. (В случае, когда $\vdash_K \exists_1 u \mathscr{A}(u)$ и $\mathscr{A}(u)$ не содержит отличных от u свободных переменных, теория K′ строится добавлением новой предметной константы b и аксиомы $\mathscr{A}(b)$. После этого соответствующий аналог предложения 2.29 доказывается практически теми же рассуждениями, которые были только что приведены.)

Упражнение

Найти f-свободные образы формул

$$\forall x \exists y (A_1^3(x, y, f(x, y, \ldots, y)) \supset f(y, x, \ldots, x) = x)$$

и

$$A_1^1(f(y_1, \ldots, y_{n-1}, f(y_1, \ldots, y_n))) \vee \exists x A_1^2(x, f(y_1, \ldots, y_n)).$$

Отметим, что предложение 2.29 применимо и в том случае, когда вводится несколько различных новых символов, например $f_1, \ldots, f_n$. Мы можем тогда считать, что каждый символ f_i добавляется к теории, уже полученной в результате добавления символов $f_1, \ldots, f_{i-1}$. Таким образом, здесь необходимо n-кратное применение предложения 2.29. Формулу $\mathscr{B}'$ теории K в предложении 2.29 можно рассматривать как свободный от f перевод формулы $\mathscr{B}$ в язык теории K.

Примеры. 1. В элементарной теории групп G (см. стр. 89) выводимо $\exists_1 x_2 (x_1 + x_2 = 0)$. Введем новую функциональную букву f с одним аргументом и, обозначив $f(t)$ через $-t$, добавим новую аксиому $x_1 + (-x_1) = 0$. Согласно предложению 2.29, после всех этих нововведений мы не сможем, однако, вывести никакую формулу теории G, которая не была бы выводима ранее. Таким образом, введение $(-t)$ по существу ничем не усиливает первоначальную теорию.

2. В элементарной теории полей F (см. стр. 90) выводима формула $\exists_1 x_2 ((x_1 \neq 0 \,\&\, x_1 \cdot x_2 = 1) \vee (x_1 = 0 \,\&\, x_2 = 0))$. Введем новую одноместную функциональную букву g и, приняв сокращение t^{-1} для $g(t)$, новую аксиому $(x_1 \neq 0 \,\&\, x_1 \cdot x_1^{-1} = 1) \vee (x_1 = 0 \,\&\, x_1^{-1} = 0)$. Из этой аксиомы можно вывести $x_1 \neq 0 \supset x_1 \cdot x_1^{-1} = 1$.

Предложение 2.29 показывает, что в теориях первого порядка существенно необходимыми являются лишь предикатные буквы, без функциональных же букв и предметных констант можно обойтись. Так функциональную букву f_i^n можно заменить новой предикатной буквой A_k^{n+1} вместе с новой аксиомой $\exists_1 u A_k^{n+1}(y_1, \ldots, y_n, u)$. Предметная константа заменяется новой предикатной буквой A_k^1 с аксиомой $\exists_1 u A_k^1(u)$.

Пример. В элементарной теории групп G мы можем заменить функциональный знак $+$ и предметную константу 0 предикатами A_1^3 и A_1^1 с дополнительными аксиомами $\forall x_1 \forall x_2 \exists x_3 A_1^3(x_1, x_2, x_3)$ и $\exists_1 x_1 A_1^1(x_1)$.

При этом, разумеется, необходимо прежние аксиомы (a), (b), (c), (g) заменить соответственно следующими аксиомами:

(a′) $A_1^3(x_2, x_3, y_1) \& A_1^3(x_1, y_1, y_2) \& A_1^3(x_1, x_2, y_3) \& A_1^3(y_3, x_3, y_4) \supset \supset y_2 = y_4$;

(b′) $A_1^1(y_1) \& A_1^3(x_1, y_1, y_2) \supset y_2 = x_1$;

(c′) $\exists x_2 \forall y_1 \forall y_2 (A_1^1(y_1) \& A_1^3(x_1, x_2, y_2) \supset y_2 = y_1)$;

(g′) $[x_1 = x_2 \& A_1^3(x_1, x_3, y_1) \& A_1^3(x_2, x_3, y_2) \& A_1^3(x_3, x_1, y_3) \& \& A_1^3(x_3, x_2, y_4)] \supset y_1 = y_2 \& y_3 = y_4$.

Следует заметить, что приведенное доказательство предложения 2.29 не конструктивно, так как оно использует семантические понятия (модель, истинность) и, кроме того, опирается на неконструктивно доказанное следствие 2.15(a). Известны, однако, и конструктивные, синтаксические доказательства предложения 2.29 (см. Клини [1952], § 74), но они, как правило, весьма сложны.

В обычном языке, а также в математике весьма часто употребляются описательные выражения типа «объект u такой, что $\mathscr{A}(u, y_1, \ldots, y_n)$». Такие выражения называются точными описаниями. Пусть $\iota u \mathscr{A}(u, y_1, \ldots \ldots, y_n)$ обозначает единственный предмет u такой, что $\mathscr{A}(u, y_1, \ldots \ldots, y_n)$, если такой единственный предмет существует, если же такого единственного предмета не существует, то договоримся считать выражение $\iota u \mathscr{A}(u, y_1, \ldots, y_n)$ лишенным смысла, или подразумевать под ним какой-нибудь фиксированный объект, скажем 0. (Так, например, мы можем сказать, что фразы «нынешний король Франции» или «наименьшее целое число» лишены смысла, или произвольно договориться считать их обозначениями для 0.) Существуют различные способы введения этих ι-термов в формализованные теории, но так как в большинстве случаев достигаемые при этом результаты могут быть получены введением новых функциональных букв, как это было сделано выше и так как все эти способы приводят к теоремам, подобным предложению 2.29, то мы не будем здесь на этом останавливаться. По этому вопросу мы отсылаем читателя к Гильберту и Бернайсу [1934] и к Россеру [1939a], [1953].

§ 10. Предваренные нормальные формы

Формула $Q_1 y_1 \ldots Q_n y_n \mathscr{A}$, где $Q_i y_i$ — квантор всеобщности или существования, y_i и y_j различны для $i \neq j$ и $\mathscr{A}$ не содержит кванторов, называется формулой *в предваренной нормальной форме*. (Сюда включается и случай $n = 0$, когда вообще нет никаких кванторов.) Мы докажем, что для любой формулы можно построить эквивалентную ей формулу в предваренной нормальной форме.

Лемма 2.30. *Во всякой теории первого порядка*

(I) $\vdash (\forall x \mathscr{C}(x) \supset \mathscr{D}) \equiv \exists y (\mathscr{C}(y) \supset \mathscr{D})$, *если* y *не входит свободно ни в* $\mathscr{C}(x)$, *ни в* $\mathscr{D}$;

(II) $\vdash \exists x \mathscr{C}(x) \supset \mathscr{D} \equiv \forall y (\mathscr{C}(y) \supset \mathscr{D})$, *если* y *не входит свободно ни в* $\mathscr{C}(x)$, *ни в* $\mathscr{D}$;
(III) $\vdash \mathscr{D} \supset \forall x \mathscr{C}(x) \equiv \forall y (\mathscr{D} \supset \mathscr{C}(y))$, *если* y *не входит свободно ни в* $\mathscr{C}(x)$, *ни в* $\mathscr{D}$;
(IV) $\vdash \mathscr{D} \supset \exists x \mathscr{C}(x) \equiv \exists y (\mathscr{D} \supset \mathscr{C}(y))$, *если* y *не входит свободно ни в* $\mathscr{C}(x)$, *ни в* $\mathscr{D}$;
(V) $\vdash \neg \forall x \mathscr{C} \equiv \exists x \neg \mathscr{C}$;
(VI) $\vdash \neg \exists x \mathscr{C} \equiv \forall x \neg \mathscr{C}$.

Доказательство I(A).

1. $\forall x \mathscr{C}(x) \supset \mathscr{D}$	гипотеза
2. $\neg \exists y (\mathscr{C}(y) \supset \mathscr{D})$	гипотеза
3. $\neg\neg \forall y \neg (\mathscr{C}(y) \supset \mathscr{D})$	2, определение квантора существования
4. $\forall y (\mathscr{C}(y) \& \neg \mathscr{D})$	3, тавтологии $\neg\neg A \supset A$, $\neg(A \supset B) \equiv (A \& \neg B)$, следствие 2.21
5. $\mathscr{C}(y) \& \neg \mathscr{D}$	4, правило A4
6. $\mathscr{C}(y)$	5, тавтология $(A \& B) \supset A$
7. $\forall y \mathscr{C}(y)$	6, Gen
8. $\forall x \mathscr{C}(x)$	7, лемма 2.8
9. $\mathscr{D}$	1, 8, MP
10. $\neg \mathscr{D}$	5, тавтология *)
11. $\mathscr{D} \& \neg \mathscr{D}$	9, 10, тавтология
12. $\forall x \mathscr{C}(x) \supset \mathscr{D}, \neg \exists y (\mathscr{C}(y) \supset \mathscr{D}) \vdash \mathscr{D} \& \neg \mathscr{D}$	1 — 11
13. $\forall x \mathscr{C}(x) \supset \mathscr{D} \vdash \neg \exists y (\mathscr{C}(y) \supset \mathscr{D}) \supset \mathscr{D} \& \neg \mathscr{D}$	12, предложение 2.4
14. $\forall x \mathscr{C}(x) \supset \mathscr{D} \vdash \exists y (\mathscr{C}(y) \supset \mathscr{D})$	13, тавтология
15. $\vdash (\forall x \mathscr{C}(x) \supset \mathscr{D}) \supset \exists y (\mathscr{C}(y) \supset \mathscr{D})$	14, предложение 2.4

Доказательство I(B).

1. $\exists y (\mathscr{C}(y) \supset \mathscr{D})$	гипотеза
2. $\forall x \mathscr{C}(x)$	гипотеза
3. $\mathscr{C}(b) \supset \mathscr{D}$	1, правило C
4. $\mathscr{C}(b)$	2, правило A4
5. $\mathscr{D}$	3, 4, MP

*) Применения очевидных тавтологий будут теперь отмечаться одним лишь словом «тавтология».

6 $\exists y(\mathscr{C}(y) \supset \mathscr{D}),\ \forall x\mathscr{C}(x) \vdash_C \mathscr{D}$ — 1 — 5

7. $\exists y(\mathscr{C}(y) \supset \mathscr{D}),\ \forall x\mathscr{C}(x) \vdash \mathscr{D}$ — 6, предложение 2.23

8. $\vdash \exists y(\mathscr{C}(y) \supset \mathscr{D}) \supset (\forall x\mathscr{C}(x) \supset \mathscr{D})$ — 7, предложение 2.4 дважды

Доказательство I (C).

$\vdash (\forall x\mathscr{C}(x) \supset \mathscr{D}) \equiv \exists y(\mathscr{C}(y) \supset \mathscr{D})$ — (A), (B), тавтология

Остающиеся части (II) — (VI) доказываются легко, читателю предлагается сделать это самому в качестве упражнения. Здесь можно только заметить, что (VI) тривиально, а (V) содержится в упражнении 1 на стр. 83. (III) и (IV) легко следуют соответственно из (II) и (I).

Лемма 2.30 позволяет в каждой формуле постепенно передвигать все кванторы влево. Собственно этот процесс и является существенной частью доказательства следующей теоремы.

Предложение 2.31. *Существует эффективная процедура, преобразующая всякую формулу $\mathscr{A}$ к такой формуле $\mathscr{B}$ в предваренной нормальной форме, что* $\vdash \mathscr{A} \equiv \mathscr{B}$ *).

Доказательство. Построение формулы $\mathscr{B}$ будет описано, следуя индукции по числу k всех связок и кванторов в формуле $\mathscr{A}$. (В силу предложения 2.18 (a) — (b), мы можем считать, что связанные переменные в кванторной приставке, которую мы хотим получить, попарно различны.) При $k = 0$ $\mathscr{B}$ совпадает с $\mathscr{A}$. Допустим, что мы умеем строить соответствующие формулы $\mathscr{B}$ при любом $k < n$. Пусть формула $\mathscr{A}$ имеет n связок и кванторов.

Случай 1. Если $\mathscr{A}$ есть $\neg\mathscr{C}$, то, согласно индуктивному предположению, мы умеем построить формулу $\mathscr{D}$ в предваренной нормальной форме такую, что $\vdash \mathscr{D} \equiv \mathscr{C}$. Отсюда $\vdash \neg\mathscr{C} \equiv \neg\mathscr{D}$, т. е. $\vdash \mathscr{A} \equiv \neg\mathscr{D}$. Применяя теперь (V) и (VI) из леммы 2.30 и следствие 2.21, мы легко построим формулу $\mathscr{B}$ в предваренной нормальной форме такую, что $\vdash \neg\mathscr{D} \equiv \mathscr{B}$, откуда получаем $\vdash \mathscr{A} \equiv \mathscr{B}$.

Случай 2. Если $\mathscr{A}$ есть $\mathscr{C} \supset \mathscr{E}$, то, по индуктивному предположению, мы можем построить формулы $\mathscr{C}_1$ и $\mathscr{E}_1$ в предваренной нормальной форме такие, что $\vdash \mathscr{C} \equiv \mathscr{C}_1$ и $\vdash \mathscr{E} \equiv \mathscr{E}_1$. Принимая во внимание соответствующую тавтологию, мы тогда получим $\vdash (\mathscr{C} \supset \mathscr{E}) \equiv (\mathscr{C}_1 \supset \mathscr{E}_1)$, т. е. $\vdash \mathscr{A} \equiv (\mathscr{C}_1 \supset \mathscr{E}_1)$. Применяя теперь (I) — (IV) из леммы 2.30 и следствие 2.21, мы можем вынести кванторные приставки в $\mathscr{C}_1$ и $\mathscr{E}_1$ за внешние скобки в $(\mathscr{C}_1 \supset \mathscr{E}_1)$, в результате чего и получим такую формулу $\mathscr{B}$ в предваренной нормальной форме, что $\vdash \mathscr{A} \equiv \mathscr{B}$.

Случай 3. $\mathscr{A}$ есть $\forall x\mathscr{C}$. По индуктивному предположению, мы умеем строить такую формулу $\mathscr{C}_1$ в предваренной нормальной форме, что $\vdash \mathscr{C} \equiv \mathscr{C}_1$. Следовательно, $\vdash \forall x\mathscr{C} \equiv \forall x\mathscr{C}_1$, т. е. $\vdash \mathscr{A} \equiv \forall x\mathscr{C}_1$. Но формула $\forall x\mathscr{C}_1$ является, очевидно, формулой в предваренной

*) Такую формулу $\mathscr{B}$ автор в дальнейшем называет иногда предваренной нормальной формой формулы $\mathscr{A}$. (*Прим. перев.*)

нормальной форме.

Примеры. 1. Пусть $\mathscr{A}$ есть формула

$$\forall x (A_1^1(x) \supset \forall y (A_2^2(x, y) \supset \neg \forall z A_3^2(y, z))).$$

Приведем ее к предваренной нормальной форме. В силу пункта (V) леммы 2.30 получаем

$$\forall x (A_1^1(x) \supset \forall y (A_2^2(x, y) \supset \exists z \neg A_3^2(y, z))).$$

В силу пункта (IV) той же леммы получаем

$$\forall x (A_1^1(x) \supset \forall y \exists u (A_2^2(x, y) \supset \neg A_3^2(y, u))).$$

В силу (III) получаем

$$\forall x \forall v (A_1^1(x) \supset \exists u (A_2^2(x, v) \supset \neg A_3^2(v, u))).$$

В силу (IV) получаем

$$\forall x \forall v \exists w (A_1^1(x) \supset (A_2^2(x, v) \supset \neg A_3^2(v, w))).$$

Наконец, произведя переименование связанных переменных (следствие 2.22), получаем

$$\forall x \forall y \exists z (A_1^1(x) \supset (A_2^2(x, y) \supset \neg A_3^2(y, z))).$$

2. Пусть $\mathscr{A}$ есть

$$A_1^2(x, y) \supset \exists y [A_1^1(y) \supset ((\exists x A_1^1(x)) \supset A_2^1(y))].$$

В силу пункта (II) леммы 2.30 получаем

$$A_1^2(x, y) \supset \exists y [A_1^1(y) \supset \forall u (A_1^1(u) \supset A_2^1(y))].$$

В силу (III) получаем

$$A_1^2(x, y) \supset \exists y \forall v (A_1^1(y) \supset (A_1^1(v) \supset A_2^1(y))).$$

В силу (IV) получаем

$$\exists w (A_1^2(x, y) \supset \forall v (A_1^1(w) \supset (A_1^1(v) \supset A_2^1(w)))).$$

В силу (III) получаем

$$\exists w \forall z (A_1^2(x, y) \supset (A_1^1(w) \supset (A_1^1(z) \supset A_2^1(w)))).$$

Упражнение

Построить предваренные нормальные формы, эквивалентные следующим формулам:

1. $\forall x (A_1^1(x) \supset A_1^2(x, y))] \supset ([\exists y A_1^1(y)] \supset [\exists z A_1^2(y, z)])$.
2. $\exists x A_1^2(x, y) \supset (A_1^1(x) \supset \neg \exists u A_1^2(x, u))$.

Исчисление предикатов первого порядка, в котором нет функциональных букв и предметных констант и в котором для каждого целого положительного n имеется бесконечно много n-местных предикатных букв, называется *чистым исчислением предикатов первого порядка*. Для чистого исчисления предикатов первого порядка может быть

доказана следующая теорема о предваренной нормальной форме некоторого весьма простого вида Назовем формулу в предваренной нормальной форме формулой *в нормальной форме Сколема*, если в ней все кванторы существования предшествуют всем кванторам всеобщности.

Предложение 2.32. *По всякой формуле $\mathscr{A}$ чистого исчисления предикатов первого порядка можно эффективно построить такую формулу $\mathscr{B}$ в нормальной форме Сколема, что $\vdash \mathscr{A}$ тогда и только тогда, когда $\vdash \mathscr{B}$ (или, что эквивалентно, в силу теоремы Гёделя о полноте* 2.14, *$\mathscr{A}$ логически общезначима тогда и только тогда, когда логически общезначима $\mathscr{B}$).*

Доказательство. Прежде всего, мы можем считать, что формула $\mathscr{A}$ замкнута, ибо всякая формула выводима одновременно со своим замыканием. Более того, в силу предложения 2.31, мы можем предполагать, что $\mathscr{A}$ уже есть формула в предваренной нормальной форме. Назовем *рангом* формулы $\mathscr{A}$ число r, показывающее, сколько кванторов всеобщности предшествует в $\mathscr{A}$ хотя бы одному квантору существования. Процесс построения нормальной формы Сколема для формулы $\mathscr{A}$ будет теперь описан с помощью индукции по r. При $r = 0$ утверждение доказываемого предложения очевидно, так как тогда формула $\mathscr{A}$ уже является формулой в нормальной форме Сколема. Допустим, что мы уже умеем строить искомую формулу в нормальной форме Сколема всякий раз, когда ранг исходной формулы меньше r, и пусть ранг $\mathscr{A}$ равен r. Формула $\mathscr{A}$ может быть записана в виде $\exists y_1 \ldots \exists y_n \forall u \mathscr{B}(y_1, \ldots, y_n, u)$, где единственными свободными переменными в $\mathscr{B}(y_1, \ldots, y_n, u)$ являются $y_1, \ldots, y_n, u$. Пусть A_j^{n+1} — первая $n+1$-местная предикатная буква, не встречающаяся в $\mathscr{A}$. Рассмотрим формулу

$$(\mathscr{A}_1) \qquad \exists y_1 \ldots \exists y_n ([\forall u (\mathscr{B}(y_1, \ldots, y_n, u) \supset A_j^{n+1}(y_1, \ldots, y_n, u))] \supset \supset \forall u A_j^{n+1}(y_1, \ldots, y_n, u)).$$

Покажем, что $\vdash \mathscr{A}$ тогда и только тогда, когда $\vdash \mathscr{A}_1$. Пусть $\vdash \mathscr{A}_1$. Рассмотрим какой-нибудь вывод $\mathscr{A}_1$. Заменим в этом выводе каждое вхождение формулы $A_j^{n+1}(z_1, \ldots, z_n, w)$ формулой $\mathscr{B}^*(z_1, \ldots, z_n, w)$, где $\mathscr{B}^*$ получается из $\mathscr{B}$ заменой в $\mathscr{B}$ всех связанных переменных, имеющих свободные вхождения где-нибудь в этом выводе, на переменные, в нем не встречающиеся. При этом, очевидно, мы получим вывод формулы

$$\exists y_1 \ldots \exists y_n ((\forall u (\mathscr{B}(y_1, \ldots, y_n, u) \supset \mathscr{B}^*(y_1, \ldots, y_n, u))) \supset \supset \forall u \mathscr{B}^*(y_1, \ldots, y_n, u)).$$

($\mathscr{B}$ заменяется на $\mathscr{B}^*$ таким образом, что применения аксиомы (4) остаются применениями той же аксиомы.) Произведя теперь обратную замену переменных, мы, на основании следствия 2.22, заключаем, что

$$\dashv \exists y_1 \ldots \exists y_n [\forall u (\mathscr{C}(y_1, \ldots, y_n, u) \supset \mathscr{B}(y_1, \ldots, y_n, u)) \supset \supset \forall u \mathscr{B}(y_1, \ldots, y_n, u)].$$

Так как $\vdash \forall u(\mathscr{B}(y_1, \ldots, y_n, u) \supset \mathscr{B}(y_1, \ldots, y_n, u))$, то, в силу следствия 2.21, $\vdash \exists y_1 \ldots \exists y_n \forall u \mathscr{B}(y_1, \ldots, y_n, u)$, т. е. $\vdash \mathscr{A}$. Обратно, пусть $\vdash \mathscr{A}$. По правилу С, получаем $\forall u \mathscr{B}(b_1, \ldots, b_n, u)$. Но для любых формул $\mathscr{D}$ и $\mathscr{F}$ $\vdash \forall u \mathscr{D} \supset (\forall u(\mathscr{D} \supset \mathscr{F}) \supset \forall u \mathscr{F})$ (см. упражнение 1, стр. 71). Поэтому $\forall u(\mathscr{B}(b_1, \ldots, b_n, u) \supset A_j^{n+1}(b_1, \ldots, b_n, u)) \supset \forall u A_j^{n+1}(b_1, \ldots, b_n, u)$. Теперь по правилу Е4 получаем $\exists y_1 \ldots \exists y_n [\forall u (\mathscr{B}(y_1, \ldots, y_n, u) \supset A_j^{n+1}(y_1, \ldots, y_n, u))] \supset \forall u A_j^{n+1}(y_1, \ldots, y_n, u))$, т. е. $\vdash \mathrm{C}\mathscr{A}_1$. Но тогда, в силу предложения 2.23, $\vdash \mathscr{A}_1$. Формула $\mathscr{A}_2$, являющаяся предваренной нормальной формой для $\mathscr{A}_1$, имеет вид $\exists y_1 \ldots \exists y_n \exists u Q_1 z_1 \ldots Q_s z_s \mathscr{C}$, где $\mathscr{C}$ не содержит кванторов существования, а $Q_1 z_1 \ldots Q_s z_s$ есть кванторная приставка в $\mathscr{B}$. (Строя $\mathscr{A}_2$, мы выносим сначала, по лемме 2.30 (I), первый квантор $\forall u$, который превращается при этом в квантор $\exists u$, затем выносим за знак первой импликации кванторную приставку в $\mathscr{B}$. При этом, в силу леммы 2.30 (I) — (II), кванторы существования превращаются в кванторы всеобщности и обратно. Но когда мы после этого выносим получившуюся кванторную приставку уже за знак второй импликации, то возвращаемся вновь к прежней кванторной приставке $Q_1 z_1 \ldots Q_s z_s$ из $\mathscr{B}$. Наконец, применив лемму 2.30 (III), выносим наружу второй квантор $\forall u$, заменяя одновременно переменную u новой переменной v.) Ранг $\mathscr{A}_2$, очевидно, на единицу меньше ранга $\mathscr{A}$ и, кроме того, на основании предложения 2.31, $\vdash \mathscr{A}_1 \equiv \mathscr{A}_2$. С другой стороны, $\vdash \mathscr{A}$ тогда и только тогда, когда $\vdash \mathscr{A}_1$. Следовательно, $\vdash \mathscr{A}$ тогда и только тогда, когда $\vdash \mathscr{A}_2$. По индуктивному предположению мы уже умеем строить нормальную форму Сколема для $\mathscr{A}_2$, которая, очевидно, является нормальной формой Сколема и для $\mathscr{A}$.

Пример. $\mathscr{A}$: $\forall x \forall y \exists z \mathscr{C}(x, y, z)$, где $\mathscr{C}$ не содержит кванторов. $\mathscr{A}_1$: $\forall x(\forall y \exists z \mathscr{C}(x, y, z) \supset A_j^1(x)) \supset \forall x A_j^1(x)$, где A_j^1 не встречается в $\mathscr{C}$. Построим сначала предваренную нормальную форму для $\mathscr{A}_1$:

$$\exists x([\forall y \exists z \mathscr{C}(x, y, z) \supset A_j^1(x)] \supset \forall x A_j^1(x)) \qquad (2.30(\mathrm{I}));$$

$$\exists x(\exists y[\exists z \mathscr{C}(x, y, z) \supset A_j^1(x)] \supset \forall x A_j^1(x)) \qquad (2.30(\mathrm{I}));$$

$$\exists x(\exists y \forall z(\mathscr{C}(x, y, z) \supset A_j^1(x)) \supset \forall x A_j^1(x)) \qquad (2.30(\mathrm{II}));$$

$$\exists x \forall y(\forall z(\mathscr{C}(x, y, z) \supset A_j^1(x)) \supset \forall x A_j^1(x)) \qquad (2.30(\mathrm{II}));$$

$$\exists x \forall y \exists z((\mathscr{C}(x, y, z) \supset A_j^1(x)) \supset \forall x A_j^1(x)) \qquad (2.30(\mathrm{I}));$$

$$\exists x \forall y \exists z \forall v((\mathscr{C}(x, y, z) \supset A_j^1(x)) \supset A_j^1(v)) \qquad (2.30(\mathrm{III})).$$

Повторим этот процесс снова, теперь уже применительно к формуле $((\mathscr{C}(x, y, z) \supset A_j^1(x)) \supset A_j^1(v))$, которую обозначим через $\mathscr{D}$. Пусть A_k^2

не встречается в $\mathscr{D}$. Строим последовательно формулы:

$\exists x(\forall y[\exists z\forall v\mathscr{D}(x, y, z, v) \supset A_k^3(x, y)] \supset \forall y A_k^3(x, y))$;

$\exists x\exists y([\exists z\forall v\mathscr{D}(x, y, z, v) \supset A_k^3(x, y)] \supset \forall y A_k^3(x, y))$ (2.30(I));

$\exists x\exists y\exists z\forall v([\mathscr{D}(x, y, z, v) \supset A_k^3(x, y)] \supset \forall y A_k^3(x, y))$ (2.30(I), (II));

$\exists x\exists y\exists z\forall v\forall w([\mathscr{D}(x, y, z, v) \supset A_k^3(x, y)] \supset A_k^3(x, w))$ (2.30(III)).

Таким образом, для формулы $\mathscr{A}$ нормальной формой Сколема будет формула $\exists x\exists y\exists z\forall v\forall w([((\mathscr{C}(x, y, z) \supset A_j^1(x)) \supset A_j^1(v)) \supset A_k^3(x, y)] \supset A_k^3(x, w))$.

Упражнения

1. Найти нормальную форму Сколема для формул:

(a) $\neg\exists x A_1^1(x) \supset \forall u\exists y\forall x A_1^3(u, x, y)$; b) $\forall x\exists y\forall u\exists v A_1^4(x, y, u, v)$.

2. Показать, что по всякой формуле $\mathscr{A}$ чистого исчисления предикатов эффективно может быть построена формула $\mathscr{B}$ того же исчисления, выполнимая тогда и только тогда, когда выполнима формула $\mathscr{A}$, и имеющая вид $\forall y_1 \ldots \forall y_n\exists z_1 \ldots \exists z_m\mathscr{C}$, где $n, m \geqslant 0$ и $\mathscr{C}$ не содержит кванторов. (Указание. Применить к $\neg\mathscr{A}$ предложение 2.32.)

3. Найти нормальную форму Сколема $\mathscr{B}$ для формулы $\forall x\exists y A_1^2(x, y)$ и показать, что не $\vdash \mathscr{B} \equiv \forall x\exists y A_1^2(x, y)$. Следовательно, в отличие от предваренной нормальной формы (предложение 2.31) нормальная форма Сколема произвольной формулы $\mathscr{A}$ может не быть логически эквивалентной $\mathscr{A}$.

§ 11. Изоморфизм интерпретаций. Категоричность теорий

Будем говорить, что интерпретация M данной теории первого порядка K *изоморфна* другой интерпретации M′ теории K, если существует такое взаимно однозначное отображение g (называемое изоморфизмом) области D интерпретации M на область D′ интерпретации M′, что

(i) если $(A_j^n)^*$ и $(A_j^n)'$ — интерпретации предикатной буквы A_j^n соответственно в M и M′, то, каковы бы ни были $b_1, \ldots, b_n$ из D, $(A_j^n)^*(b_1, \ldots, b_n)$ выполнено тогда и только тогда, когда выполнено $(A_j^n)'(g(b_1), \ldots, g(b_n))$;

(ii) если $(f_j^n)^*$ и $(f_j^n)'$ — интерпретации функциональной буквы f_j^n соответственно в M и M′, то для любых $b_1, \ldots, b_n$ из D $(f_j^n)^*(b_1, \ldots, b_n) = (f_j^n)'(g(b_1), \ldots, g(b_n))$;

(iii) если a_j^* и a_j' — интерпретации предметной постоянной a_j соответственно в M и M′, то $a_j' = g(a_j^*)$.

Отметим, что если интерпретации M и M′ изоморфны, то их области имеют одинаковую мощность.

Предложение 2.33. *Если* g — *изоморфизм интерпретаций* M *и* M′, *то* (1) *каковы бы ни были формула* $\mathscr{A}$ *теории* K *и последовательность* $s = (b_1, b_2, \ldots)$ *элементов области* D, *формула* $\mathscr{A}$ *выполнена на* s *тогда и только тогда, когда она выполнена на соответствующей последовательности* $g(s) = (g(b_1), g(b_2), \ldots)$ *и, следовательно,* (2) *формула* $\mathscr{A}$ *истинна в* M *тогда и только тогда, когда она истинна в* M′.

Доказательство. (2) вытекает непосредственно из (1). Доказательство (1) легко может быть выполнено индукцией по числу связок и кванторов в $\mathscr{A}$; мы оставляем его читателю в качестве упражнения.

Предложение 2.33 говорит о том, что изоморфные интерпретации имеют одинаковую «структуру», существенно друг от друга не отличаясь.

Упражнения

1. Если M — интерпретация с областью D для некоторой теории, а D′ — множество той же мощности, что и D, то можно построить интерпретацию M′ с областью D′ для той же теории такую, что интерпретация M будет изоморфна интерпретации M′.

2. M изоморфна M. Если M изоморфна M′, то M′ изоморфна M. Если M изоморфна M′ и M′ изоморфна M″, то M изоморфна M″.

Пусть $\mathfrak{m}$ — кардинальное число. Теория K первого порядка с равенством называется $\mathfrak{m}$-категоричной, если 1) всякие две нормальные модели теории K, имеющие мощность $\mathfrak{m}$, изоморфны, и 2) K имеет хотя бы одну нормальную модель мощности $\mathfrak{m}$ (см. Лось [1954c]).

Примеры. 1. Пусть K^2 — теория, получающаяся присоединением к теории K_1 (элементарная теория равенства, см. стр. 88—89) следующей аксиомы (E2):

$$\exists x_1 \exists x_2 (x_1 \neq x_2 \,\&\, \forall x_3 (x_3 = x_1 \vee x_3 = x_2)).$$

Теория K^2 2-категорична Более того, всякая нормальная модель этой теории имеет в точности два элемента. Вообще, пусть (En) обозначает выражение

$$\exists x_1 \ldots \exists x_n \Big(\mathop{\&}_{1 \leqslant i < j \leqslant n} x_i \neq x_j \,\&\, \forall x_{n+1} (x_{n+1} = x_1 \vee \ldots \vee x_{n+1} = x_n)\Big),$$

где $\mathop{\&}_{1 \leqslant i < j \leqslant n} x_i \neq x_j$ — сокращенная запись для конъюнкции всевозможных формул $x_i \neq x_j$ таких, что $1 \leqslant i < j \leqslant n$. Тогда теория K^n, полученная присоединением к K_1 новой аксиомы (En), n-категорична и всякая нормальная модель имеет в точности n элементов.

2. Описанная на стр. 89 теория K_2 плотно упорядоченных множеств без первого и последнего элементов $\aleph_0$-категорична (см. Камке [1950], стр. 71: всякая счетная нормальная модель K_2 изоморфна модели, состоящей из упорядоченного естественным образом множества всех рациональных чисел). При этом можно доказать, что теория K_2 не является $\mathfrak{m}$-категоричной ни для какого $\mathfrak{m}$, отличного от $\aleph_0$.

Упражнения

[A] **1.** Построить теорию первого порядка с равенством, которая не была бы $\aleph_0$-категоричной, но была бы $\mathfrak{m}$-категоричной при любом $\mathfrak{m} > \aleph_0$. (Указание. Рассмотрим теорию G_C коммутативных групп (стр. 89—90). Пусть для любого n nx обозначает терм $\underbrace{(\ldots(x + x) + \ldots + x)}_{n \text{ раз}}$. Присоединим к G_C новые аксиомы

($\mathscr{B}_n$): $\forall x \exists y (ny = x)$, где $n = 2, 3, \ldots$ Новая теория является теорией коммутативных групп с однозначным делением. Ее нормальные модели являются по существу векторными пространствами над полем рациональных чисел. Однако, как известно, любые два таких пространства одной и той же несчетной мощности изоморфны и в то же время существуют счетные не изоморфные друг другу векторные пространства над полем рациональных чисел (см. Бурбаки [1947]).)

A **2.** Построить теорию первого порядка с равенством, $\mathfrak{m}$-категоричную для любой бесконечной мощности $\mathfrak{m}$. (Указание. Присоединить к теории G_C коммутативных групп аксиому $\forall x_1 (2x_1 = 0)$. Нормальные модели полученной таким образом теории — это как раз векторные пространства над полем классов вычетов целых чисел по модулю 2. Любые два таких векторных пространства одинаковой мощности изоморфны (см. Бурбаки [1947]).)

3. Существует ли теория первого порядка с равенством, $\mathfrak{m}$-категоричная для некоторой несчетной мощности $\mathfrak{m}$ и не $\mathfrak{n}$-категоричная для какой-нибудь другой несчетной мощности $\mathfrak{n}$? Выше в примере 2 мы имели дело с теорией, $\mathfrak{m}$-категоричной только для $\mathfrak{m} = \aleph_0$, в упражнении 1 — с теорией, которая не $\aleph_0$-категорична и $\mathfrak{m}$-категорична для любой бесконечной мощности $\mathfrak{m}$, большей $\aleph_0$, и в упражнении 2 — с теорией, $\mathfrak{m}$-категоричной при любом бесконечном $\mathfrak{m}$. Наконец, элементарная теория групп G не является $\mathfrak{m}$-категоричной ни при каком бесконечном $\mathfrak{m}$. Возникает вопрос, не исчерпываются ли этими четырьмя случаями все имеющиеся здесь возможности? (Доказательство того, что дело обстоит именно так, объявил М. Д. Морли в Notices Amer. Math. Soc. **9**, No. 3 (1962), p. 218.)

4. Доказать, что теоремами теории K'^n из предыдущего примера 1 являются те и только те формулы теории K^n, которые истинны в каждой нормальной модели мощности n.

A § 12. Обобщенные теории первого порядка. Полнота и разрешимость *)

Если при определении понятия теории первого порядка мы не будем запрещать несчетные количества предикатных или функциональных букв, а также предметных констант, то получим понятие обобщенной теории первого порядка. Таким образом, теории первого порядка представляют собой частные случаи обобщенных теорий первого порядка. Читатель легко поймет, что все результаты о теориях первого порядка до леммы 2.9 включительно остаются в силе и для обобщенных теорий первого порядка, причем без изменений могут быть сохранены и доказательства. Лемма 2.10 заменяется леммой 2.10′: если множество символов обобщенной теории первого порядка K может быть вполне упорядочено и имеет мощность $\aleph_\alpha$, то множество выражений теории K также может быть вполне упорядочено и имеет мощность $\aleph_\alpha$. (Упорядочим сперва выражения по их длине, которая всегда есть некоторое целое положительное число; пусть теперь e_1 и e_2 — два различных выражения одинаковой длины и j — номер первого, считая слева, символа, входящего в e_1, отличного от j-го символа в e_2, тогда будем считать, что e_1 предшест-

*) Этот параграф предполагает у читателя более детальное знакомство с порядковыми и кардинальными числами (см. гл. 4, а также Камке [1950] или Серпинский [1958]).

вует e_2, если j-й символ из e_1 предшествует j-му символу из e_2 в упорядочении всех символов теории K.) Лемма Линденбаума 2.11′ может быть доказана в тех же предположениях, что и лемма 2.10, причем теми же рассуждениями, которыми доказывался прежний вариант леммы Линденбаума, с той только разницей, что теперь все нумерации (формул $\mathfrak{B}_i$ и теорий J_i) должны быть трансфинитными, а доказательство непротиворечивости и полноты J должно опираться на трансфинитную индукцию Аналог теоремы Генкина 2.12 гласит:

Предложение 2.34. *Если множество символов непротиворечивой обобщенной теории первого порядка* K *может быть вполне упорядочено и имеет мощность* $\aleph_\alpha$, *то* K *имеет модель мощности* $\aleph_\alpha$.

Доказательство. Прежнее доказательство предложения 2.12 модифицируется теперь следующим образом. Добавим $\aleph_\alpha$ новых предметных констант b_1, b_2, ..., b_λ, ... Как и прежде, новая теория K_0 непротиворечива. Пусть $F_1(x_{i_1})$, ..., $F_\lambda(x_{i_\lambda})$, ... $(\lambda < \omega_\alpha)$ — последовательность всех формул теории K_0, содержащих не более одной свободной переменной. Пусть (S_λ) обозначает формулу $\neg \forall x_{i_\lambda} F_\lambda(x_{i_\lambda}) \supset \neg F_\lambda(b_{j_\lambda})$, где последовательность b_{j_1}, ..., b_{j_λ} различных предметных констант выбрана так, что b_{j_λ} не входит в $F_\beta(x_{i_\beta})$ при $\beta \leqslant \lambda$. Новая теория K_∞, полученная присоединением всех формул (S_λ) в качестве новых аксиом, непротиворечива, что доказывается так же, как и прежде, только теперь уже по трансфинитной индукции. После этого, на основании аналога 2.11′ леммы Линденбаума, мы делаем заключение о существовании полного непротиворечивого расширения J теории K_∞. Модель строится теперь так же, как при доказательстве предложения 2.12, ее область, т. е. множество всех замкнутых термов теории K_0, имеет мощность $\aleph_\alpha$.

Следствие 2.35 (1). *Если множество символов непротиворечивой обобщенной теории* K *первого порядка с равенством может быть вполне упорядочено и имеет мощность* $\aleph_\alpha$, *то теория* K *имеет нормальную модель мощности* $\leqslant \aleph_\alpha$. (2) *Если, кроме того,* K *имеет бесконечную нормальную модель (или если* K *имеет сколь угодно большие конечные нормальные модели), то* K *имеет нормальную модель любой мощности* $\aleph_\beta \geqslant \aleph_\sigma$. (3) *В частности, если* K *есть обычная теория первого порядка с равенством (т. е. если* $\aleph_\alpha = \aleph_0$*) и если* K *имеет бесконечную нормальную модель (или если* K *имеет сколь угодно большие конечные нормальные модели), то* K *имеет нормальную модель любой мощности* $\aleph_\beta$ $(\beta \geqslant 0)$.

Доказательство. (1) Существующая на основании предложения 2.34 модель может быть сужена до нормальной (см. стр. 91) модели. Область этой модели состоит из классов эквивалентности в некотором множестве мощности $\aleph_\alpha$ и, следовательно, имеет мощность $\leqslant \aleph_\alpha$.

(2) Пусть $\aleph_\beta \geqslant \aleph_\sigma$, и пусть b_1, b_2 ... — множество новых предметных констант мощности $\aleph_\beta$. Присоединим аксиомы $b_\lambda \neq b_\mu$ для $\lambda \neq \mu$. Повторяя рассуждения доказательства следствия 2.28, можно показать,

что полученная таким образом новая теория непротиворечива и, следовательно, в силу (1), имеет нормальную модель мощности $\leqslant \aleph_\beta$ (поскольку эта новая теория имеет уже $\aleph_\beta$ символов). Но ввиду аксиом $b_\lambda \neq b_\mu$ эта нормальная модель имеет в точности $\aleph_\beta$ элементов.

(3) Есть частный случай (2).

Из леммы 2.9′ и следствия 2.35(1),(2) легко следует, что если обобщенная теория K первого порядка с равенством имеет $\aleph_\alpha$ символов, $\aleph_\beta$-категорична для некоторого $\beta \geqslant \alpha$ и не имеет конечных моделей, то эта теория полна в том смысле, что для любой замкнутой формулы $\mathscr{A}$ либо $\vdash_K \mathscr{A}$, либо $\vdash_K \neg\mathscr{A}$ (Воот [1954]). В самом деле, если не $\vdash_K \mathscr{A}$ и не $\vdash_K \neg\mathscr{A}$, то, в силу леммы 2.9′, теории $K' = K + \{\neg\mathscr{A}\}$ и $K'' = K + \{\mathscr{A}\}$ непротиворечивы, и, в силу следствия 2.35 (1), для этих теорий существуют соответственно модели M_1 и M_2 мощности $\leqslant \aleph_\alpha$. Поскольку K не имеет конечных моделей, то M_1 и M_2 бесконечны. Поэтому, в силу следствия 2.35(2), существуют нормальные модели N_1 и N_2 соответственно теорий K′ и K″, имеющие мощность $\aleph_\beta$. Так как теория K $\aleph_\beta$-категорична, то модели N_1 и N_2 должны быть изоморфны, что невозможно, однако, из-за того, что в модели N_1 должна быть истинна формула $\neg\mathscr{A}$, а в модели N_2 должна быть истинна формула $\mathscr{A}$. Поэтому либо $\vdash_K \mathscr{A}$, либо $\vdash_K \neg\mathscr{A}$.

В частности, если K есть обычная теория первого порядка с равенством, не имеющая конечных моделей и $\aleph_\beta$-категоричная для какого-нибудь $\beta \geqslant 0$, то K — полная теория. Примером такой теории является теория K_2 плотно упорядоченных множеств без первого и последнего элементов (см. стр. 89, упражнение 2): она не имеет конечных моделей и $\aleph_0$-категорична.

Если обычная теория первого порядка K является эффективно аксиоматизированной, т. е. если существует эффективный способ распознавания аксиом этой теории в множестве всех ее формул, и полной, то она разрешима, т. е. существует эффективная процедура, позволяющая для всякой формулы ответить на вопрос, выводима эта формула в K или нет. Чтобы убедиться в этом, следует вспомнить, что теоремы эффективно аксиоматизированной теории можно эффективно перенумеровать. Всякая формула $\mathscr{A}$ выводима тогда и только тогда, когда выводимо ее замыкание. Поэтому мы можем ограничиться рассмотрением одних только замкнутых формул. Так как теория K — полная, то одна из формул $\mathscr{A}$, $\neg\mathscr{A}$ является теоремой теории K и, следовательно, встретится в нашем пересчете теорем. Это и дает нам искомую эффективную процедуру. Заметим, что если теория K противоречива, то всякая формула выводима в K и процедура, распознающая теоремы, тривиальна. Если же теория K непротиворечива, то обе формулы $\mathscr{A}$ и $\neg\mathscr{A}$ не могут появиться при пересчете теорем, и нам отстается лишь ждать, когда появится какая-нибудь одна из них.

Если обычная эффективно аксиоматизированная теория первого порядка с равенством K не имеет конечных моделей и $\aleph_\beta$-категорична при некотором $\beta \geqslant 0$, то, в силу только что доказанного, эта теория

разрешима. Так, например, разрешима теория K_2 плотно упорядоченных множеств без первого и последнего элементов.

В некоторых случаях возможны более прямые способы доказательства полноты и разрешимости В качестве примера рассмотрим только что упомянутую теорию K_2 Ленгфорд [1927] предложил следующую процедуру для K_2. Пусть $\mathscr{A}$ — произвольная замкнутая формула. В силу предложения 2.31, мы можем считать, что $\mathscr{A}$ есть формула в предваренной нормальной форме вида $Qy_1 \ldots Qy_n \mathscr{B}$, где $\mathscr{B}$ не содержит кванторов. Если Qy_n есть $\forall y_n$, то заменим $Qy_n \mathscr{B}$ на $\neg \exists y_n \neg \mathscr{B}$. Таким образом, в любом случае мы можем справа выделить часть $\exists y_n \mathscr{C}$, где $\mathscr{C}$ не содержит кванторов. Затем всякое отрицание $x \neq y$ можно заменить на $x < y \vee y < x$, а отрицание $x \not< y$ — на $x = y \vee y < x$. Следовательно, из $\mathscr{C}$ могут быть изгнаны все знаки отрицания. Мы можем теперь привести $\mathscr{C}$ к дизъюнктивной нормальной форме, т. е. к дизъюнкции конъюнкций элементарных формул (см. стр. 34, упражнение 2). Далее, как мы знаем, формула $\exists y_n (\mathscr{C}_1 \vee \ldots \vee \mathscr{C}_k)$ эквивалентна формуле $\exists y_n \mathscr{C}_1 \vee \ldots \vee \exists y_n \mathscr{C}_k$. Рассмотрим отдельно каждый дизъюнктивный член $\exists y_n \mathscr{C}_i$. $\mathscr{C}_i$ есть конъюнкция элементарных формул вида $t < s$ и $t = s$. Опустим квантор $\exists y_n$ перед $\mathscr{C}_i$, если $\mathscr{C}_i$ не содержит y_n. Заметим, что если $\mathscr{D}$ не содержит y_n, то $\exists y_n (\mathscr{D} \& \mathscr{E})$ можно заменить на $\mathscr{D} \& \exists y_n \mathscr{E}$. Таким образом, мы приходим к рассмотрению формулы вида $\exists y_n \mathscr{F}$, где $\mathscr{F}$ есть конъюнкция элементарных формул, каждая из которых содержит y_n. Если при этом один из конъюнктивных членов есть $y_n = z$, где z — переменная, отличная от y_n, то заменим в $\mathscr{F}$ все вхождения y_n на z и опустим $\exists y_n$. Если $y_n = y_n$ является единственным конъюнктивным членом в $\mathscr{F}$, то тоже опустим $\exists y_n$. Если же $\mathscr{F}$ содержит $y_n = y_n$ вместе с какими-нибудь конъюнктивными членами, то опустим $y_n = y_n$. Всякое выражение $\exists y_n \mathscr{F}$, содержащее конъюнктивным членом в $\mathscr{F}$ неравенство $y_n < y_n$, заменим на $y_n < y_n$. Если $\mathscr{F}$ имеет вид $y_n < z_1 \& \ldots \& y_n < z_j$ или $u_1 < y_n \& \ldots \& u_m < y_n$, где $z_1, \ldots, z_j, u_1, \ldots, u_m$ отличны от y_n, то заменим $\exists y_n \mathscr{F}$ на $y_n = y_n$. Если же $\mathscr{F}$ имеет вид $y_n < z_1 \& \ldots \& y_n < z_j \& u_1 < y_n \& \ldots \& u_m < y_n$, то заменим $\exists y_n \mathscr{F}$ на конъюнкцию всевозможных формул $u_i < z_l$, $1 \leqslant i \leqslant m$, $1 \leqslant l \leqslant j$. Исчерпав таким образом все возможные случаи, мы заменим формулу $\exists y_n \mathscr{C}$ на некоторую формулу $\mathscr{R}$, не содержащую квантора $\exists y_n$, т. е. исключим квантор $\exists y_n$. Мы приходим к формуле $Qy_1 \ldots Qy_{n-1} \mathscr{C}$, где $\mathscr{C}$ не содержит кванторов. Применим ту же процедуру последовательно к кванторам $Qy_{n-1}, \ldots, Qy_1$. В результате мы получим некоторую бескванторную формулу, построенную из элементарных формул вида $x = x$ и $x < x$. Если, наконец, в этой последней формуле заменить всякую элементарную формулу $x = x$ на $x = x \supset x = x$, а всякую элементарную формулу $x < x$ на $\neg (x = x \supset x = x)$, то результатом будет некоторая формула, являющаяся частным случаем тавтологии или отрицания тавтологии. (Доказать!) В силу предложения 2.1 либо выводима сама эта формула, либо выводимо ее отрицание. Легко видеть, что вся описанная процедура представляет собой последовательность переходов

от некоторых формул $\mathscr{T}$ к некоторым формулам $\mathscr{U}$ с сохранением условия $\vdash_K \mathscr{T} \equiv \mathscr{U}$. Отсюда на основании следствия 2.21 заключаем, что если выводима формула, являющаяся окончательным результатом описанной процедуры, то выводима формула $\mathscr{A}$, если же выводимо отрицание окончательного результата процедуры, то выводима формула $\neg\mathscr{A}$. Таким образом, теория K_2 является полной и разрешимой.

Использованный в этом доказательстве метод последовательного исключения кванторов существования был применен также и к другим теориям. С его помощью была получена (Гильберт и Бернайс [1934]), т. I, § 5) разрешающая процедура для элементарной теории равенства K_1 (см. стр. 89). Тарский [1951] доказал этим методом полноту и разрешимость элементарной алгебры (т. е. элементарной теории вещественно замкнутых полей, см. Ван дер Варден [1930—1931]), а Шмелева [1955] доказала разрешимость элементарной теории абелевых групп. (Одно полезное применение этого метода имеется также у Фефермана и Воота [1959].)

[D] Упражнения

1. (Генкин [1955].) Если обычная теория первого порядка с равенством K конечно аксиоматизируема и $\aleph_\alpha$-категорична при каком-нибудь α, то K — разрешимая теория. (Указание. Пусть (B_n) — формула, содержательно выражающая существование не менее n элементов; расширим теорию K, присоединив к ней в качестве новых аксиом формулы (B_n) при $n = 1, 2, \ldots$ Новая теория не имеет конечных моделей.)

2. Доказать разрешимость элементарной теории равенства K_1 (см. стр. 89). (Указание. Рассмотреть формулы (B_n), где (B_n) утверждает существование по крайней мере n элементов. При исключении кванторов существования формулы (B_n) считать элементарными.)

Математические приложения

(1) Пусть F — элементарная теория полей (см. стр. 90) и n служит обозначением для $1 + 1 + \ldots + 1$. Утверждение о том, что поле имеет характеристику p, может быть выражено формулой $\mathscr{C}_p$: $p = 0$. Для любой замкнутой формулы $\mathscr{A}$ теории F, которая истинна во всех полях характеристики 0, существует простое число q такое, что формула $\mathscr{A}$ истинна для каждого поля характеристики $\geqslant q$. В самом деле, пусть F′ — теория, полученная присоединением к F аксиом $\neg\mathscr{C}_2$, $\neg\mathscr{C}_3$, ..., $\neg\mathscr{C}_p$, ... (для всех простых p). Нормальными моделями теории F′ являются поля характеристики нуль. Поэтому, принимая во внимание, что если формула $\mathscr{A}$ истинна во всех нормальных моделях, то она истинна и вообще во всех моделях, мы, на основании следствия 2.15 (а), заключаем, что $\vdash_{F'} \mathscr{A}$. Следовательно, для некоторого конечного набора $\neg\mathscr{C}_{q_1}, \ldots, \neg\mathscr{C}_{q_n}$ новых аксиом мы имеем $\neg\mathscr{C}_{q_1}, \ldots, \neg\mathscr{C}_{q_n} \vdash_F \mathscr{A}$. Пусть q — какое-нибудь простое число, большее каждого из чисел $q_1, \ldots, q_n$. В каждом поле характеристики $\geqslant q$ формулы $\neg\mathscr{C}_{q_1}, \ldots, \neg\mathscr{C}_{q_n}$

истинны; следовательно, истинна и формула $\mathscr{A}$ (А. Робинсон [1951]).

(2) Всякий граф можно рассматривать как множество, частично упорядоченное некоторым бинарным симметричным отношением R (т. е. отношением, выполненным для любых двух вершин тогда и только тогда, когда эти вершины соединены ребром). Назовем граф k-хроматическим, если он может быть разбит на k попарно непересекающихся (возможно пустых) множеств так, чтобы никакие два элемента из одного и того же множества не были связаны отношением R. (Содержательно этим k множествам можно сопоставить k различных цветов, в которые вершины графа окрашиваются таким образом, чтобы всякие две вершины, соединенные ребром, были окрашены в разные цвета.) Очевидно, что всякий подграф k-хроматического графа есть также k-хроматический граф. Докажем, что если множество вершин графа $\mathscr{G}$ может быть вполне упорядочено, а всякий его конечный подграф k-хроматический, то и сам граф $\mathscr{G}$ является k-хроматическим. Для доказательства построим следующую обобщенную теорию K первого порядка с равенством (Бет [1953]). В этой теории будут иметься две двуместные предикатные буквы $A_1^2(=)$ и A_2^2 (соответствующая отношению R на $\mathscr{G}$), k одноместных предикатных букв $A_1^1, \ldots, A_k^1$ (соответствующих тем k множествам, на которые мы стремимся разбить $\mathscr{G}$) и предметные константы a_c, по одной для каждого элемента c графа $\mathscr{G}$. В качестве собственных аксиом, помимо обычных аксиом равенства (6) — (7) (см. стр. 86), возьмем следующие формулы:

(I)	$\neg A_2^2(x, x)$	(иррефлексивность R);
(II)	$A_2^2(x, y) \supset A_2^2(y, x)$	(симметричность R);
(III)	$\forall x (A_1^1(x) \vee \ldots \vee A_k^1(x))$	(разбиение на k классов);
(IV)	$\forall x \neg (A_i^1(x) \& A_j^1(x))$	для $1 \leqslant i < j \leqslant k$ (классы разбиения попарно не пересекаются);
(V)	$\forall x \forall y (A_i^1(x) \wedge A_i^1(y) \supset \neg A_2^2(x, y))$	для $1 \leqslant i \leqslant k$ (никакие два элемента одного и того же класса не связаны отношением R);
(VI)	$a_b \neq a_c$	для любых двух различных элементов b, c из графа $\mathscr{G}$;
(VII)	$A_2^2(a_b, a_c)$	для любых b, c из $\mathscr{G}$, для которых R (b, c).

Рассмотрим произвольное конечное множество этих аксиом. Оно содержит лишь конечное число предметных констант $a_{c_1}, \ldots, a_{c_n}$. Поэтому соответствующий подграф $\{c_1, \ldots, c_n\}$ тоже конечен и, по предположению, k-хроматический. Это означает, что данное конечное множество аксиом имеет модель и потому непротиворечиво. Из непротиворечивости всякого конечного множества аксиом теории K следует,

очевидно, непротиворечивость и самой теории K. Теперь мы видим, что теория K удовлетворяет всем условиям следствия 2.35 (1) и потому имеет нормальную модель, мощность которой меньше или равна мощности графа $\mathcal{G}$. Эта модель является k-хроматическим графом и, в силу (VI) — (VII), содержит граф $\mathcal{G}$ в качестве подграфа. Поэтому и граф $\mathcal{G}$ k-хроматический. (Поучительно сравнить это доказательство с обычным математическим доказательством той же теоремы у д е Б р е й н а и Э р д ё ш а [1951]. Продемонстрированный только что метод часто избавляет от запутанных рассуждений с применением теоремы Тихонова или леммы Кёнига.)

Упражнения

1. (Л о с ь [1954 b.]) Группа B называется упорядочиваемой, если существует такое упорядочивающее группу B отношение R, для которого из xRy следует $(x+z)\,R\,(y+z)$ и $(z+x)\,R\,(z+y)$. Методом, подобным примененному в примере (2) выше, показать, что группа B упорядочиваема тогда и только тогда, когда упорядочиваема любая ее конечно порожденная подгруппа. (При этом, как и в предыдущем примере, предполагается также, что группа B может быть вполне упорядочена.)

2. Построить теорию первого порядка алгебраически замкнутых полей характеристики $p\,(\geqslant 0)$, присоединив к теории F полей новые аксиомы P_n, где P_n утверждает существование корня у всякого отличного от константы полинома степени $\leqslant n$, а также аксиомы для определения характеристики. Показать, что формула теории F, истинная в каком-нибудь одном алгебраически замкнутом поле характеристики нуль, истинна во всяком таком поле. (У к а з а н и е. Эта теория $\aleph_\beta$-категорична для $\beta > 0$, аксиоматизируема и не имеет конечной модели.) (См. А. Р о б и н с о н [1952].)

3. Обычными математическими рассуждениями решить конечную задачу бракосочетания: пусть M — конечное множество, состоящее из m мужчин, и N — некоторое множество женщин, причем каждый мужчина знает лишь конечное число женщин, а если $1 \leqslant k \leqslant m$, то мужчины всякого подмножества мощности k множества M знакомы не менее чем с k женщинами из N (т. е. существует не менее k женщин из N, каждая из которых знакома по крайней мере с одним из данных k мужчин); тогда имеется возможность сочетать браком (моногамно) всех мужчин из M с женщинами из N таким образом, чтобы каждый мужчина женился на знакомой ему женщине. (У к а з а н и е (Х а л м о ш и В о о т [1950]). При $m = 1$ решение тривиально, для $m > 1$ применить индукцию, рассмотрев два случая: (I) при любом k, где $1 \leqslant k < m$, всякое множество из k мужчин знакомо не менее чем с $k+1$ женщинами и (II) для некоторого k, где $1 \leqslant k < m$, существует множество из k мужчин, знакомых в точности с k женщинами.) Распространить этот результат на бесконечный случай, т. е. на тот случай, когда, при прежних предположениях для любого конечного k, само множество M бесконечно (и может быть вполне упорядочено). (У к а з а н и е. Построить подходящую обобщенную теорию первого порядка, аналогичную той, что была использована выше в примере (2) математических приложений, и применить следствие 2.35 (1).)

4. Решение 17-й проблемы Гильберта методом, изложенным в этом параграфе, можно найти в работе А. Р о б и н с о н а [1955].

Пусть $\mathscr{A}$ — какая-нибудь формула в предваренной нормальной форме, являющаяся своим замыканием, например,

$$\exists y_1 \forall y_2 \forall y_3 \exists y_4 \exists y_5 \forall y_6 \mathscr{B}(y_1, y_2, y_3, y_4, y_5, y_6),$$

где $\mathscr{B}$ не содержит кванторов. Опустим квантор $\exists y_1$ и заменим y_1 в $\mathscr{B}$ новой предметной константой b_1: $\forall y_2 \forall y_3 \exists y_4 \exists y_5 \forall y_6 \mathscr{B}(b_1, y_2, y_3, y_4, y_5, y_6)$. Теперь опустим кванторы $\forall y_2$, $\forall y_3$ и получим формулу $\exists y_4 \exists y_5 \forall y_6 \mathscr{B}(b_1, y_2, y_3, y_4, y_5, y_6)$. Опустим, далее, квантор $\exists y_4$ и заменим переменную y_4 в $\mathscr{B}$ новой функциональной буквой $g(y_2, y_3)$: $\exists y_5 \forall y_6 \mathscr{B}(b_1, y_2, y_3, g(y_2, y_3), y_5, y_6)$. Опустим квантор $\exists y_5$, заменив в $\mathscr{B}$ переменную y_5 на новую функциональную букву $h(y_2, y_3)$: $\forall y_6 \mathscr{B}(b_1, y_1, y_2, g(y_2, y_3), h(y_2, y_3), y_6)$. Наконец, опустим и квантор $\forall y_6$: $\mathscr{B}(b_1, y_2, y_3, g(y_2, y_3), h(y_2, y_3), y_6)$. Последняя формула не содержит кванторов. Таким образом, вводя новые функциональные буквы, мы можем исключить все кванторы из произвольной замкнутой формулы $\mathscr{A}$ в предваренной нормальной форме. Обозначим через $\mathscr{A}^*$ результат такой переработки формулы $\mathscr{A}$.

Примеры. 1. Пусть $\mathscr{A}$ есть $\forall y_1 \exists y_2 \forall y_3 \forall y_4 \exists y_5 \mathscr{B}(y_1, y_2, y_3, y_4, y_5)$, тогда в качестве $\mathscr{A}^*$ имеем

$$\mathscr{B}(y_1, g(y_1), y_3, y_4, h(y_1, y_3, y_4)).$$

2. Если $\mathscr{A}$ есть $\exists y_1 \exists y_2 \forall y_3 \forall y_4 \exists y_5 \mathscr{B}(y_1, y_2, y_3, y_4, y_5)$, то соответствующей формулой $\mathscr{A}^*$ будет формула $\mathscr{B}(b, c, y_3, y_4, g(y_3, y_4))$.

Отметим, что $\mathscr{A}^* \vdash \mathscr{A}$, так как кванторы можно вернуть назад несколькими последовательными применениями правил Gen и E4. (В самом деле, ведь, говоря точно, мы в процессе построения $\mathscr{A}^*$ опускаем все кванторы общности и все кванторы существования и при этом каждую связанную квантором существования переменную y_i заменяем термом $g(z_1, \ldots, z_k)$, где g — некоторая новая функциональная буква и $z_1, \ldots, z_k$ — все те переменные, которые связаны кванторами всеобщности, предшествующими квантору $\exists y_i$.)

Предложение 2.36. (Вторая ε-теорема; Расёва [1956], Гильберт и Бернайс [1939].) *Пусть* K — *теория первого порядка. Заменим каждую аксиому* $\mathscr{A}$ *теории* K *новой аксиомой* $\mathscr{A}^*$. (*При этом предполагается, что при построении этих формул* $\mathscr{A}^*$ *новые функциональные буквы и предметные переменные, вводимые для какой-нибудь одной формулы, отличны от таковых же, вводимых для других формул.*) *Пусть* K* *есть теория первого порядка с собственными аксиомами* $\mathscr{A}^*$. *Тогда* (a) *если* $\mathscr{C}$ — *формула теории* K *и* $\vdash_{K^*} \mathscr{C}$, *то* $\vdash_K \mathscr{C}$, (b) *теория* K *непротиворечива тогда и только тогда, когда непротиворечива теория* K*.

Доказательство. (1) Пусть $\vdash_{K^*} \mathscr{C}$, где $\mathscr{C}$ — формула теории K, и пусть M — счетная модель теории K. Мы всегда можем считать, что областью модели M является множество P всех натуральных чисел (см. упражнение 1 на стр. 103). Пусть $\mathscr{A}$ — какая-нибудь аксиома теории K; предположим для определенности, что она имеет вид $\exists y_1 \forall y_2 \forall y_3 \exists y_4 \mathscr{B}(y_1, y_2, y_3, y_4)$, где $\mathscr{B}$ не содержит кванторов. Тогда $\mathscr{A}^*$ будет иметь вид $\mathscr{B}(b, y_2, y_3, g(y_2, y_3))$. Последовательными шагами расширим теперь модель M (не изменяя, однако, ее области P) следующим образом. Так как формула $\exists y_1 \forall y_2 \forall y_3 \exists y_4 \mathscr{B}(y_1, y_2, y_3, y_4)$ истинна

в модели M, то существуют целые положительные числа y_1, для которых $\forall y_2 \forall y_3 \exists y_4 \mathscr{B}(y_1, y_2, y_3, y_4)$ истинно в M; число b^*, являющееся наименьшим среди таких y_1, сделаем интерпретацией предметной константы b. В расширенной таким образом модели, очевидно, истинна формула $\exists y_4 \mathscr{B}(b, y_2, y_3, y_4)$. Для любых целых положительных y_2, y_3 интерпретацией $g(y_2, y_3)$ пусть будет то наименьшее y_4, при котором формула $\mathscr{B}(b, y_2, y_3, y_4)$ истинна в расширенной модели. Итак, формула $\mathscr{B}(b, y_2, y_3, g(y_2, y_3))$ истинна в расширенной модели. Поступив аналогичным образом с каждой аксиомой $\mathscr{A}$ теории K, мы построим модель M* теории K*. Так как $\vdash_{K^*} \mathscr{C}$, то формула $\mathscr{C}$ истинна в M*. Но тогда формула $\mathscr{C}$ истинна, очевидно, и в модели M, ибо модель M* тем только и отличается от модели M, что заключает в себе интерпретации нововведенных функциональных букв и предметных констант, которых $\mathscr{C}$, как всякая формула теории K, не содержит. Итак, доказано, что формула $\mathscr{C}$ истинна во всякой счетной модели теории K. Отсюда, на основании следствия 2.15 (а), следует $\vdash_K \mathscr{C}$. (Конструктивное доказательство эквивалентного результата см. у Гильберта и Бернайса [1939].)

(2) Ввиду того, что $\mathscr{A}^* \vdash \mathscr{A}$, теория K* является расширением теории K. Следовательно, если теория K* непротиворечива, то непротиворечива и теория K. Предположим теперь, что непротиворечива теория K. Пусть $\mathscr{C}$ — произвольная формула теории K. Если бы теория K* была противоречива, то мы имели бы $\vdash_{K^*} \mathscr{C} \& \neg \mathscr{C}$. Тогда, в силу части (1) настоящего доказательства, мы имели бы и $\vdash_K \mathscr{C} \& \neg \mathscr{C}$, что невозможно из-за непротиворечивости теории K.

Назовем *обобщенной теоремой полноты* предложение, гласящее, что всякая непротиворечивая обобщенная теория первого порядка имеет модель. Очевидно, если предположить, что можно вполне упорядочить всякое множество (или, что эквивалентно, при допущении аксиомы выбора), обобщенная теорема полноты является следствием предложения 2.34.

Теоремой о максимальном идеале мы называем следующее утверждение: всякая булева алгебра имеет максимальный идеал. Это утверждение эквивалентно теореме о булевом представлении, согласно которой всякая булева алгебра изоморфна некоторой булевой алгебре множеств. (См. Стоун [1936]. О теории булевых алгебр см. Сикорский [1960].) Единственное известное доказательство теоремы о максимальном идеале использует аксиому выбора. Любопытно, однако, что эта теорема эквивалентна обобщенной теореме полноты и что эта эквивалентность может быть доказана без применения аксиомы выбора.

Предложение 2.37. (Лось [1954а], Расёва и Сикорский [1951], [1952].) *Обобщенная теорема о полноте эквивалентна теореме о максимальном идеале.*

Доказательство. (1) Допустим, что верна обобщенная теорема о полноте. Пусть B — булева алгебра. Построим обобщенную теорию K

первого порядка с равенством, имеющую двуместные функциональные буквы $\cup$ и $\cap$, одноместную функциональную букву f_1^1 ($f_1^1(t)$ мы будем обозначать через $\bar{t}$), предикатные буквы $=$ и A_1^1 и для каждого элемента b алгебры B предметную константу a_b. В качестве аксиом мы возьмем обычные аксиомы булевой алгебры (см. Сикорский [1960]), аксиомы (6) — (7) равенства, полное описание B (т. е. всевозможные формулы $a_b \neq a_c$, $a_b \cup a_c = a_d$, $a_b \cap a_c = a_e$, $\bar{a}_b = a_{b_1}$, где соответственно $b \neq c$, $b \cup c = d$, $b \cap c = e$, $\bar{b} = b_1$ в B) и, наконец, аксиомы, выражающие тот факт, что A_1^1 определяет максимальный идеал (т. е. $A_1^1(x \cap \bar{x})$, $A_1^1(x) \& A_1^1(y) \supset A_1^1(x \cup y)$, $A_1^1(x) \supset A_1^1(x \cap y)$, $A_1^1(x) \vee \vee A_1^1(\bar{x})$ и $\neg A_1^1(x \cup \bar{x})$. Теория K непротиворечива. В самом деле, вывод противоречия в K, если бы такой существовал, содержал бы лишь конечное число символов a_b, a_c, ..., например, a_{b_1}, ..., a_{b_n}, и тогда соответствующие элементы b_1, ..., b_n алгебры B порождали бы некоторую конечную подалгебру B′ алгебры B. Но всякая конечная булева алгебра, очевидно, имеет максимальный идеал. Следовательно, подалгебра B′ была бы моделью для формул, встречающихся в выводе противоречия, а само это противоречие было бы истинно в B′, что невозможно. В силу своей непротиворечивости, теория K имеет, согласно обобщенной теореме полноты, некоторую модель A, являющуюся, естественно, булевой алгеброй с некоторым максимальным идеалом I. Но алгебра B, очевидно, есть подалгебра алгебры A, и следовательно, множество $I \cap B$ является максимальным идеалом в B.

(2) Предположим, что верна теорема о максимальном идеале. Пусть K — непротиворечивая обобщенная теория первого порядка. Для каждой аксиомы $\mathscr{A}$ теории K построим формулу $\mathscr{A}^*$, приведя сначала $\mathscr{A}$ к предваренной нормальной форме, а затем исключив кванторы путем введения новых функциональных букв и предметных констант. Пусть K′ — теория, имеющая своими аксиомами построенные таким образом формулы $\mathscr{A}^*$, а также все частные случаи тавтологий, и такая, в которой все формулы не содержат кванторов, а правилами вывода служат modus ponens и правило подстановки для переменных (т. е. подстановки термов вместо переменных). Теория K′ непротиворечива, так как теоремы этой теории являются одновременно теоремами непротиворечивой теории K* из предложения 2.36. Пусть B — алгебра Линденбаума, порожденная теорией K′. (Поясним, что это значит: пусть для произвольных формул $\mathscr{A}$ и $\mathscr{B}$ $\mathscr{A}\,\mathrm{Eq}\,\mathscr{B}$ означает $\vdash_{K'} \mathscr{A} \equiv \mathscr{B}$; отношение Eq есть отношение эквивалентности; пусть $[\mathscr{A}]$ — класс эквивалентности, определяемый формулой $\mathscr{A}$; зададим операции $\cup$, $\cap$, $^-$ над классами эквивалентности равенствами $[\mathscr{A}] \cup [\mathscr{B}] = [\mathscr{A} \vee \mathscr{B}]$, $[\mathscr{A}] \cap [\mathscr{B}] = = [\mathscr{A} \& \mathscr{B}]$ и $\overline{[\mathscr{A}]} = [\neg \mathscr{A}]$; относительно этих операций классы эквивалентности образуют булеву алгебру, которая и называется алгеброй Линденбаума, порожденной теорией K′.) Пусть, согласно теореме о максимальном идеале, I есть максимальный идеал алгебры B. Построим модель M теории K′ с областью, состоящей из термов теории K′.

в которой предметные константы и функциональные буквы интерпретируют самих себя, и для всякой предикатной буквы A_j^n предикат $A_j^n(t_1, \ldots, t_n)$ считается истинным в M тогда и только тогда, когда $[A_j^n(t_1, \ldots, t_n)]$ не принадлежит I. Легко показать, что любая формула $\mathscr{A}$ теории K′ истинна в M тогда и только тогда, когда $[\mathscr{A}]$ не принадлежит I. Но для всякой теоремы $\mathscr{B}$ теории K′ $[\mathscr{B}]=1$ и, следовательно, $[\mathscr{B}]$ не принадлежит I. Поэтому M на самом деле является моделью K′. Для любой аксиомы $\mathscr{A}$ теории K каждый результат подстановки в формулу $\mathscr{A}^*(y_1, \ldots, y_n)$ является теоремой теории K′, следовательно, формула $\mathscr{A}^*(y_1, \ldots, y_n)$ истинна в модели M при любых $y_1, \ldots, y_n$. Обращая процесс, в результате которого формула $\mathscr{A}^*$ возникает из формулы $\mathscr{A}$, теперь легко доказать, что и эта последняя формула истинна в модели M. Таким образом, M есть также модель и для теории K.

Является ли обобщенная теорема полноты существенно более слабой, чем аксиома выбора, или она ей эквивалентна? Некоторые частичные результаты, относящиеся к этой проблеме, можно найти у Лося и Рылль-Нардзевского [1954] и у Генкина [1954]. О найденном доказательстве неэквивалентности этих предложений заявил Дж. Д. Гальперн в Notices Amer. Math. Soc. **9**, No. 4 (1962), p. 315.

Упражнения

1. Доказать, что обобщенная теорема о полноте влечет утверждение о том, что всякое множество может быть упорядочено (и, следовательно, аксиому выбора для любого множества непустых попарно не пересекающихся конечных множеств).

2. Проанализировать доказательство предложения 2.37(2) и показать, что если K есть обычная теория первого порядка, то алгебра Линденбаума B счетна, и все рассуждение может быть проведено без использования теоремы о максимальном идеале.

Алгебраические структуры, естественным образом связанные с исчислениями высказываний, оказываются булевыми алгебрами (см. стр. 52, упражнение 3, а также Розенблюм [1950], гл. 1—2). В случае теорий первого порядка наличие кванторов приводит к более сложным алгебраическим структурам. Так, например, если K есть теория первого порядка, то в соответствующей алгебре Линденбаума B имеет место $[\exists x A(x)] = \sum\limits_t [\mathscr{A}(t)]$, где $\sum\limits_t$ означает наименьшую верхнюю грань в B, а t пробегает множество всех термов, свободных для x в $\mathscr{A}(x)$. В свое время были предложены два типа алгебраических структур в качестве алгебраических аналогов рассмотренных в этой главе логических теорий. Один из них — цилиндрические алгебры — был детально изучен Тарским, Томпсоном, Генкиным и другими (см. Генкин и Тарский [1961]). Другим подходом явилась теория полиадических алгебр, введенная и развитая Халмошем [1962].

Глава 3

Формальная арифметика

§ 1. Система аксиом

Наряду с геометрией арифметика является наиболее непосредственно интуитивной областью математики. Вполне естественно поэтому именно с арифметики начать попытку формализации и строгого обоснования математики. Первое, полуаксиоматическое построение этой дисциплины было предложено Дедекиндом [1901] и стало известно под названием «системы аксиом Пеано» *). Эту систему можно сформулировать следующим образом:

(P1) 0 есть натуральное число.

(P2) для любого натурального числа x существует другое натуральное число, обозначаемое x′ и называемое: (*непосредственно*) *следующее* за x.

(P3) $0 \neq x'$ для любого натурального числа x.

(P4) Если $x' = y'$, то $x = y$.

(P5) Если Q есть свойство, которым, быть может, обладают одни и не обладают другие натуральные числа, и если

(I) натуральное число 0 обладает свойством Q и

(II) для всякого натурального числа x из того, что x обладает свойством Q, следует, что и натуральное число x′ обладает свойством Q, то свойством Q обладают все натуральные числа (*принцип индукции*).

Этих аксиом, вместе с некоторым фрагментом теории множеств, достаточно для построения не только арифметики, но и теории рациональных, вещественных и комплексных чисел (см. Ландау [1930]). Однако в этих аксиомах содержатся интуитивные понятия такие, как, например, «свойство», что мешает всей системе быть строгой формализацией. Поэтому мы сейчас построим некоторую теорию первого порядка S, основанную на системе аксиом Пеано, которая окажется, по всей видимости, достаточной для вывода всех основных результатов элементарной арифметики.

Эта теория первого порядка S будет иметь единственную предикатную букву A_1^2, единственную предметную константу a_1 и три функциональные буквы f_1^1, f_1^2, f_2^2. Впрочем, чтобы не порывать с привычными нам по неформальной арифметике обозначениями, в дальнейшем м

*) Исторические сведения по этому вопросу можно найти у Ван Х[illegible] [1957a].

будем обычно писать $t = s$ вместо $A_1^2(t, s)$, 0 вместо a_1 и t', $t + s$, $t \cdot s$ соответственно вместо $f_1^1(t)$, $f_1^2(t, s)$, $f_2^2(t, s)$, где t и s — термы. Вот собственные аксиомы теории S:

(S1) $x_1 = x_2 \supset (x_1 = x_3 \supset x_2 = x_3)$;
(S2) $x_1 = x_2 \supset x_1' = x_2'$,
(S3) $0 \neq (x_1)'$;
(S4) $x_1' = x_2' \supset x_1 = x_2$;
(S5) $x_1 + 0 = x_1$;
(S6) $x_1 + x_2' = (x_1 + x_2)'$;
(S7) $x_1 \cdot 0 = 0$;
(S8) $x_1 \cdot (x_2') = (x_1 \cdot x_2) + x_1$;
(S9) $\mathscr{A}(0) \supset (\forall x (\mathscr{A}(x) \supset \mathscr{A}(x')) \supset \forall x \mathscr{A}(x))$, где $\mathscr{A}(x)$ — произвольная формула теории S.

Заметим, что аксиомы (S1) — (S8) являются конкретными формулами, в то время как (S9) представляет собой схему аксиом, порождающую бесконечное множество аксиом. При этом схема аксиом (S9), которую мы будем называть *принципом математической индукции*, не соответствует полностью аксиоме (P5) системы аксиом Пеано, поскольку в этой последней интуитивно предполагаются $2^{\aleph_0}$ свойств натуральных чисел, а схема аксиом (S9) может иметь дело лишь со счетным множеством свойств, определяемых формулами теории S.

Аксиомы (S3) и (S4) соответствуют аксиомам (P3) и (P4) системы аксиом Пеано. Аксиомы (P1) и (P2) пеановской системы обеспечивают существование нуля 0 и операции «непосредственно следующий», которым в теории S соответствуют предметная константа a_1 и функциональная буква f_1^1. Наши аксиомы (S1) — (S2) обеспечивают некоторые необходимые свойства равенства, которые Дедекиндом и Пеано предполагались как интуитивно очевидные. Аксиомы (S5) — (S8) представляют собой рекурсивные равенства, служащие определениями операций сложения и умножения. Никаких постулатов, соответствующих этих аксиомам, Дедекинд и Пеано не формулировали, потому что они допускали использование интуитивной теории множеств, в рамках которой существование операций $+$ и $\cdot$, удовлетворяющих аксиомам (S5) — (S8), выводимо. (См. Ландау [1930], теоремы 4 и 28.)

С помощью MP из схемы аксиом (S9) мы можем получить следующее *правило индукции*: из $\mathscr{A}(0)$ и $\forall x (\mathscr{A}(x) \supset \mathscr{A}(x'))$ выводится $\forall x \mathscr{A}(x)$.

Наша ближайшая цель состоит в том, чтобы вывести обычные свойства равенства; другими словами, мы хотим доказать, что свойства (6) — (7) равенства (см. стр. 86) выводимы в S, и, следовательно, S является теорией первого порядка с равенством.

Прежде всего, отметим некоторые непосредственные и очевидные следствия из аксиом. Этими следствиями мы будем в дальнейшем поль-

зоваться для сокращения и вообще для более удобного проведения доказательств.

Лемма 3.1. *Для любых термов* t, s *и* r *теории* S *следующие формулы суть теоремы в* S:

(S1′) $t=r\supset(t=s\supset r=s)$;
(S2′) $t=r\supset t'=r'$;
(S3′) $0\neq t'$;
(S4′) $t'=r'\supset t=r$;
(S5′) $t+0=t$;
(S6′) $t+r'=(t+r)'$;
(S7′) $t\cdot 0=0$;
(S8′) $t\cdot r'=(t\cdot r)+t$.

Доказательство. (S1′) — (S8′) следуют соответственно из (S1) — (S8): сперва следует образовать замыкания по правилу Gen, а затем применить правило A4 с подходящими термами t, r, s.

Предложение 3.2. *Для любых термов* t, s *и* r *следующие формулы являются теоремами теории* S:

(a) $t=t$;
(b) $t=r\supset r=t$;
(c) $t=r\supset(r=s\supset t=s)$;
(d) $r=t\supset(s=t\supset r=s)$;
(e) $t=r\supset t+s=r+s$;
(f) $t=0+t$;
(g) $t'+r=(t+r)'$;
(h) $t+r=r+t$;
(i) $t=r\supset s+t=s+r$;
(j) $(t+r)+s=t+(r+s)$;
(k) $t=r\supset t\cdot s=r\cdot s$;
(l) $0\cdot t=0$;
(m) $t'\cdot r=t\cdot r+r$;
(n) $t\cdot r=r\cdot t$;
(o) $t=r\supset s\cdot t=s\cdot r$.

Доказательство.

(a) 1. $t+0=t$ (S5′)
2. $(t+0=t)\supset(t+0=t\supset t=t)$ (S1′)
3 $t+0=t\supset t=t$ 1, 2, MP
4. $t=t$ 1, 3, MP

(b) 1. $t=r \supset (t=t \supset r=t)$ (S1′)
2. $t=t \supset (t=r \supset r=t)$ 1, тавтология
3. $t=r \supset r=t$ 2, (a), MP

(c) 1. $r=t \supset (r=s \supset t=s)$ (S1′)
2. $t=r \supset r=t$ (b)
3. $t=r \supset (r=s \supset t=s)$ 1, 2, тавтология

(d) 1. $r=t \supset (t=s \supset r=s)$ (c)
2. $t=s \supset (r=t \supset r=s)$ 1, тавтология
3. $s=t \supset t=s$ (b)
4. $s=t \supset (r=t \supset r=s)$ 2, 3, тавтология
5. $r=t \supset (s=t \supset r=s)$ 4, тавтология

(e) Применим правило индукции к следующей формуле $\mathscr{A}(z)$: $x=y \supset (x+z=y+z)$.

(i) 1. $x+0=x$ (S5′)
2. $y+0=y$ (S5′)
3. $x=y$ гипотеза
4. $x+0=y$ 1, 3, (c)
5. $x+0=y+0$ 2, 4, (d)
6. $x=y \supset x+0=y+0$ 1—5, теорема дедукции
т. е. $\vdash \mathscr{A}(0)$.

(ii) 1. $x=y \supset x+z=y+z$ гипотеза
2. $x=y$ гипотеза
3. $x+z'=(x+z)'$ (S6′)
4. $y+z'=(y+z)'$ (S6′)
5. $x+z=y+z$ 1, 2, MP
6. $(x+z)'=(y+z)'$ 5, (S2′)
7. $x+z'=(y+z)'$ 3, 6, (c)
8. $x+z'=y+z'$ 4, 7, (d)
9. $(x=y \supset (x+z=y+z)) \supset$
$\supset (x=y \supset (x+z'=y+z'))$ 1—8, теорема дедукции
т. е. $\vdash \mathscr{A}(z) \supset \mathscr{A}(z')$.

По правилу индукции из (i) и (ii) следует $\vdash \forall z\, \mathscr{A}(z)$, откуда с помощью правил Gen и A4 окончательно получаем $\vdash t=r \supset t+s=r+s$.

(f) Обозначим через $\mathscr{A}(x)$ формулу $x=0+x$.

(i) $0=0+0$, в силу (S5′) и (b),
т. е. $\vdash \mathscr{A}(0)$.

(ii) 1. $x=0+x$ гипотеза
2. $(0+x')=(0+x)'$ (S6′)
3. $x'=(0+x)'$ 1, (S2′)
4. $x'=0+x'$ 2, 3, (d)
5. $x=0+x\supset x'=0+x'$ 1—4, Теорема дедукции
т. е. $\vdash\mathscr{A}(x)\supset\mathscr{A}(x')$.

Из (i) и (ii) получаем по правилу индукции $\vdash\forall x(x=0+x)$, откуда по правилу A4 $\vdash t=0+t$.

(g) Пусть $\mathscr{A}(y)$ обозначает $x'+y=(x+y)'$.

(i) 1. $x'+0=x'$ (S5′)
2. $x+0=x$ (S5′)
3. $(x+0)'=x'$ 2, (S2′)
4. $x'+0=(x+0)'$ 1, 3, (d)
т. е. $\vdash\mathscr{A}(0)$.

(ii) 1. $x'+y=(x+y)'$ гипотеза
2. $x'+y'=(x'+y)'$ (S6′)
3. $(x'+y)'=(x+y)''$ 1, (S2′)
4. $x'+y'=(x+y)''$ 2, 3, (c)
5. $(x+y')=(x+y)'$ (S6′)
6. $(x+y')'=(x+y)''$ 5, (S2′)
7. $x'+y'=(x+y')'$ 4, 6, (d)
8. $x'+y=(x+y)'\supset$
$\supset x'+y'=(x+y')'$ 1—7, теорема дедукции
т. е. $\vdash\mathscr{A}(y)\supset\mathscr{A}(y')$.

Теперь из (i) и (ii) получаем с помощью правила индукции $\vdash\forall y(x'+y=(x+y)')$ и затем в силу Gen и A4 $\vdash t'+r=(t+r)'$.

(h) Пусть $\mathscr{A}(x)$ обозначает $x+y=y+x$.

(i) 1. $x+0=x$ (S5′)
2. $x=0+x$ (f)
3. $x+0=0+x$ 1, 2, (c)
т. е. $\vdash\mathscr{A}(0)$.

(ii) 1. $x+y=y+x$ гипотеза
2. $x+y'=(x+y)'$ (S6′)
3. $y'+x=(y+x)'$ (g)
4. $(x+y)'=(y+x)'$ 1, (S2′)
5. $x+y'=(y+x)'$ 2, 4, (c)
6. $x+y'=y'+x$ 3, 5, (d)
7. $x+y=y+x\supset$
$\supset x+y'=y'+x$ 1—6, теорема дедукции
т. е. $\vdash\mathscr{A}(y)\supset\mathscr{A}(y')$.

Отсюда, в силу (i) и (ii), по правилу индукции имеем $\vdash \forall y\,(x+y = y+x)$ и затем по правилам Gen и A4 получаем $\vdash t+r = r+t$.

(i)	1. $t=r \supset t+s=r+s$	(e)
	2. $t+s=s+t$	(h)
	3. $r+s=s+r$	(h)
	4. $t=r$	гипотеза
	5. $t+s=r+s$	1, 4, MP
	6. $s+t=r+s$	2, 5, (S1′)
	7. $s+t=s+r$	3, 6, (c)
	8. $t=r \supset s+t=s+r$	1—7, теорема дедукции

(j) Берем в качестве $\mathscr{A}(z)$ формулу $(x+y)+z=x+(y+z)$.

(i)	1. $(x+y)+0=x+y$	(S5′)
	2. $y+0=y$	(S5′)
	3. $x+(y+0)=x+y$	2, (i)
	4. $(x+y)+0=x+(y+0)$	1, 3, (d)
	т. е. $\vdash \mathscr{A}(0)$.	
(ii)	1. $(x+y)+z=x+(y+z)$	гипотеза
	2. $(x+y)+z'=((x+y)+z)'$	(S6′)
	3. $((x+y)+z)'=(x+(y+z))'$	1, (S2′)
	4. $(x+y)+z'=(x+(y+z))'$	2, 3, (c)
	5. $y+z'=(y+z)'$	(S6′)
	6. $x+(y+z')=x+(y+z)'$	5, (i)
	7. $x+(y+z)'=(x+(y+z))'$	(S6′)
	8. $x+(y+z')=(x+(y+z))'$	6, 7, (d)
	9. $(x+y)+z'=x+(y+z')$	4, 8, (d)
	10. $(x+y)+z=x+(y+z) \supset$ $\supset (x+y)+z'=x+(y+z')$	1—9, теорема дедукции
	т. е. $\vdash \mathscr{A}(z) \supset \mathscr{A}(z')$.	

И снова, применяя к (i) и (ii) правило индукции, получаем $\vdash \forall z\,((x+y)+z=x+(y+z))$, откуда по правилам Gen и A4 заключаем $\vdash (t+r)+s=t+(r+s)$.

Доказательство пунктов (k) — (o) оставляем читателю в качестве упражнений.

Следствие 3.3. *Теория* S *является теорией первого порядка с равенством, т. е. в этой теории* $\vdash x_1=x_1$ *и* $\vdash x=y \supset (\mathscr{A}(x,x) \supset \supset \mathscr{A}(x,y))$, *где* $\mathscr{A}(x,y)$ *получается из* $\mathscr{A}(x,x)$ *заменой одного или нескольких вхождений* x *на* y *при условии, что переменная* y *свободна для этих вхождений* x (см. стр. 86).

Доказательство. В силу предложения 2.26 утверждение 3.3 является непосредственным следствием предложения 3.2 (a) — (e), (i), (k), (o) и (S2′).

Отметим, что интерпретация теории S, в которой

(a) множество всех неотрицательных целых чисел служит областью,

(b) целое число 0 интерпретирует символ 0,

(c) операция взятия последующего (прибавление единицы) интерпретирует функцию $'$ (т. е. функциональную букву f_1^1),

(d) обычные сложение и умножение интерпретируют $+$ и $\cdot$,

(e) предикатная буква $=$ интерпретируется отношением тождества, является нормальной моделью теории S. Эта модель называется *стандартной моделью* теории S. Всякая нормальная модель теории S, не изоморфная ее стандартной модели, называется *нестандартной моделью* теории S.

Если мы признаем эту стандартную интерпретацию моделью теории S, то тогда мы должны будем признать и факт непротиворечивости этой теории. Однако семантические методы, включающие в себя, как правило, известную долю теоретико-множественных рассуждений, по мнению некоторых математиков являются слишком ненадежной основой для доказательства непротиворечивости. Более того, мы и не доказываем строго, что аксиомы теории S истинны в стандартной интерпретации, а принимаем это утверждение всего лишь как интуитивно очевидное. Поэтому, а также по ряду других причин принято всякий раз, когда на утверждение о непротиворечивости теории S опирается какое-либо доказательство, явно ссылаться на это утверждение как на некоторую недоказанную гипотезу. (В Приложении мы приводим одно «доказательство» непротиворечивости теории S.)

Ряд важных свойств сложения и умножения содержится в следующих предложениях.

Предложение 3.4. *Для любых термов* t, r, s *следующие формулы являются теоремами теории* S:

(a) $t\cdot(r+s)=(t\cdot r)+(t\cdot s)$ (дистрибутивность);

(b) $(r+s)\cdot t=(r\cdot t)+(s\cdot t)$ (дистрибутивность);

(c) $(t\cdot r)\cdot s=t\cdot(r\cdot s)$ (ассоциативность умножения);

(d) $t+s=r+s\supset t=r$ (правило сокращения для $+$).

Доказательство.

(a) Индукцией по z доказать $\vdash x\cdot(y+z)=(x\cdot y)+(x\cdot z)$.

(b) Следует из (a) с помощью предложения 3.2 (n).

(c) Индукцией по z доказать $\vdash (x\cdot y)\cdot z=x\cdot(y\cdot z)$.

(d) Индукцией по z, с использованием (S4′), доказать $\vdash x+z=y+z\supset x=y$.

Термы 0, 0′, 0″, 0‴, ... мы в дальнейшем будем называть цифрами и обозначать, как обычно, 0, $\bar{1}$, $\bar{2}$, $\bar{3}$, ... И вообще, для любого целого

неотрицательного n соответствующую цифру $0'''\cdots'$, т. е. 0 с n штрихами, будем обозначать через $\bar{n}$. Цифры можно определить рекурсивно: 0 есть цифра; если u — цифра, то и u' — цифра.

Предложение 3.5.

(a) $\vdash t + \bar{1} = t'$;
(b) $\vdash t \cdot \bar{1} = t$;
(c) $\vdash t \cdot \bar{2} = t + t$ (и т. д. для $\bar{3}$, $\bar{4}$, ...);
(d) $\vdash t + s = 0 \supset t = 0 \,\&\, s = 0$;
(e) $\vdash t \neq 0 \supset (s \cdot t = 0 \supset s = 0)$;
(f) $\vdash t + s = \bar{1} \supset (t = 0 \,\&\, s = \bar{1}) \vee (t = \bar{1} \,\&\, s = 0)$;
(g) $\vdash t \cdot s = \bar{1} \supset (t = \bar{1} \,\&\, s = \bar{1})$;
(h) $\vdash t \neq 0 \supset \exists y\,(t = y')$;
(i) $\vdash s \neq 0 \supset (t \cdot s = r \cdot s \supset t = r)$;
(j) $\vdash t \neq 0 \supset (t \neq \bar{1} \supset \exists y\,(t = y''))$.

Доказательство.

(a)
1. $t + 0' = (t + 0)'$ (S6′)
2. $t + 0 = t$ (S5′)
3. $(t + 0)' = t'$ 2, (S2′)
4. $t + 0' = t'$ 1, 3, предложение 3.2(c)
5. $t + \bar{1} = t'$ 4, определение цифры $\bar{1}$

(b)
1. $t \cdot 0' = t \cdot 0 + t$ (S8′)
2. $t \cdot 0 = 0$ (S7′)
3. $(t \cdot 0) + t = 0 + t$ 2, предложение 3.2(e)
4. $t \cdot 0' = 0 + t$ 1, 3, предложение 3.2(c)
5. $0 + t = t$ предложение 3.2(f),(b)
6. $t \cdot 0' = t$ 4, 5, предложение 3.2(c)
7. $t \cdot \bar{1} = t$ 6, определение цифры $\bar{1}$

(c)
1. $t \cdot \bar{1}' = (t \cdot \bar{1}) + t$ (S8′)
2. $t \cdot \bar{1} = t$ (b)
3. $(t \cdot \bar{1}) + t = t + t$ 2, предложение 3.2(e)
4. $t \cdot \bar{1}' = t + t$ 1, 3, предложение 3.2(c)
5. $t \cdot \bar{2} = t + t$ 4, определение цифры $\bar{2}$

(d) Обозначим через $\mathscr{A}(y)$ формулу $x + y = 0 \supset x = 0 \;\&\; y = 0$. Легко показать, что $\vdash \mathscr{A}(0)$. В силу (S3′), $\vdash (x + y)' \neq 0$. Отсюда на основании (S6′) получаем $\vdash x + y' \neq 0$. Следовательно, в силу тавтологии $\neg A \supset (A \supset B)$, $\vdash \mathscr{A}(y')$ и далее, в силу тавтологии $A \supset (B \supset A)$, получаем $\vdash \mathscr{A}(y) \supset \mathscr{A}(y')$. Применив теперь правило индукции,

получим $\vdash \forall y\, \mathscr{A}(y)$, а затем с помощью правил Gen и A4 и утверждение (d).

(e) Доказывается аналогично (d). Предоставляется в качестве упражнения читателю.

(f) Доказывается индукцией по y в формуле

$$x + y = \bar{1} \supset ((x = 0 \,\&\, y = \bar{1}) \vee (x = \bar{1} \,\&\, y = 0)).$$

(g) Индукция по y в $x \cdot y = \bar{1} \supset (x = \bar{1} \,\&\, y = \bar{1})$.

(h) Провести индукцию по x в $x \neq 0 \supset \exists w\, (x = w')$.

(i) Пусть $\mathscr{A}(y)$ есть формула

$$\forall x\, (z \neq 0 \supset (x \cdot z = y \cdot z \supset x = y)).$$

(i)	1.	$z \neq 0$	гипотеза
	2.	$x \cdot z = 0 \cdot z$	гипотеза
	3.	$0 \cdot z = 0$	предложение 3.2(l)
	4.	$x \cdot z = 0$	2, 3, предложение 3.2(c)
	5.	$x = 0$	1, 4, (e)
	6.	$z \neq 0 \supset (x \cdot z = 0 \cdot z \supset x = 0)$	1—5, теорема дедукции
	7.	$\forall x\, (z \neq 0 \supset (x \cdot z = 0 \cdot z \supset x = 0))$ т. е. $\vdash \mathscr{A}(0)$.	6, Gen
(ii)	1.	$\forall x\, (z \neq 0 \supset (x \cdot z = y \cdot z \supset x = y))$	гипотеза ($\mathscr{A}(y)$)
	2.	$z \neq 0$	гипотеза
	3.	$x \cdot z = y' \cdot z$	гипотеза
	4.	$y' \neq 0$	(S3′), предложение 3.2(b)
	5.	$y' \cdot z \neq 0$	2, 4, (e), тавтология
	6.	$x \cdot z \neq 0$	3, 5, (S1′), тавтологии
	7.	$x \neq 0$	6, (S7′), предложение 3.2(o), (e), тавтологии
	8.	$\exists w\, (x = w')$	7, (h)
	9.	$x = w'$	8, правило C
	10.	$w' \cdot z = y' \cdot z$	3, 9, свойство (7) равенства
	11.	$w \cdot z + z = y \cdot z + z$	10, предложение 3.2 (m), (d)
	12.	$w \cdot z = y \cdot z$	11, предложение 3.4 (d)

13. $z \neq 0 \supset ((w \cdot z = y \cdot z) \supset (w = z))$	1, правило A4
14. $w \cdot z = y \cdot z \supset w = y$	2, 13, MP
15. $w = y$	12, 14, MP
16. $w' = y'$	15, (S2′)
17. $x = y'$	9, 16, предложение 3.2 (c)
18. $\mathscr{A}(y),\ z \neq 0,\ x \cdot z = y' \cdot z \vdash x = y'$	1—17, предложение 2.23
19. $\mathscr{A}(y) \vdash z \neq 0 \supset (x \cdot z = y' \cdot z \supset x = y')$	18, теорема дедукции (дважды)
20. $\mathscr{A}(y) \vdash \forall x\,(z \neq 0 \supset \supset (x \cdot z = y' \cdot z \supset x = y'))$	19, Gen
21. $\vdash \mathscr{A}(y) \supset \mathscr{A}(y')$	20, теорема дедукции

Теперь к (i) и (ii) применяем правило индукции, чтобы получить $\vdash \forall y\, \mathscr{A}(y)$, после чего доказательство завершаем с помощью правил Gen и A4.

Доказательство (j) предоставляем читателю в качестве упражнения.

Предложение 3.6. (a) *Для любых натуральных* m *и* n, *если* $m \neq n$, *то* $\vdash \overline{m} \neq \overline{n}$. *Кроме того* $\vdash \overline{m+n} = \overline{m} + \overline{n}$ *и* $\vdash \overline{m \cdot n} = \overline{m} \cdot \overline{n}$. (b) *Всякая модель* S *бесконечна.* (c) *Каково бы ни было кардинальное число* $\aleph_\beta$, S *имеет нормальную модель мощности* $\aleph_\beta$.

Доказательство. (a) Допустим, что $m \neq n$. Тогда $m < n$ или $n < m$; пусть для определенности $m < n$.

1. $\overline{m} = \overline{n}$	гипотеза
2. $0\overbrace{'\ldots'}^{m\text{ раз}} = 0\overbrace{'\ldots'}^{n\text{ раз}}$	1, определение цифр $\overline{m}$, $\overline{n}$

3. Применяем m раз (S4′):

$$0 = 0\overbrace{'\ldots'}^{n-m\text{ раз}}.$$

Обозначим $\overline{n-m-1}$ через t. Так как $m < n$, то $n - m - 1 \geqslant 0$. Поэтому $0 = t'$.

4. $0 \neq t'$	(S3′)
5. $0 = t' \,\&\, 0 \neq t'$	3, 4, тавтология
6. $\vdash \overline{m} = \overline{n} \supset (0 = t' \,\&\, 0 \neq t')$	1—5, теорема дедукции
7. $\vdash \overline{m} \neq \overline{n}$	6, тавтология

Аналогичное рассуждение можно провести для случая $m < n$. Теперь индукцией по n в метаязыке мы можем доказать и $\vdash \overline{m+n} = \overline{m} + \overline{n}$. Во-первых, $\overline{m+0}$ есть $\overline{m}$. Следовательно, по (S5′), $\vdash \overline{m+0} = \overline{m} + 0$. Предположим, что $\vdash \overline{m+n} = \overline{m} + \overline{n}$. Тогда, в силу (S2′) и (S6′),

$\vdash (\overline{m+n})' = \bar{m} + (\bar{n})'$. Но $\overline{m+(n+1)}$ есть $(\overline{m+n})'$ и $\overline{n+1}$ есть $(\bar{n})'$, следовательно, $\vdash \overline{m+(n+1)} = \bar{m} + \overline{n+1}$. Подобным же образом индукцией по n в метаязыке нетрудно доказать и $\vdash \overline{m \cdot n} = \bar{m} \cdot \bar{n}$.

(b) В силу доказанного только что пункта (a), во всякой модели теории S объекты, соответствующие различным цифрам, должны быть различны, всех же цифр имеется счетное множество.

(c) Это утверждение следует из следствия 2.35(c) и из того факта, что стандартная модель является бесконечной нормальной моделью.

Отношение порядка в S можно ввести следующим образом.

Определения

$t < s$ означает $\exists w\,(w \neq 0 \,\&\, t + w = s)$,
$t \leqslant s$ означает $t < s \vee t = s$,
$t > s$ означает $s < t$,
$t \geqslant s$ означает $s \leqslant t$,
$t \not< s$ означает $\neg(t < s)$ и т. д.

Чтобы первое из этих определений было корректным, можно, например, считать, что w — это первая предметная переменная, которая не входит в термы t и s.

Предложение 3.7. *Каковы бы ни были термы t, r и s, следующие формулы выводимы в* S:

(a) $t \not< t$;
(b) $t < s \supset (s < r \supset t < r)$;
(c) $t < s \supset s \not< t$;
(d) $t < s \equiv t + r < s + r$;
(e) $t \leqslant t$;
(f) $t \leqslant s \supset (s \leqslant r \supset t \leqslant r)$;
(g) $t \leqslant s \supset (t + r \leqslant s + r)$;
(h) $t \leqslant s \supset (s < r \supset t < r)$.
(i) $0 \leqslant t$;
(j) $0 < t'$;
(k) $t < r \equiv t' \leqslant r$;
(l) $t \leqslant r \equiv t < r'$;
(m) $t < t'$;
(n) $(0 < \bar{1}) \,\&\, (\bar{1} < \bar{2}) \,\&\, (\bar{2} < \bar{3}) \,\&\, \ldots$;
(o) $t \neq r \supset (t < r \vee r < t)$;
(o′) $t = r \vee t < r \vee r < t$;
(p) $t \leqslant r \vee r \leqslant t$;
(q) $t + r \geqslant t$;
(r) $r \neq 0 \supset t + r > t$;
(s) $r \neq 0 \supset t \cdot r \geqslant t$;
(t) $r \neq 0 \equiv r > 0$;
(u) $r > 0 \supset (t > 0 \supset r \cdot t > 0)$;
(v) $r \neq 0 \supset (t > \bar{1} \supset t \cdot r > r)$;
(w) $r \neq 0 \supset (t < s \equiv t \cdot r < s \cdot r)$;
(x) $r \neq 0 \supset (t \leqslant s \equiv t \cdot r \leqslant s \cdot r)$;
(y) $t \not< 0$;
(z) $t \leqslant r \,\&\, r \leqslant t \supset t = r$.

Доказательство.

(a) Следует из предложения 3.4(d).

(b) 1. $t < s$ гипотеза
2. $s < r$ гипотеза

3. $\exists w\,(w \neq 0 \,\&\, t + w = s)$	1, определение
4. $\exists v\,(v \neq 0 \,\&\, s + v = r)$	2, определение и, возможно, переименование связанных переменных
5. $w \neq 0 \,\&\, t + w = s$	3, правило С
6. $v \neq 0 \,\&\, s + v = r$	4, правило С
7. $t + w = s$	5, тавтология
8. $s + v = r$	6, тавтология
9. $(t + w) + v = r$	7, 8, предложение 3.2(e)
10. $t + (w + v) = r$	9, предложение 3.2(j)
11. $w \neq 0$	5, тавтология
12. $v \neq 0$	6, тавтология
13. $w + v \neq 0$	11, 12, предложение 3.5(d), тавтология
14. $w + v \neq 0 \,\&\, t + (w + v) = r$	10, 13, тавтология
15. $\exists u\,(u \neq 0 \,\&\, t + u = r)$	14, правило Е4
16. $t < r$	15, определение
17. $\vdash t < s \supset (s < r \supset t < r)$	1—16, теорема о дедукции, предложение 2.23

Доказательство выводимости формул (c)—(z) оставляется читателю в качестве упражнения.

Теоремы (a)—(z) не расположены в каком-нибудь специальном порядке, если не считать того, что при этом порядке каждая из них может быть выведена более или менее непосредственно из предыдущих.

Предложение 3.8. (a) *Для каждого натурального* k

$$\vdash x = 0 \vee \ldots \vee x = \bar{k} \equiv x \leqslant \bar{k}.$$

(a′) *Для каждого натурального* k *и для всякой формулы* $\mathscr{A}$

$$\vdash \mathscr{A}(0) \,\&\, \ldots \,\&\, \mathscr{A}(\bar{k}) \equiv \forall x\,(x \leqslant \bar{k} \supset \mathscr{A}(x)).$$

(b) *Для каждого натурального* $k > 0$

$$\vdash x = 0 \vee \ldots \vee x = \overline{k-1} \equiv x < \bar{k}.$$

(b′) *Для каждого натурального* $k > 0$ *и для любой формулы* $\mathscr{A}$

$$\vdash \mathscr{A}(0) \,\&\, \ldots \,\&\, \mathscr{A}(\overline{k-1}) \equiv \forall x\,(x < \bar{k} \supset \mathscr{A}(x)).$$

(c) $\vdash (\forall x\,(x < y \supset \mathscr{A}(x)) \,\&\, \forall x\,(x \geqslant y \supset \mathscr{B}(x))) \supset$
$\supset \forall x\,(\mathscr{A}(x) \vee \mathscr{B}(x))$.

Доказательство. (a) Мы докажем $\vdash x = 0 \vee \ldots \vee x = \bar{k} \equiv x \leqslant \bar{k}$ индукцией по k в метаязыке. В случае $k = 0$ утверждение $\vdash x = 0 \equiv x \leqslant 0$ легко следует из определений и предложения 3.7. Предположим, что $\vdash x = 0 \vee \ldots \vee x = \bar{k} \equiv x \leqslant \bar{k}$. Пусть теперь

$x=0 \vee \ldots \vee x=\bar{k} \vee x=\overline{k+1}$. Но $x=\overline{k+1} \supset x \leqslant \overline{k+1}$ и, кроме того, $x=0 \vee \ldots \vee x=\bar{k} \supset x \leqslant \bar{k}$ и $x \leqslant \bar{k} \supset x \leqslant \overline{k+1}$. Следовательно, $x=0 \vee \ldots \vee x=\overline{k+1} \supset x \leqslant \overline{k+1}$. Предположим теперь, что $x \leqslant \overline{k+1}$; тогда $x=\overline{k+1}$ или $x<\overline{k+1}$. Если $x=\overline{k+1}$, то $x=0 \vee \ldots \vee x=\overline{k+1}$. Если же $x<\overline{k+1}$, то, так как $\overline{k+1}$ есть $(\bar{k})'$, мы имеем $x \leqslant \bar{k}$, по предположению 3.7 (1), откуда, в силу индуктивного предположения, $x=0 \vee \ldots \vee x=\bar{k}$ и, наконец, $x=0 \vee \ldots \vee x=\overline{k+1}$. (Мы сейчас доказали пункт (a) предложения 3.8 неформально. Мы и в дальнейшем будем иногда так поступать. В проведенном только что доказательстве неявно используются теорема дедукции, элиминируемость правила C, теорема о замене (следствие 2.21), а также ряд тавтологий).

Пункты (a′), (b) и (b′) легко следуют из (a). Пункт (c) вытекает почти непосредственно из предложения 3.7 (o) с помощью очевидных тавтологий.

Теперь мы можем вывести некоторые более сильные формы принципа индукции.

Предложение 3.9.

(a) (Полная индукция.)

$$\vdash \forall x (\forall z (z<x \supset \mathscr{A}(z)) \supset \mathscr{A}(x)) \supset \forall x \mathscr{A}(x).$$

(*Пусть свойство* P *таково, что для любого натурального числа* x *из того, что этим свойством обладают все натуральные числа, меньшие* x, *вытекает, что им обладает и число* x. *Тогда свойством* P *обладают все натуральные числа.*).

(b) (Принцип наименьшего числа.)

$$\vdash \mathscr{A}(x) \supset \exists y (\mathscr{A}(y) \,\&\, \forall z (z<y \supset \neg \mathscr{A}(z))).$$

(*Если свойством* P *обладает хотя бы одно натуральное число, то среди всех натуральных чисел, обладающих свойством* P, *существует наименьшее.*).

Доказательство. (a) Обозначим формулу $\forall z (z \leqslant x \supset \mathscr{A}(z))$ через $\mathscr{B}(x)$.

(i)	1.	$\forall x (\forall z (z<x \supset \mathscr{A}(z)) \supset \mathscr{A}(x))$	гипотеза
	2.	$\forall z (z<0 \supset \mathscr{A}(z)) \supset \mathscr{A}(0)$	1, правило A4
	3.	$z \not< 0$	предложение 3.7 (y)
	4.	$\forall z (z<0 \supset \mathscr{A}(z))$	3, тавтология, Gen
	5.	$\mathscr{A}(0)$	4, 2, MP
	6.	$\forall z (z \leqslant 0 \supset \mathscr{A}(z))$ т. е. $\mathscr{B}(0)$	5, предложение 3.8(a′)
	7.	$\forall x (\forall z (z<x \supset \mathscr{A}(z)) \supset \mathscr{A}(x)) \vdash \mathscr{B}(0)$	1—6

(ii)	1. $\forall x\,(\forall z\,(z<x \supset \mathscr{A}(z)) \supset \mathscr{A}(x))$	гипотеза
	2. $\mathscr{B}(x)$, т. е. $\forall z\,(z \leqslant x \supset \mathscr{A}(z))$	гипотеза
	3. $\forall z\,(z<x' \supset \mathscr{A}(z))$	2, предложение 3,7(l)
	4. $\forall z\,(z<x' \supset \mathscr{A}(z)) \supset \mathscr{A}(x')$	1, правило A4
	5. $\mathscr{A}(x')$	3, 4, MP
	6. $z \leqslant x' \supset z<x' \vee z=x'$	определение, тавтология
	7. $z<x' \supset \mathscr{A}(z)$	3, правило A4
	8. $z=x' \supset \mathscr{A}(z)$	5, аксиома (7) равенства
	9. $\forall z\,(z \leqslant x' \supset \mathscr{A}(z))$, т. е. $\mathscr{B}(x')$	6, 7, 8, тавтология, Gen
	10. $\forall x\,(\forall z\,(z<x \supset \mathscr{A}(z)) \supset \supset \mathscr{A}(x)) \vdash \forall x\,(\mathscr{B}(x) \supset \mathscr{B}(x'))$	1—9, теорема дедукции, Gen

Из (i), (ii) по правилу индукции получаем $\mathscr{C} \vdash \forall x\,\mathscr{B}(x)$, т. е. $\mathscr{C} \vdash \forall x\,\forall z\,(z \leqslant x \supset \mathscr{A}(z))$, где $\mathscr{C}$ есть формула $\forall x\,(\forall z\,(z<x \supset \supset \mathscr{A}(z)) \supset \mathscr{A}(x))$. Дважды применив правило A4, получим $\mathscr{C} \vdash x \leqslant x \supset \mathscr{A}(x)$; но так как $\vdash x \leqslant x$, то $\mathscr{C} \vdash \mathscr{A}(x)$, откуда, по правилу Gen и теореме дедукции, окончательно имеем $\vdash \mathscr{C} \supset \forall x\,\mathscr{A}(x)$.

(b)	1. $\neg \exists y\,(\mathscr{A}(y) \& \forall z\,(z<y \supset \neg \mathscr{A}(z)))$	гипотеза
	2. $\forall y \neg (\mathscr{A}(y) \& \forall z\,(z<y \supset \neg \mathscr{A}(z)))$	1, тавтология
	3. $\forall y\,(\forall z\,(z<y \supset \neg \mathscr{A}(z)) \supset \neg \mathscr{A}(y))$	2, тавтология
	4. $\forall y \neg \mathscr{A}(y)$	3, (a) с $\neg \mathscr{A}$ вместо $\mathscr{A}$
	5. $\neg \mathscr{A}(x)$	4, правило A4
	6. $\neg \exists y\,(\mathscr{A}(y) \& \forall z\,(z<y \supset \neg \mathscr{A}(z))) \supset \supset \neg \mathscr{A}(x)$	1—5, теорема дедукции
	7. $\mathscr{A}(x) \supset \exists y\,(\mathscr{A}(y) \supset \forall z\,(z<y \supset \supset \neg \mathscr{A}(z)))$	6, тавтология

Упражнение

Показать, что

$$\vdash \forall x\,(\mathscr{A}(x) \supset \exists y\,(y<x \& \mathscr{A}(y))) \supset \forall x \neg \mathscr{A}(x)$$

(*метод бесконечного спуска*).

Следующим важным арифметическим понятием, которое мы теперь определим, является понятие делимости.

Определение. $t \mid s$ служит сокращением для $\exists z\,(s=t \cdot z)$, где z — первая переменная, не входящая в t и s.

Предложение 3.10. *Следующие формулы выводимы в* S:

(a) $t \mid t$;
(b) $\bar{1} \mid t$;
(c) $t \mid 0$;
(d) $t \mid s \,\&\, s \mid r \supset t \mid r$;
(e) $s \neq 0 \,\&\, t \mid s \supset t \leqslant s$;
(f) $t \mid s \,\&\, s \mid t \supset s = t$;
(g) $t \mid s \supset t \mid r \cdot s$;
(h) $t \mid s \,\&\, t \mid r \supset t \mid s + r$.

Доказательство. (a) $t = t \cdot \bar{1}$. Следовательно, $t \mid t$.

(b) $t = \bar{1} \cdot t$. Следовательно, $\bar{1} \mid t$.

(c) $0 = t \cdot 0$, поэтому $t \mid 0$.

(d) Если $s = t \cdot z$ и $r = s \cdot w$, то $r = t \cdot (z \cdot w)$.

(e) Если $s \neq 0$ и $t \mid s$, то $s = t \cdot z$ для некоторого z, при этом, очевидно, $z \neq 0$, т. е. $z = u'$ для некоторого u. Итак, $s = t \cdot (u') = t \cdot u + t \geqslant t$.

Читатель легко докажет выводимость и остающихся формул (f)—(h).

Упражнение

Доказать:

1. $\vdash t \mid \bar{1} \supset t = \bar{1}$. **2.** $\vdash (t \mid s \supset t \mid s') \supset t = \bar{1}$.

Для дальнейших целей полезно будет доказать единственность частного и остатка при делении одного числа на другое.

Предложение 3.11. $\vdash y \neq 0 \supset \exists_1 u \exists_1 v (x = y \cdot u + v \,\&\, v < y)$.

Доказательство. Обозначим через $\mathscr{A}(x)$ формулу

$$y \neq 0 \supset \exists u \exists v (x = y \cdot u + v \,\&\, v < y).$$

(i)	1.	$y \neq 0$	гипотеза
	2.	$0 = y \cdot 0 + 0$	(S 5′), (S 7′)
	3.	$0 < y$	1, предложение 3.7 (t)
	4.	$0 = y \cdot 0 + 0 \,\&\, 0 < y$	2, 3, тавтология
	5.	$\exists u \exists v (0 = y \cdot u + v \,\&\, v < y)$	4, правило E4
	6.	$y \neq 0 \supset \exists u \exists v (0 = y \cdot u + v \,\&\, v < y)$	1—5, теорема дедукции
(ii)	1.	$\mathscr{A}(x)$, т. е. $y \neq 0 \supset \exists u \exists v (x = y \cdot u + v \,\&\, v < y)$	гипотеза
	2.	$y \neq 0$	гипотеза
	3.	$\exists u \exists v (x = y \cdot u + v \,\&\, v < y)$	1, 2, MP
	4.	$x = y \cdot a + b \,\&\, b < y$	3, правило C дважды
	5.	$b < y$	4, тавтология
	6.	$b' \leqslant y$	5, предложение 3.7 (k)

7. $b' < y \vee b' = y$	6, определение
8. $b' < y \supset x' = y \cdot a + b' \,\&\, b' < y$	4, (S 6′)
9. $b' < y \supset \exists u \exists v (x' = y \cdot u + v \,\&\, v < y)$	8, правило E4, теорема дедукции
10. $b' = y \supset x' = y \cdot a + y \cdot \bar{1}$	4, (S 6′), предложение 3.5 (b)
11. $b' = y \supset (x' = y \cdot (a + \bar{1}) + 0 \,\&\, 0 < y)$	10, предложение 3.4, 2, предложение 3.7 (t), (S5′)
12. $b' = y \supset \exists u \exists v (x' = y \cdot u + v \,\&\, v < y)$	11, теорема дедукции, правило E4
13. $\exists u \exists v (x' = y \cdot u + v \,\&\, v < y)$	7, 9, 12, тавтология
14. $\mathscr{A}(x) \supset (y \neq 0 \supset \exists u \exists v (x' = y \cdot u + v \,\&\, v < y))$ т. е. $\mathscr{A}(x) \supset \mathscr{A}(x')$	1—13, теорема дедукции

Из (i) и (ii) по правилу индукции получаем $\vdash \forall x \mathscr{A}(x)$.

Таким образом, мы доказали существование частного u и остатка v. Докажем теперь единственность частного и остатка. Пусть $y \neq 0$. Допустим, что $x = y \cdot u_1 + v_1 \,\&\, v_1 < y$ и $x = y \cdot u_2 + v_2 \,\&\, v_2 < y$. Возможны случаи: $u_1 = u_2$, $u_1 < u_2$ и $u_2 < u_1$. Если $u_1 = u_2$, то, в силу предложения 3.4 (d), $v_1 = v_2$. Если $u_1 < u_2$, то при некотором $w \neq 0$ имеем $u_2 = u_1 + w$ и тогда $y \cdot u_1 + v_1 = y \cdot (u_1 + w) + v_2 = y \cdot u_1 + y \cdot w + v_2$, откуда $v_1 =$, $= y \cdot w + v_2$. Но так как $w \neq 0$, то тогда $y \cdot w \geqslant y$ и, следовательно, $v_1 = y \cdot w + v_2 \geqslant y$, чего не может быть из-за $v_1 < y$. Таким образом, $u_1 \not< u_2$. Аналогично доказывается, что $u_2 \not< u_1$. Поэтому $u_1 = u_2$, а следовательно, и $v_1 = v_2$.

После всего сделанного нет никаких принципиальных препятствий к тому, чтобы всякую теорему, доказываемую в курсах элементарной теории чисел (например, в книге Виноградова [1952]), перевести на язык теории S и построить вывод такого перевода в этой теории. Имеются некоторые теоретико-числовые функции такие, как, например, $x!$ и x^y, которые можно определить в S, и мы это сделаем ниже в этой главе. (В большинстве случаев можно, правда, обойтись без явного определения этих функций, но это очень скоро приводит к громоздким и запутанным построениям.) С другой стороны, некоторые классические результаты теории чисел такие, как теорема Дирихле, доказаны с помощью теории функций комплексного переменного, причем зачастую неизвестно даже, можно ли получить элементарные доказательства (или выводы в S) для таких теорем. Некоторые же теоремы теории чисел (например, теорема о простых числах) в самих формулировках содержат

неэлементарные понятия, вроде понятия логарифмической функции, и такие теоремы не могут быть даже сформулированы на языке теории S, если только для них не существует эквивалентной элементарной формы. Позже вопрос о силе и выразительных возможностях теории S будет рассмотрен подробнее. Будет, например, доказано, что существуют такие замкнутые формулы, которые недоказуемы и неопровержимы в теории S, если только она непротиворечива; следовательно, существует формула, истинная в стандартной интерпретации, но невыводимая в S. Мы увидим также, что такая неполнота теории S не может быть отнесена за счет нехватки каких-то существенных аксиом и что в основе этого явления кроются более глубокие причины, действующие также и в случае других теорий.

Упражнения

1. Показать, что принцип индукции (S9) не зависит от остальных аксиом теории S. (Указание. Рассмотреть интерпретацию, областью которой служит множество полиномов с целыми коэффициентами и с неотрицательным старшим коэффициентом и в которой операции $+$ и $\cdot$ интерпретируются как обычные сложение и умножение полиномов. Проверить истинность в такой интерпретации аксиом (S1) — (S8) и опровергнуть предложение 3.11, подставляя вместо x полином x и вместо y — полином 2.)

[D]**2.** Существует нестандартная модель теории S любой мощности $\aleph_\alpha$. (Указание. Построить новую теорию S', присоединив к S новую предметную константу b и аксиомы $b \neq 0$, $b \neq \bar{1}$, ..., $b \neq \bar{n}$, ... Показать, что теория S' непротиворечива, и применить предложение 2.27 и следствие 2.35 (c).) Эренфойхт [1958] доказал, что существует по меньшей мере $2^{\aleph_\alpha}$ неизоморфных моделей мощности $\aleph_\alpha$.

[D]**3.** Для системы аксиом Пеано дать обычное математическое доказательство ее категоричности в смысле изоморфности всяких двух ее «моделей». Объяснить, почему такое доказательство не применимо к теории первого порядка S.

[D]**4.** (Пресбургер [1929].) Если удалить из теории S функциональную букву f_2^2 для умножения и аксиомы (S7) — (S8), то полученная таким образом новая теория S_+ полна и разрешима. (Указание. Использовать процедуру сведения, подобную той, что применялась для теории K_2 на стр. 107 — 108. Для любого k определим $k \cdot t$ по индукции: $0 \cdot t$ есть 0, $(k+1) \cdot t$ есть $(k \cdot t) + t$, т. е. $k \cdot t$ есть сумма k слагаемых, каждое из которых есть t. Пусть также $t \equiv s \pmod{k}$ при каждом k служит сокращением для $\exists x (t = s + k \cdot x \vee s = t + k \cdot x)$. При сведении будем обращаться с формулами вида $t \equiv s \pmod{k}$ и $t < s$ как с элементарными (хотя на самом деле они таковыми, разумеется, не являются). Относительно всякой формулы теории S_+ мы заранее можем предполагать, что она уже приведена к предваренной нормальной форме. Теперь остается описать процедуру, следуя которой, по каждой формуле $\exists y \mathscr{C}$, где $\mathscr{C}$ не содержит кванторов, строится эквивалентная ей формула, не содержащая кванторов (не забывая при этом о том, что элементарными формулами сейчас считаются формулы вида $t \equiv s \pmod{k}$ и $t < s$). Дальнейшую помощь в деталях читатель получит у Гильберта и Бернайса [1934], т. I, стр. 359 — 366.)

5. (a) Всякая замкнутая элементарная формула $t = s$ теории S разрешима в S, т. е. либо $\vdash_S t = s$, либо $\vdash_S t \neq s$.

b) Всякая замкнутая формула теории S, не содержащая кванторов, разрешима в S.

§ 2. Арифметические функции и отношения

Арифметическими функциями мы называем функции, у которых область определения и множество значений состоят из натуральных чисел, а арифметическим отношением является всякое отношение, заданное на множестве натуральных чисел. Так, например, умножение есть арифметическая функция с двумя аргументами, а выражение $x + y < z$ определяет некоторое арифметическое отношение с тремя аргументами. Арифметические функции и отношения являются понятиями интуитивными и не связаны ни с какой формальной системой.

Арифметическое отношение $R(x_1, \ldots, x_n)$ называется *выразимым* в теории S, если существует формула $\mathscr{A}(x_1, \ldots, x_n)$ теории S с n свободными переменными такая, что для любых натуральных чисел $k_1, \ldots, k_n$

(1) если $R(k_1, \ldots, k_n)$ истинно, то $\vdash_S \mathscr{A}(\bar{k}_1, \ldots, \bar{k}_n)$,

(2) если $R(k_1, \ldots, k_n)$ ложно, то $\vdash_S \neg\mathscr{A}(\bar{k}_1, \ldots, \bar{k}_n)$.

Так, например, отношение равенства между натуральными числами выразимо в S формулой $x_1 = x_2$. В самом деле, если $k_1 = k_2$, то термы $\bar{k}_1$ и $\bar{k}_2$ совпадают, и тогда, по предложению 3.2 (a), $\vdash_S \bar{k}_1 = \bar{k}_2$. Аналогично, если $k_1 \neq k_2$, то, в силу предложения 3.6 (a), $\vdash_S \bar{k}_1 \neq \bar{k}_2$. В свою очередь формулой $x_1 < x_2$ выразимо в S отношение «меньше». Если $k_1 < k_2$, то существует отличное от нуля число n такое, что $k_2 = k_1 + n$, и тогда, в силу предложения 3.6 (a), $\vdash_S \bar{k}_2 = \bar{k}_1 + \bar{n}$, а в силу (S3′) и $n \neq 0$, $\vdash_S \bar{n} \neq 0$. Следовательно, в S можно вывести формулу $\exists w(\bar{k}_2 = \bar{k}_1 + w \,\&\, w \neq 0)$, т. е. $\bar{k}_1 < \bar{k}_2$. Если же $k_1 \not< k_2$, то $k_1 = k_2$ или $k_2 < k_1$, причем в этом последнем случае, так же как и для случая $k_1 < k_2$, доказывается $\vdash_S \bar{k}_2 < \bar{k}_1$. Наконец, если $k_1 = k_2$, то $\vdash_S \bar{k}_1 = \bar{k}_2$. Итак, в обоих случаях $\vdash_S \bar{k}_2 \leqslant \bar{k}_1$ и тогда, по предложению 3.7 (a), (c), $\vdash_S \bar{k}_1 \not< \bar{k}_2$.

Упражнения

1. Показать, что отрицание, конъюнкция и дизъюнкция выразимых в S отношений выразимы в S.

2. Доказать, что отношение $x + y = z$ выразимо в S.

Арифметическая функция $f(x_1, \ldots, x_n)$ называется *представимой* в S, если существует формула $\mathscr{A}(x_1, \ldots, x_{n+1})$ теории S со свободными переменными $x_1, \ldots, x_{n+1}$ такая, что для любых натуральных чисел $k_1, \ldots, k_{n+1}$

(1) если $f(k_1, \ldots, k_n) = k_{n+1}$, то $\vdash_S \mathscr{A}(\bar{k}_1, \ldots, \bar{k}_n, \bar{k}_{n+1})$,

(2) $\vdash_S \exists_1 x_{n+1} \mathscr{A}(\bar{k}_1, \ldots, \bar{k}_n, x_{n+1})$.

Если в этом определении условие (2) заменить условием

(2′) $\vdash_S \exists_1 x_{n+1} \mathscr{A}(x_1, \ldots, x_n, x_{n+1})$,

то мы получим понятие *сильно представимой* в S функции. Заметим, что, в силу правил Gen и A4, из (2′) следует (2). Следовательно, всякая сильно представимая функция является также представимой функцией.

Примеры. (a) Нуль-функция $Z(x) = 0$ сильно представима в S с помощью формулы $x_1 = x_1 \& x_2 = 0$. В самом деле, если $Z(k_1) = k_2$, то $k_2 = 0$ и $\vdash \bar{k}_1 = \bar{k}_1 \& 0 = 0$, т. е. выполнен пункт (1) определения сильно представимой функции. Кроме того, очевидно, $\vdash \exists_1 x_2 (x_1 = x_1 \& x_2 = 0)$, т. е. выполнен и пункт (2′) этого определения.

(b) Функция $N(x) = x + 1$ сильно представима в S формулой $x_2 = x_1'$. Действительно, при любом k_1 из $N(k_1) = k_2$, т. е. из $k_2 = k_1 + 1$, следует, что термы $\bar{k}_2$ и $(\bar{k}_1)'$ совпадают и потому $\vdash \bar{k}_2 = (\bar{k}_1)'$. Кроме того, $\vdash \exists_1 x_2 (x_2 = x_1')$.

(c) Проектирующая функция $U_i^n(x_1, \ldots, x_n) = x_i$ сильно представима в S с помощью формулы $x_1 = x_1 \& \ldots \& x_n = x_n \& x_{n+1} = x_i$. Если $U_i^n(k_1, \ldots, k_n) = k_{n+1}$, то $k_{n+1} = k_i$ и $\bar{k}_{n+1} = \bar{k}_i$. Следовательно, $\vdash \bar{k}_1 = \bar{k}_1 \& \ldots \& \bar{k}_n = \bar{k}_n \& \bar{k}_{n+1} = k_i$, и условие (1) выполнено. Кроме того, $\vdash \exists_1 x_{n+1} (x_1 = x_1 \& \ldots \& x_n = x_n \& x_{n+1} = x_i)$, т. е. выполнено и условие (2′) определения сильно представимой в S функции.

(d) Предположим, что функции $g(x_1, \ldots, x_m)$, $h_1(x_1, \ldots, x_n)$, $\ldots$, $h_m(x_1, \ldots, x_n)$ (сильно) представимы в S соответственно формулами $\mathscr{B}(x_1, \ldots, x_m, x_{m+1})$, $\mathscr{A}_1(x_1, \ldots, x_{n+1})$, $\ldots$, $\mathscr{A}_m(x_1, \ldots, x_{n+1})$. Зададим новую функцию f равенством $f(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n))$. Говорят, что функция f получена из g, $h_1, \ldots, h_n$ с помощью подстановки. Функция f также (сильно) представима в S, например, с помощью формулы

$$\exists y_1 \ldots \exists y_m (\mathscr{A}_1(x_1, \ldots, x_n, y_1) \& \ldots \& \mathscr{A}_m(x_1, \ldots, x_n, y_m) \& \mathscr{B}(y_1, \ldots, y_m, x_{n+1})),$$

которую обозначим через $\mathscr{A}(x_1, x_2, \ldots, x_{n+1})$. В самом деле, пусть $f(k_1, \ldots, k_n) = k_{n+1}$ и $h_i(k_1, \ldots, k_n) = r_i$, где $1 \leqslant i \leqslant m$; тогда $g(r_1, \ldots, r_m) = k_{n+1}$. Согласно предположению о (сильной) представимости g, $h_1, \ldots, h_m$, $\vdash \mathscr{A}_i(\bar{k}_1, \ldots, \bar{k}_n, \bar{r}_i)$ для $1 \leqslant i \leqslant m$ и $\vdash \mathscr{B}(\bar{r}_1, \ldots, \bar{r}_m, \bar{k}_{n+1})$. Следовательно, $\vdash \mathscr{A}(\bar{k}_1, \ldots, \bar{k}_n, \bar{r}_1) \& \ldots \& \mathscr{A}(\bar{k}_1, \ldots, \bar{k}_n, \bar{r}_m) \& \mathscr{B}(\bar{r}_1, \ldots, \bar{r}_m, \bar{k}_{n+1})$. По правилу E4 $\vdash \mathscr{A}(\bar{k}_1, \ldots, \bar{k}_n, \bar{k}_{n+1})$, т. е. выполнено условие (1) определения представимости. Переходя ко второму пункту этого определения, мы остановимся на варианте сильной представимости. Допустим в качестве гипотез

$$\exists y_1 \ldots \exists y_m (\mathscr{A}_1(x_1, \ldots, x_n, y_1) \& \ldots \& \mathscr{A}_m(x_1, \ldots, x_n, y_m) \& \mathscr{B}(y_1, \ldots, y_m, u)) \quad (*)$$

и

$$\exists y_1 \ldots \exists y_m (\mathscr{A}_1(x_1, \ldots, x_n, y_1) \& \ldots \& \mathscr{A}_m(x_1, \ldots, x_n, y_m) \& \mathscr{B}(y_1, \ldots, y_m, v)). \quad (**)$$

Применив m раз правило C, получаем из (*)

$$\mathscr{A}_1(x_1, \ldots, x_n, b_1) \& \ldots \& \mathscr{A}_m(x_1, \ldots, x_n, b_m) \& \mathscr{B}(y_1, \ldots, y_m, u)$$

и из (**)

$$\mathscr{A}_1(x_1, \ldots, x_n, c_1) \& \ldots \& \mathscr{A}_m(x_1, \ldots, x_n, c_m) \& \mathscr{B}(y_1, \ldots, y_m, v).$$

Так как $\vdash \exists_1 x_{n+1} \mathscr{A}_i(x_1, \ldots, x_n, x_{n+1})$, то из $\mathscr{A}_i(x_1, \ldots, x_n, b_i)$ и $\mathscr{A}_i(x_1, \ldots, x_n, c_i)$ следует $b_i = c_i$. Из $\mathscr{B}(b_1, \ldots, b_m, u)$ и $b_1 = c_1, \ldots, b_m = c_m$ следует $\mathscr{B}(c_1, \ldots, c_m, u)$. Поэтому из $\vdash \exists_1 x_{m+1} \mathscr{B}(x_1, \ldots, x_m, x_{m+1})$ и $\mathscr{B}(c_1, \ldots, c_m, v)$ мы получаем $u = v$. Таким образом, $\vdash \mathscr{A}(x_1, \ldots, x_n, u) \& \mathscr{A}(x_1, \ldots, x_n, v) \supset u = v$. Также легко показать, что $\vdash \exists x_{n+1} \mathscr{A}(x_1, \ldots, x_{n+1})$ (предоставляется читателю в качестве упражнения). Отсюда получаем $\vdash \exists_1 x_{n+1} \mathscr{A}(x_1, \ldots, x_n, x_{n+1})$, т. е. утверждение (2′) определения сильной представимости. Вариант (2) для случая представимости рассматривается аналогично.

Упражнение

Показать, что следующие функции сильно представимы в S:

1. $Z_n(x_1, \ldots, x_n) = 0$. (Указание. $Z_n(x_1, \ldots, x_n) = Z(U_1^n(x_1, \ldots, x_n))$, применить (a), (c), (d).)

2. $C_k^n(x_1, \ldots, x_n) = k$ для любого данного k. (Указание. В силу 1, C_0^n сильно представима; допустим, что сильно представима функция C_k^n, тогда используем равенство $C_{k+1}^n(x_1, \ldots, x_n) = N(C_k^n(x_1, \ldots, x_n))$ и (b), (d).)

3. Сложение.

4. Умножение.

Характеристической функцией данного отношения $R(x_1, \ldots, x_n)$ называется функция $C_R(x_1, \ldots, x_n)$, задаваемая условиями:

$$C_R(x_1, \ldots, x_n) = \begin{cases} 0, & \text{если } R(x_1, \ldots, x_n) \text{ истинно,} \\ 1, & \text{если } R(x_1, \ldots, x_n) \text{ ложно.} \end{cases}$$

Предложение 3.12. *Если отношение* $R(x_1, \ldots, x_n)$ *выразимо в* S, *то характеристическая функция* $C_R(x_1, \ldots, x_n)$ *этого отношения сильно представима в* S, *а если функция* $C_R(x_1, \ldots, x_n)$ *представима в* S, *то в* S *выразимо и отношение* $R(x_1, \ldots, x_n)$.

Доказательство. Не составляет труда проверить, что

1) если отношение $R(x_1, \ldots, x_n)$ выразимо в S с помощью формулы $\mathscr{A}(x_1, \ldots, x_n)$, то функция $C_R(x_1, \ldots, x_n)$ сильно представима в S с помощью формулы $(\mathscr{A}(x_1, \ldots, x_n) \& x_{n+1} = 0) \vee (\neg \mathscr{A}(x_1, \ldots, x_n) \& x_{n+1} = 1)$, и 2) если функция $C_R(x_1, \ldots, x_n)$ представима в S с помощью формулы $\mathscr{B}(x_1, \ldots, x_n, x_{n+1})$, то отношение $R(x_1, \ldots, x_n)$ выразимо в S с помощью формулы $\mathscr{B}(x_1, \ldots, x_n, 0)$.

Упражнения

1. Показать, что если функция $f(x_1, \ldots, x_n)$ представима в S, то в S выразимо и отношение $f(x_1, \ldots, x_n) = x_{n+1}$, называемое *представляющим отношением* (или *графиком*) функции f.

2. Доказать, что для всяких двух n-аргументных отношений R_1 и R_2 $C_{\text{не } R_1} = 1 - C_{R_1}$, $C_{(R_1 \text{ или } R_2)} = C_{R_1} \cdot C_{R_2}$, $C_{(R_1 \text{ и } R_2)} = C_{R_1} + C_{R_2} - C_{R_1} \cdot C_{R_2}$.

§ 3. Примитивно рекурсивные и рекурсивные функции

Изучение представимости функций в S приводит к одному классу функций, играющих весьма важную роль в математической логике.

Определение

(1) Следующие функции называются *исходными функциями.*

(I) Нуль-функция: $Z(x) = 0$ при каждом x.

(II) Прибавление единицы: $N(x) = x + 1$ при каждом x.

(III) Проектирующие функции: $U_i^n(x_1, \ldots, x_n) = x_i$ при всех $x, \ldots, x_n$ ($i = 1, \ldots, n$; $n = 1, 2, \ldots$).

(2) Следующие два правила служат для получения новых функций, исходя из уже имеющихся функций.

(IV) *Подстановка:*

$$f(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n));$$

говорят, что функция f получена с помощью подстановки из функций $g(y_1, \ldots, y_m)$, $h_1(x_1, \ldots, x_n)$, $\ldots$, $h_m(x_1, \ldots, x_n)$.

(V) *Рекурсия:*

$$f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n),$$
$$f(x_1, \ldots, x_n, y + 1) = h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)),$$

при этом исключается случай $n = 0$, для которого отдельно:

$f(0) = k$ (где k — фиксированное целое неотрицательное число),

$$f(y + 1) = h(y, f(y)).$$

Мы будем говорить, что функция f получена из функций g и h (или в случае $n = 0$ из одной лишь функции h) с помощью рекурсии, а $x_1, \ldots, x_n$ назовем *параметрами* рекурсии. Заметим, что функция f вполне определена: значение $f(x_1, \ldots, x_n, 0)$ определяется из первого равенства, а если мы уже знаем значение $f(x_1, \ldots, x_n, y)$, то из второго равенства мы можем найти значение $f(x_1, \ldots, x_n, y + 1)$.

(VI) μ-оператор: пусть функция $g(x_1, \ldots, x_n, y)$ такова, что для любых $x_1, \ldots, x_n$ существует по крайней мере одно значение y, при котором $g(x_1, \ldots, x_n, y) = 0$. Обозначим через $\mu y\,(g(x_1, \ldots, x_n, y) = 0)$ наименьшее значение y, при котором $g(x_1, \ldots, x_n, y) = 0$. Вообще, для всякого отношения $R(x_1, \ldots, x_n, y)$ будем через $\mu y R(x_1, \ldots, x_n, y)$ обозначать то наименьшее значение y, при котором $R(x_1, \ldots, x_n, y)$ истинно, если вообще такие значения существуют. Пусть $f(x_1, \ldots, x_n) =$

$= \mu y\,(g(x_1, \ldots, x_n, y) = 0)$. Будем тогда говорить, что функция f получена из функции g с помощью μ-оператора, если выполнено вышеприведенное предположение о функции g: для любых $x_1, \ldots, x_n$ существует по крайней мере одно значение y, для которого $g(x_1, \ldots, x_n, y) = 0$.

(3) Функция f называется *примитивно рекурсивной*, если она может быть получена из исходных функций с помощью конечного числа подстановок (IV) и рекурсий (V), т. е. если существует такая конечная последовательность функций $f_1, \ldots, f_n$, что $f_n = f$ и для каждого i, $0 \leqslant i \leqslant n$, функция f_i либо исходная, либо может быть получена из некоторых предшествующих ей в этой последовательности функций с помощью применения правила (IV) (подстановки) или правила (V) (рекурсии).

(4) Функция f называется *рекурсивной*, если она может быть получена из начальных функций с помощью конечного числа применений подстановки (IV), рекурсии (V) и μ-оператора (VI). Это последнее определение отличается от определения примитивно рекурсивной функции лишь дополнительным разрешением применять μ-оператор. Поэтому всякая примитивно рекурсивная функция является также и рекурсивной функцией. Позже мы увидим, что обратное неверно.

Мы покажем, что класс рекурсивных функций совпадает с классом функций, представимых в S. (В литературе вместо термина «рекурсивный» иногда употребляется термин «общерекурсивный».)

Докажем сначала, что введение фиктивных переменных, а также перестановка и отождествление переменных не выводят за пределы класса примитивно рекурсивных функций и класса рекурсивных функций.

Предложение 3.13. *Пусть* $g(y_1, \ldots, y_k)$ — *примитивно рекурсивная* (*или рекурсивная*) *функция, и пусть* $x_1, \ldots, x_n$ — *различные переменные*; *тогда, если при каждом* i, $1 \leqslant i \leqslant k$, z_i *есть одна из переменных* $x_1, \ldots, x_n$, *то функция* $f(x_1, \ldots, x_n) = g(z_1, \ldots, z_k)$ *тоже примитивно рекурсивная* (*соответственно рекурсивная*).

Доказательство. Пусть $z_i = x_{j_i}$, где $1 \leqslant j_i \leqslant n$. Тогда $z_i = U^n_{j_i}(x_1, \ldots, x_n)$ и $f(x_1, \ldots, x_n) = g(U^n_{j_1}(x_1, \ldots, x_n), \ldots, U^n_{j_k}(x_1, \ldots, x_n))$. Таким образом, функция f может быть получена из функций g, $U^n_{j_1}, \ldots, U^n_{j_k}$ с помощью подстановки, т. е. f есть примитивно рекурсивная (соответственно рекурсивная) функция.

Примеры. 1. (Введение фиктивных переменных.) Если $g(x_1, x_3)$ — примитивно рекурсивная функция и $f(x_1, x_2, x_3) = g(x_1, x_3)$, то $f(x_1, x_2, x_3)$ есть также примитивно рекурсивная функция. Для доказательства положить $z_1 = x_1$ и $z_2 = x_3$ и применить предложение 3.13.

2. (Перестановка переменных.) Если $g(x_1, x_2)$ — примитивно рекурсивная функция и $f(x_1, x_2) = g(x_2, x_1)$, то f есть также примитивно рекурсивная функция.

Доказательство. В предложении 3.13 положить $z_1 = x_2$ и $z_2 = x_1$.

3. (Отождествление переменных.) Если $g(x_1, x_2, x_3)$ — примитивно рекурсивная функция и $f(x_1, x_2) = g(x_1, x_2, x_1)$, то $f(x_1, x_2)$ есть также примитивно рекурсивная функция.

Доказательство. В 3.13 положить $n = 2$, $z_1 = x_1$, $z_2 = x_2$, $z_3 = x_1$.

Следствие 3.14. (a) *Нуль-функция* $Z_n(x_1, \ldots, x_n) = 0$ *примитивно рекурсивна.* (b) *Постоянная функция* $C_k^n(x_1, \ldots, x_n) = k$, *где* k — *некоторое фиксированное целое неотрицательное число, примитивно рекурсивна.* (c) *Правило подстановки* (IV) *может быть распространено на случай, когда каждая функция* h_i, *возможно, является функцией лишь от некоторых из переменных* $x_1, \ldots, x_n$. *Точно так же и в правиле рекурсии* (V) *функция* g *может фактически не зависеть от каких-либо из переменных* $x_1, \ldots, x_n$, *а функция* h *может не зависеть от каких-либо из переменных* $x_1, \ldots, x_n$, y *или* $f(x_1, \ldots, x_n, y)$.

Доказательство. (a) Пусть в предложении 3.13 g есть нуль-функция Z. Тогда $k = 1$ и остается лишь положить $z_1 = x_1$. (b) Для $k = 0$ искомое утверждение совпадает с доказанным только что пунктом (a). Предположим, что оно верно при некотором k, тогда для $k + 1$ достаточно воспользоваться равенством $C_{k+1}^n(x_1, \ldots, x_n) = N(C_k^n(x_1, \ldots, x_n))$. (c) В силу предложения 3.13, каждая из переменных $x_1, \ldots, x_n$ может быть введена как фиктивная переменная, если это необходимо. Например, если $h(x_1, x_3)$ — данная примитивно рекурсивная (или рекурсивная) функция, то функция $h^*(x_1, x_2, x_3) = h(x_1, x_3) = h(U_1^3(x_1, x_2, x_3), U_3^3(x_1, x_2, x_3))$ тоже является примитивно рекурсивной (или рекурсивной).

Предложение 3.15. *Следующие функции являются примитивно рекурсивными:*

(a) $x + y$; (b) $x \cdot y$; (c) x^y; (d) $\delta(x) = \begin{cases} x - 1, & \text{если } x > 0, \\ 0, & \text{если } x = 0; \end{cases}$

(e) $x \dot{-} y = \begin{cases} x - y, & \text{если } x \geqslant y, \\ 0, & \text{если } x < y; \end{cases}$ (f) $|x - y| = \begin{cases} x - y, & \text{если } x \geqslant y. \\ y - x, & \text{если } x < y; \end{cases}$

(g) $sg(x) = \begin{cases} 0, & \text{если } x = 0, \\ 1, & \text{если } x \neq 0; \end{cases}$ (h) $\overline{sg}(x) = \begin{cases} 1, & \text{если } x = 0, \\ 0, & \text{если } x \neq 0; \end{cases}$

(i) $x!$; (j) $\min(x, y) =$ *наименьшему из чисел* x *и* y;

(k) $\min(x_1, \ldots, x_n)$; (l) $\max(x, y) =$ *наибольшему из чисел* x *и* y;

(m) $\max(x_1, \ldots, x_n)$; (n) $rm(x, y) =$ *остатку от деления* y *на* x, *если* $x \neq 0$, *и* y, *если* $x = 0$;

(o) $qt(x, y) =$ *частному от деления* y *на* x.

Доказательство.

(a) По правилу рекурсии (V):

$$\begin{matrix} x + 0 = x \\ x + (y + 1) = N(x + y) \end{matrix}, \text{ т. е. } \begin{matrix} f(x, 0) = U_1^1(x) \\ f(x, y + 1) = N(f(x, y)). \end{matrix}$$

(b)
$$\begin{matrix} x \cdot 0 = 0 \\ x \cdot (y + 1) = (x \cdot y) + x \end{matrix}, \text{ т. е. } \begin{matrix} g(x, 0) = Z(x) \\ g(x, y + 1) = f(g(x, y), x), \end{matrix}$$

где f есть функция сложения.

(c) $x^0 = 1$ (d) $\delta(0) = 0$ (e) $x \dot{-} 0 = x$

$x^{y+1} = (x^y) \cdot x$ $\delta(y + 1) = y$ $x \dot{-} (y + 1) = \delta(x \dot{-} y)$

(f) $|x - y| = (x \dot{-} y) + (y \dot{-} x)$ (подстановка)

(g) $$sg(0) = 0$$
$$sg(y + 1) = 1$$

(h) $$\overline{sg}(x) = 1 \dot{-} sg(x)$$

(i) $$0! = 1$$
$$(y + 1)! = (y!) \cdot (y + 1)$$

(j) $$\min(x, y) = x \dot{-} (x \dot{-} y)$$

(k) Предположим, что функция $\min(x_1, \ldots, x_n)$ — примитивно рекурсивная. Для $\min(x_1, \ldots, x_{n+1})$ имеем

$$\min(x_1, \ldots, x_{n+1}) = \min(\min(x_1, \ldots, x_n), x_{n+1})$$

(l) $$\max(x, y) = y + (x \dot{-} y)$$

(m) $$\max(x_1, \ldots, x_{n+1}) = \max(\max(x_1, \ldots, x_n), x_{n+1})$$

(n) $$rm(x, 0) = 0$$
$$rm(x, y + 1) = N(rm(x, y)) \cdot sg(|x - N(rm(x, y))|)$$

(o) $$qt(x, 0) = 0$$
$$qt(x, y + 1) = qt(x, y) + \overline{sg}(|x - N(rm(x, y))|)$$

Определения

$$\sum_{y<z} f(x_1, \ldots, x_n, y) = \begin{cases} 0, \text{ если } z = 0, \\ f(x_1, \ldots, x_n, 0) + \ldots + f(x_1, \ldots, x_n, z-1), \text{ если } z > 0; \end{cases}$$

$$\sum_{y \leqslant z} f(x_1, \ldots, x_n, y) = \sum_{y<z+1} f(x_1, \ldots, x_n, y);$$

$$\prod_{y<z} f(x_1, \ldots, x_n, y) = \begin{cases} 1, \text{ если } z = 0, \\ f(x_1, \ldots, x_n, 0) \cdot \ldots \cdot f(x_1, \ldots, x_n, z - 1), \text{ если } z > 0; \end{cases}$$

$$\prod_{y \leqslant z} f(x_1, \ldots, x_n, y) = \prod_{y<z+1} f(x_1, \ldots, x_n, y).$$

Эти *ограниченные суммы и произведения* являются функциями аргументов $x_1, \ldots, x_n, z$. Суммы и произведения, ограниченные с двух сторон, можно теперь определить через введенные только что ограниченные **суммы и**

произведения, например:

$$\sum_{u<y<v} f(x_1, \ldots, x_n, y) = f(x_1, \ldots, x_n, u+1) + \ldots + f(x_1, \ldots, x_n, v-1) = \\ = \sum_{y<(v \dot{-} u) \dot{-} 1} f(x, \ldots, x_n, y + u + 1).$$

Предложение 3.16. *Если* f — *примитивно рекурсивная* (*или рекурсивная*) *функция, то все определенные выше ограниченные суммы и произведения этой функции являются также примитивно рекурсивными* (*или рекурсивными*) *функциями.*

Доказательство. Пусть $g(x_1, \ldots, x_n, z) = \sum_{y<z} f(x_1, \ldots, x_n, y)$. Тогда мы имеем следующую рекурсию:

$$g(x_1, \ldots, x_n, 0) = 0;$$
$$g(x_1, \ldots, x_n, z+1) = g(x_1, \ldots, x_n, z) + f(x_1, \ldots, x_n, z).$$

Если же $h(x_1, \ldots, x_n, z) = \sum_{y \leqslant z} f(x_1, \ldots, x_n, y)$, то имеем $h(x_1, \ldots, x_n, z) = g(x_1, \ldots, x_n, z+1)$ (подстановка). Доказательство соответствующих утверждений для сумм и произведений, ограниченных с двух сторон, мы предоставляем читателю.

Пример. Функция $D(x)$, равная 1 при $x = 0$ и числу делителей x, когда $x > 0$, примитивно рекурсивна, так как

$$D(x) = \sum_{y \leqslant x} \overline{sg}(rm(y, x)).$$

Если нам заданы некоторые отношения в области натуральных чисел, то, применяя к ним логические связки исчисления высказываний, мы можем получить новые отношения. Мы будем пользоваться для этого теми же символами: $\neg$, $\&$, $\vee$, $\supset$, $\equiv$ (если только при этом не будет возникать недоразумений из-за одновременного употребления этих символов в нашем метаязыке и в формальных теориях первого порядка). Например, для любых двух отношений $R_1(x_1, \ldots, x_n)$ и $R_2(x_1, \ldots, x_n)$ $R_1(x_1, \ldots, x_n) \vee R_2(x_1, \ldots, x_n)$ есть отношение, которое выполнено для $x_1, \ldots, x_n$ тогда и только тогда, когда выполнено $R_1(x_1, \ldots, x_n)$ или $R_2(x_1, \ldots, x_n)$. Выражение $\forall y_{y<z} R(x_1, \ldots, x_n, y)$ мы будем употреблять для записи отношения: «При всяком y, если $y < z$, то $R(x_1, \ldots, x_n, y)$». В аналогичном смысле будут употребляться выражения $\forall y_{y \leqslant z}$, $\exists y_{y<z}$ и $\exists y_{y \leqslant z}$; так, например, под $\exists y_{y<z} R(x_1, \ldots, x_n, y)$ мы будем понимать утверждение: «Существует y такое, что $y < z$ и $R(x_1, \ldots, x_n, y)$». Выражения $\forall y_{y<z}$, $\forall y_{y \leqslant z}$, $\exists y_{y<z}$ и $\exists y_{y \leqslant z}$ мы назовем *ограниченными кванторами*. Наконец, *ограниченный* μ-*оператор* определим так:

$$\mu y_{y<z} R(x_1, \ldots, x_n, y) = \begin{cases} \text{наименьшему } y \text{ такому, что } y < z \text{ и} \\ R(x_1, \ldots, x_n, y), \text{ если такое } y \text{ существует;} \\ z \text{ в противном случае.} \end{cases}$$

(Здесь выбор z в качестве значения оператора во втором случае

продиктован только интересами удобства в дальнейших доказательствах, никакого содержательного смысла в это не вкладывается.)

Отношение $R(x_1, \ldots, x_n)$ называется *примитивно рекурсивным* (*рекурсивным*) *отношением*, если примитивно рекурсивной (соответственно рекурсивной) является его характеристическая функция $C_R(x_1, \ldots, x_n)$. В частности, данное множество A натуральных чисел является *примитивно рекурсивным* (*рекурсивным*), если примитивно рекурсивной (рекурсивной) является его характеристическая функция $C_A(x)$.

Примеры. (1) Отношение $x_1 = x_2$ примитивно рекурсивно, так как характеристическая функция его совпадает с функцией $\overline{sg}(|x_1 - x_2|)$, которая примитивно рекурсивна, в силу предложения 3.15 (f), (g).

(2) Примитивно рекурсивная функция $\overline{sg}(x_2 \dot{-} x_1)$ (предложение 3.15 (e), (h)) служит характеристической функцией отношения $x_1 < x_2$, которое, таким образом, примитивно рекурсивно.

(3) Отношение $x_1 \mid x_2$ примитивно рекурсивно, так как его характеристической функцией является примитивно рекурсивная функция $sg(rm(x_1, x_2))$.

(4) Отношение $Pr(x)$, т. е. «x есть простое число», примитивно рекурсивно, так как $C_{Pr}(x) = sg((D(x) \dot{-} 2) + \overline{sg}(|x - 1|) + \overline{sg}(|x - 0|))$. (Напомним, что число x является простым тогда и только тогда, когда оно имеет не более двух делителей и отлично от 0 и 1.)

Предложение 3.17. *Отношения, которые можно получить из примитивно рекурсивных* (*или рекурсивных*) *с помощью пропозициональных связок и ограниченных кванторов, также примитивно рекурсивны* (*соответственно рекурсивны*); *применение ограниченных* μ*-операторов* $\mu y_{y<z}$ *или* $\mu y_{y\leqslant z}$ *к примитивно рекурсивным* (*рекурсивным*) *отношениям приводит к примитивно рекурсивным* (*рекурсивным*) *функциям.*

Доказательство. Пусть отношения $R_1(x_1, \ldots, x_n)$ и $R_2(x_1, \ldots, x_n)$ примитивно рекурсивны (или рекурсивны). Это значит, что их характеристические функции C_{R_1} и C_{R_2} примитивно рекурсивны (соответственно рекурсивны). Но $C_{\neg R_1}(x_1, \ldots, x_n) = 1 \dot{-} C_{R_1}(x_1, \ldots, x_n)$, следовательно, и отношение $\neg R_1$ примитивно рекурсивно (рекурсивно). Кроме того, $C_{R_1 \vee R_2}(x_1, \ldots, x_n) = C_{R_1}(x_1, \ldots, x_n) \cdot C_{R_2}(x_1, \ldots, x_n)$, а потому и отношение $R_1 \vee R_2$ примитивно рекурсивно (рекурсивно). Для пропозициональных связок доказательство на этом и заканчивается, так как все остальные пропозициональные связки выражаются через связки $\neg$ и $\vee$.

Пусть теперь $R(x_1, \ldots, x_n, y)$ — примитивно рекурсивное (рекурсивное) отношение. Обозначим через $Q(x_1, \ldots, x_n, z)$ отношение $\exists y_{y<z} R(x_1, \ldots, x_n, y)$. Нетрудно проверить, что $C_Q(x_1, \ldots, x_n, z) = \prod_{y<z} C_R(x_1, \ldots, x_n y)$, откуда, в силу предложения 3.16, следует, что C_Q является примитивно рекурсивной (рекурсивной) функцией. Ограниченный квантор $\exists y_{y\leqslant z}$ равносилен, очевидно, ограниченному квантору $\exists y_{y<z+1}$, который в свою

очередь может быть получен с помощью подстановки из ограниченного квантора $\exists y_{y<z}$.

Кванторы $\forall y_{y<z}$ и $\forall y_{y\leqslant z}$ эквивалентны соответственно приставкам $\neg\exists y_{y<z}\neg$ и $\neg\exists y_{y\leqslant z}\neg$. Ограниченные с двух сторон кванторы такие, как $\exists y_{u<y<v}$, могут быть определены с помощью подстановок в уже рассмотренные ограниченные кванторы. Наконец, заметим, что функция $\prod_{u\leqslant y} C_R(x_1, \ldots, x_n, u)$ принимает значение 1 при каждом y, для которого $R(x_1, \ldots, x_n, u)$ ложно при всех $u\leqslant y$, и принимает значение 0 всякий раз, когда существует такое $u\leqslant y$, при котором $R(x_1, \ldots, x_n, u)$ истинно. Поэтому, если для данного z существуют числа y меньшие, чем z, и такие, что $R(x_1, \ldots, x_n, y)$ истинно, то значение функции $\sum_{y<z}\prod_{u\leqslant y} C_R(x_1, \ldots, x_n, u)$ равно числу целых неотрицательных чисел, меньших чем наименьшее из таких чисел y; в противном случае значение функции $\sum_{y<z}\prod_{u\leqslant y} C_R(x_1, \ldots, x_n, u)$ равно z. Но это значит, что $\sum_{y<z}\prod_{u\leqslant y} C_R(x_1, \ldots, x_n, u) = \mu y_{y<z} R(x_1, \ldots, x_n, y)$. Отсюда, на основании предложения 3.16, и следует, что применение ограниченного μ-оператора к примитивно рекурсивному (рекурсивному) отношению приводит к примитивно рекурсивной (рекурсивной) функции.

Примеры. (1) Пусть $p(x)$ — функция, принимающая для каждого x значение, равное простому числу с номером x при пересчете всех простых чисел в порядке возрастания, начиная с $p(0)=2$.

В дальнейшем мы будем для краткости вместо $p(x)$ писать p_x. Оказывается, что p_x есть примитивно рекурсивная функция аргумента x. В самом деле, заметим прежде всего, что

(i) $p_0 = 2$; (ii) $p_{x+1} = \mu y_{y\leqslant (p_x)!+1}(p_x < y \,\&\, Pr(y))$.

Здесь следует обратить внимание на то, что отношение $u < y \,\&\, Pr(y)$ примитивно рекурсивное. Следовательно, в силу предложения 3.17, функция $\mu y_{y\leqslant v}(u < y \,\&\, Pr(y))$ является примитивно рекурсивной функцией аргументов u и v; обозначим ее $g(u, v)$. Подставив в $g(u, v)$ примитивно рекурсивные функции z и $z!+1$ соответственно вместо u и v, получим примитивно рекурсивную функцию $h(z) = \mu y_{y\leqslant z!+1}(z < y \,\&\, Pr(y))$. Теперь мы видим, что правая часть равенства (ii) есть $h(p_x)$ и, таким образом, p_x получается из (i), (ii) по правилу рекурсии (V). Граница $(p_x)!+1$ для следующего за p_x простого числа взята из евклидова доказательства бесконечности множества простых чисел (см., например, Виноградов [1952], стр. 19).

(2) Всякое целое положительное число x однозначно разложимо в произведение степеней простых чисел: $x = p_0^{a_0} p_1^{a_1} \ldots p_k^{a_k}$. Обозначим через $(x)_i$ показатель a_i в таком разложении. Если $x = 1$, то $(x)_i = 0$ при любом i. Положим, наконец, $(x)_i = 0$ для любого i, если $x = 0$. Функция $(x)_i$ примитивно рекурсивна, так как при любом x $(x)_i = \mu y_{y<x}(p_i^y \mid x \,\&\, \neg(p_i^{y+1} \mid x))$.

(3) Обозначим через $\mathrm{lh}(x)$ число отличных от нуля показателей в разложении x на простые множители. Пусть $\mathrm{lh}(0)=0$. Функция lh примитивно рекурсивна. В самом деле, пусть $R(x, y)$ обозначает примитивно рекурсивный предикат $\mathrm{Pr}(y) \& y \mid x \& x \neq 0$, тогда $\mathrm{lh}(x)=\sum_{y \leqslant x} \overline{\mathrm{sg}}(C_R(x, y))$.

(4) Если число $x=2^{a_0} \cdot 3^{a_1} \cdot \ldots \cdot p_k^{a_k}$ «представляет» последовательность положительных чисел $a_0, a_1, \ldots, a_k$, а число $y=2^{b_0} \cdot 3^{b_1} \cdot \ldots \cdot p_m^{b_m}$ «представляет» последовательность $b_0, b_1, \ldots, b_m$, то число $x * y=2^{a_0} \cdot 3^{a_1} \cdot \ldots \cdot p_k^{a_k} \cdot p_{k+1}^{b_0} \cdot p_{k+2}^{b_1} \cdot \ldots \cdot p_{k+m+1}^{b_m}$ «представляет» последовательность $a_0, a_1, \ldots, a_k, b_0, b_1, b_2, \ldots, b_m$, которая получается, если вторую из данных последовательностей записать непосредственно вслед за первой. Здесь мы имеем $k+1=\mathrm{lh}(x)$, $m+1=\mathrm{lh}(y)$ и $b_j=(y)_j$. Поэтому $x * y=x \cdot \prod_{j<\mathrm{lh}(y)} (p_{\mathrm{lh}(x)+j})^{(y)_j}$ и, следовательно, функция $*$ является примитивно рекурсивной. При записи повторных применений операции $*$ скобки можно опускать ввиду того, что $x * (y * z)=(x * y) * z$.

(5) Пусть дана функция $f(x_1, \ldots, x_n, y)$. Положим

$$f^*(x_1, \ldots, x_n, 0)=f(x_1, \ldots, x_n, 0),$$
$$f^*(x_1, \ldots, x_n, y+1)=f^*(x_1, \ldots, x_n, y) * f(x_1, \ldots, x_n, y+1).$$

Тогда $f^*(x_1, \ldots, x_n, z)=f(x_1, \ldots, x_n, 0) * f(x_1, \ldots, x_n, 1) * \ldots * f(x_1, \ldots, x_n, z)$, и если функция f — примитивно рекурсивная (рекурсивная), то такова же и f^*.

Упражнения

1. С помощью предложения 3.17 показать, что если отношение $R(x_1, \ldots, x_n, y)$ примитивно рекурсивно (рекурсивно), то примитивно рекурсивны (рекурсивны) отношения

$$\exists y_{u<y<v} R(x_1, \ldots, x_n, y), \quad \exists y_{u \leqslant y \leqslant v} R(x_1, \ldots, x_n, y),$$
$$\exists y_{u \leqslant y<v} R(x_1, \ldots, x_n, y), \quad \exists y_{u<y \leqslant v} R(x_1, \ldots, x_n, y)$$

и функции

$$\mu y_{u<y<z} R(x_1, \ldots, x_n, y), \quad \mu y_{u \leqslant y \leqslant z} R(x_1, \ldots, x_n, y),$$
$$\mu y_{u \leqslant y<z} R(x_1, \ldots, x_n, y), \quad \mu y_{u<y \leqslant z} R(x_1, \ldots, x_n, y).$$

2. Доказать, что класс всех примитивно рекурсивных (рекурсивных) множеств замкнут относительно операций объединения, пересечения и дополнения и что всякое конечное множество примитивно рекурсивно.

3. Пусть (a) $[\sqrt{n}]$ обозначает наибольшее целое число, квадрат которого не превосходит n; (b) $\Pi(n)$ равно числу простых чисел, не превосходящих n. Показать, что функции $[\sqrt{n}]$ и $\Pi(n)$ — примитивно рекурсивные.

[A] **4.** Пусть e есть основание натуральных логарифмов и при каждом n $[ne]$ обозначает наибольшее целое число, не превосходящее ne. Доказать, что функция $[ne]$ примитивно рекурсивна. (Указание. Рассмотреть функцию $S(n)$, определяемую рекурсией $S(0)=0$, $S(n+1)=(n+1) \cdot S(n)+1$.)

[A] **5.** Обозначим через $RP(y, z)$ высказывание «числа y и z взаимно просты», и пусть $\varphi(n)$ — функция, значение которой при каждом n равно числу целых

положительных чисел, не превосходящих n и взаимно простых с n. Доказать, что отношение $RP(y, z)$ и функция $\varphi(n)$ примитивно рекурсивны.

Мы теперь докажем следующую теорему об «определении с перебором случаев»; теорема эта будет полезна при дальнейшем изучении рекурсивных функций.

Предложение 3.18. *Пусть*

$$f(x_1, \ldots, x_n) = \begin{cases} g_1(x_1, \ldots, x_n), & \text{если } R_1(x_1, \ldots, x_n) \text{ истинно,} \\ g_2(x_1, \ldots, x_n), & \text{если } R_2(x_1, \ldots, x_n) \text{ истинно,} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ g_k(x_1, \ldots, x_n) & \text{если } R_k(x_1, \ldots, x_n) \text{ истинно.} \end{cases}$$

Если при этом функции $g_1, \ldots, g_k$ *и отношения* $R_1, \ldots, R_k$ *примитивно рекурсивны (или рекурсивны) и если для любых* $x_1, \ldots, x_n$ *истинно одно и только одно из высказываний* $R_1(x_1, \ldots, x_n), \ldots, R_k(x_1, \ldots, x_n)$, *то функция* f *примитивно рекурсивна (рекурсивна).*

Доказательство. $f(x_1, \ldots, x_n) = g_1(x_1, \ldots, x_n) \cdot \overline{sg}(C_{R_1}(x_1, \ldots, x_n)) + \ldots + g_k(x_1, \ldots, x_n) \cdot \overline{sg}(C_{R_k}(x_1, \ldots, x_n))$.

Упражнения

1. Показать, что в предложении 3.18 предположение о том, что отношение R_k примитивно рекурсивно (или рекурсивно), можно опустить.

2. Пусть

$$f(x) = \begin{cases} x^2, & \text{если } x \text{ четно,} \\ x + 1, & \text{если } x \text{ нечетно.} \end{cases}$$

Доказать, что функция f примитивно рекурсивна.

3. Пусть при каждом x

$$h(x) = \begin{cases} 2, & \text{если великая теорема Ферма истинна,} \\ 1, & \text{если великая теорема Ферма ложна.} \end{cases}$$

Является ли h(x) примитивно рекурсивной функцией?

Весьма часто бывает необходимо устанавливать примитивно рекурсивное соответствие между множеством всех упорядоченных пар натуральных чисел и множеством всех натуральных чисел. Построим одно такое соответствие. С этой целью перенумеруем все упорядоченные пары натуральных чисел следующим образом:

$$\overbrace{(0, 0)}, \quad \overbrace{(0, 1), (1, 0), (1, 1)}, \quad \overbrace{(0, 2), (2, 0), (1, 2), (2, 1), (2, 2)}, \ldots,$$

и вообще, перенумеровав все пары, компоненты которых не превосходят k, мы строим новую $(k+1)$-ю группу всех тех, еще не перенумерованных пар, компоненты которых не превосходят $k+1$, перечисляя их в следующем порядке: $(0, k+1)$, $(k+1, 0)$, $(1, k+1)$, $(k+1, 1)$, $\ldots$, $(k, k+1)$, $(k+1, k)$, $(k+1, k+1)$. (При этом группа, состоящая из одной только пары (0, 0), считается нулевой.) Припишем паре (0, 0) номер 0. Всего

имеется $(y+1)^2$ пар, компоненты которых не превосходят y, причем последняя из них, т. е. пара (y, y), получает при нашем пересчете номер $(y+1)^2-1=y^2+2y$. Если $x<y$, то пара (x, y) непосредственно предшествует паре (y, x), и обе они принадлежат одной и той же y-й группе. Номером пары (x, y) при $x\leqslant y$ будет, очевидно, число $(y^2-1)+(2x+1)=y^2+2x$, а при $y<x$ — число $(x^2-1)+(2y+2)=x^2+2y+1$. Теперь легко видеть, что функция $\sigma^2(x, y)$, вычисляющая номер пары (x, y) в нашей нумерации, имеет следующее представление:

$$\sigma^2(x,\ y)=\operatorname{sg}(x\dot{-}y)\cdot(x^2+2y+1)+\overline{\operatorname{sg}}(x\dot{-}y)\cdot(y^2+2x)$$

и, следовательно, является примитивно рекурсивной.

Рассмотрим обратные функции, т. е. такие функции σ_1^2 и σ_2^2, что $\sigma_1^2(\sigma^2(x, y))=x$, $\sigma_2^2(\sigma^2(x, y))=y$ и $\sigma^2(\sigma_1^2(z), \sigma_2^2(z))=z$. При каждом z, таким образом, числа $\sigma_1^2(z)$ и $\sigma_2^2(z)$ суть соответственно первая и вторая компоненты упорядоченной пары с номером z в построенной нумерации. Заметим, что $\sigma_1^2(0)=0$, $\sigma_2^2(0)=0$,

$$\sigma_1^2(n+1)=\begin{cases}\sigma_2^2(n), & \text{если } \sigma_1^2(n)<\sigma_2^2(n),\\ \sigma_2^2(n)+1, & \text{если } \sigma_1^2(n)>\sigma_2^2(n),\\ 0, & \text{если } \sigma_1^2(n)=\sigma_2^2(n),\end{cases}$$

и

$$\sigma_2^2(n+1)=\begin{cases}\sigma_1^2(n), & \text{если } \sigma_1^2(n)\neq\sigma_2^2(n),\\ \sigma_1^2(n)+1, & \text{если } \sigma_1^2(n)=\sigma_2^2(n).\end{cases}$$

Следовательно,

$$\sigma_1^2(n+1)=\sigma_2^2(n)\cdot(\operatorname{sg}(\sigma_2^2(n)\dot{-}\sigma_1^2(n)))+$$
$$+(\sigma_2^2(n)+1)\cdot(\operatorname{sg}(\sigma_1^2(n)\dot{-}\sigma_2^2(n)))=\varphi(\sigma_1^2(n),\ \sigma_2^2(n)),$$

$$\sigma_2^2(n+1)=\operatorname{sg}(|\sigma_1^2(n)-\sigma_2^2(n)|)\cdot\sigma_1^2(n)+$$
$$+\overline{\operatorname{sg}}(|\sigma_1^2(n)\dot{-}\sigma_2^2(n)|)\cdot(\sigma_1^2(n)+1)=\psi(\sigma_1^2(n),\ \sigma_2^2(n)),$$

где функции φ и ψ примитивно рекурсивны. Таким образом, функции σ_1^2 и σ_2^2 могут быть определены рекурсивно, но одновременно обе. Можно доказать, однако, что на самом деле каждая из функций σ_1^2 и σ_2^2 является примитивно рекурсивной. Доказательство, которое мы здесь приводим, носит несколько искусственный характер. Пусть $\tau(u)=2^{\sigma_1^2(u)}\cdot 3^{\sigma_2^2(u)}$. Функция τ примитивно рекурсивна. В самом деле, $\tau(0)=2^{\sigma_1^2(0)}\cdot 3^{\sigma_2^2(0)}=2^0\cdot 3^0=1$, а $\tau(n+1)=2^{\sigma_1^2(n+1)}\cdot 3^{\sigma_2^2(n+1)}=2^{\varphi(\sigma_1^2(n),\,\sigma_2^2(n))}\cdot 3^{\psi(\sigma_1^2(n),\,\sigma_2^2(n))}=2^{\varphi((\tau(n))_0,\,(\tau(n))_1)}\cdot 3^{\psi((\tau(n))_0,\,(\tau(n))_1)}$; отсюда, вспоминая, что функции $(x)_i$ примитивно рекурсивны (см. пример 2, стр. 141), заключаем, что функция τ может быть получена из примитивно рекурсивных функций по правилу рекурсии (V). Но $\sigma_1^2(x)=(\tau(x))_0$ и $\sigma_2^2(x)=(\tau(x))_1$, и, следовательно, функции σ_1^2 и σ_2^2 примитивно рекурсивны, как результаты применения правила подстановки (IV) к примитивно рекурсивным функциям. Теперь, индукцией по n, могут быть построены взаимно однозначные примитивно рекурсивные соответствия между множеством всех

упорядоченных n-ок натуральных чисел и множеством всех натуральных чисел. Для $n=2$ такое соответствие уже построено. Предположим, что для $n=k$ мы имеем примитивно рекурсивные функции $\sigma^k(x_1, \ldots, x_k)$, $\sigma_1^k(x), \ldots, \sigma_k^k(x)$ такие, что $\sigma_i^k(\sigma^k(x_1, \ldots, x_k)) = x_i$, где $1 \leqslant i \leqslant k$, и $\sigma^k(\sigma_1^k(x), \ldots, \sigma_k^k(x)) = x$. Тогда для $n=k+1$ положим $\sigma^{k+1}(x_1, \ldots, x_k, x_{k+1}) = \sigma^2(\sigma^k(x_1, \ldots, x_k), x_{k+1})$, $\sigma_i^{k+1}(x) = \sigma_i^k(\sigma_1^2(x))$ $(1 \leqslant i \leqslant k)$ и $\sigma_{k+1}^{k+1}(x) = \sigma_2^2(x)$. Эти новые функции, очевидно, также примитивно рекурсивны, и читатель без труда докажет, что $\sigma_i^{k+1}(\sigma^{k+1}(x_1, \ldots, x_{k+1})) = x_i$ для $1 \leqslant i \leqslant k+1$ и $\sigma^{k+1}(\sigma_i^{k+1}(x), \ldots, \sigma_{k+1}^{k+1}(x)) = x$.

Иногда удобно бывает определять функции с помощью такой рекурсии, при которой значение $f(x_1, \ldots, x_n, y+1)$ зависит не только от $f(x_1, \ldots, x_n, y)$, но и от некоторых, или даже всех значений $f(x_1, \ldots, x_n, u)$, где $u \leqslant y$. Рекурсия этого типа называется *возвратной рекурсией*.

Положим $f_\#(x_1, \ldots, x_n, y) = \prod\limits_{u<y} p_u^{f(x_1, \ldots, x_n, u)}$. Легко видеть, что $f(x_1, \ldots, x_n, y) = (f_\#(x_1, \ldots, x_n, y+1))_y$.

Предложение 3.19. *Если функция* $h(x_1, \ldots, x_n, y, z)$ *примитивно рекурсивна (рекурсивна) и* $f(x_1, \ldots, x_n, y) = h(x_1, \ldots, x_n, y, f_\#(x_1, \ldots, x_n, y))$, *то функция* f *примитивно рекурсивна (рекурсивна).*

Доказательство. Из определения операции П на стр. 138 имеем

$$f_\#(x_1, \ldots, x_n, 0) = 1;$$

кроме того, очевидно,

$$f_\#(x_1, \ldots, x_n, y+1) = f_\#(x_1, \ldots, x_n, y) \cdot p_y^{f(x_1, \ldots, x_n, y)} =$$
$$= f_\#(x_1, \ldots, x_n, y) \cdot p_y^{h(x_1, \ldots, x_n, y, f_\#(x_1, \ldots, x_n, y))}.$$

Таким образом, согласно правилу рекурсии (V), функция $f_\#$ является примитивно рекурсивной (рекурсивной), а так как $f(x_1, \ldots, x_n, y) = (f_\#(x_1, \ldots, x_n, y+1))_y$, то и функция f примитивно рекурсивна (рекурсивна).

Пример. Так называемая последовательность Фибоначчи задается рекурсивно равенствами: $f(0)=1$, $f(1)=2$, $f(k+2)=f(k)+f(k+1)$ при $k \geqslant 0$. Докажем, что функция f примитивно рекурсивна. В самом деле, во-первых,

$$f(k) = \overline{sg}(k) + 2 \cdot \overline{sg}(|k-1|) + ((f_\#(k))_{k \dot{-} 1} + (f_\#(k))_{k \dot{-} 2}) \cdot sg(k \dot{-} 1),$$

во-вторых, функция

$$h(y, z) = \overline{sg}(y) + 2 \cdot \overline{sg}(|y-1|) + ((z)_{y \dot{-} 1} + (z)_{y \dot{-} 2}) \cdot sg(y \dot{-} 1)$$

примитивно рекурсивна и, наконец, $f(k) = h(k, f_\#(k))$.

Упражнение

Пусть $g(0)=2$, $g(1)=4$, $g(k+2) = 3g(k+1) \dot{-} (2g(k)+1)$. Показать, что g есть примитивно рекурсивная функция.

Следствие 3.20. *Если отношение* $H(x_1, \ldots, x_n, y, z)$ *примитивно рекурсивно (рекурсивно) и* $R(x_1, \ldots, x_n, y)$ *выполнено тогда и только тогда, когда выполнено* $H(x_1, \ldots, x_n, y, (C_R)_{\#}(x_1, \ldots, x_n, y))$, *где* C_R — *характеристическая функция отношения* R, *то отношение* R *примитивно рекурсивно (рекурсивно).*

Доказательство. Так как характеристическая функция C_H отношения H примитивно рекурсивна (рекурсивна) и $C_R(x_1, \ldots, x_n, y) = C_H(x_1, \ldots, x_n, y, (C_R)_{\#}(x_1, \ldots, x_n, y))$, то, согласно предложению 3.19, примитивно рекурсивной (рекурсивной) является и функция C_R, а с нею вместе и отношение R.

В дальнейшем мы часто будем опираться на предложение 3.19 и на следствие 3.20. Эти два предложения оказываются полезными там, где приходится иметь дело с отношениями и функциями, значения которых для произвольного y определяются через их значения для аргументов, меньших чем y. В связи с этим заметим, что $R(x_1, \ldots, x_n, u)$ эквивалентно равенству $C_R(x_1, \ldots, x_n, u) = 0$, которое в свою очередь при $u < y$ эквивалентно равенству $((C_R)_{\#}(x_1, \ldots, x_n, y))_u = 0$.

Упражнения

1. Доказать, что множество всех общерекурсивных функций счетно.

2. Доказать, что если $f_1, f_2, \ldots$ — какой-нибудь пересчет всех примитивно рекурсивных (всех рекурсивных) функций от одной переменной, то функция $\psi(x, y) = f_x(y)$ не является примитивно рекурсивной (рекурсивной).

Предложение 3.21. (β-функция Гёделя.) *Пусть* $\beta(x_1, x_2, x_3) = \mathrm{rm}(1 + (x_3 + 1) \cdot x_2, x_1)$. *Функция* β *примитивно рекурсивна, в силу предложения* 3.15 (n). *Эта функция, кроме того, сильно представима в* S *следующей формулой* $Bt(x_1, x_2, x_3, x_4)$:

$$\exists w\,(x_1 = (1 + (x_3 + 1) \cdot x_2) \cdot w + x_4 \,\&\, x_4 < 1 + (x_3 + 1) \cdot x_2).$$

Доказательство. Из предложения 3.11 следует, что $\vdash \exists_1 x_4\, Bt(x_1, x_2, x_3, x_4)$. Пусть $\beta(k_1, k_2, k_3) = k_4$. Тогда при некотором k $k_1 = (1 + (k_3 + 1) \cdot k_2) \cdot k + k_4$ и $k_4 < 1 + (k_3 + 1) \cdot k_2$. Поэтому, в силу предложения 3.6 (a), $\vdash \bar{k}_1 = (\bar{1} + (\bar{k}_3 + \bar{1}) \cdot \bar{k}_2) \cdot \bar{k} + \bar{k}_4$ и, опять же в силу предложения 3.6 (a), а также на основании выразимости в S отношения $<$, имеем $\vdash \bar{k}_4 < \bar{1} + (\bar{k}_3 + \bar{1}) \cdot \bar{k}_2$. Следовательно, $\vdash \bar{k}_1 = (\bar{1} + (\bar{k}_3 + \bar{1}) \cdot \bar{k}_2)\,\bar{k} + \bar{k}_4 \,\&\, \bar{k}_4 < \bar{1} + (\bar{k}_3 + \bar{1}) \cdot \bar{k}_2$, откуда по правилу E4 получаем $\vdash Bt(\bar{k}_1, \bar{k}_2, \bar{k}_3, \bar{k}_4)$ Сильная представимость β в S формулой *Bt* доказана.

Предложение 3.22. *Для любой конечной последовательности натуральных чисел* $k_0, k_1, \ldots, k_n$ *существуют такие натуральные числа* b *и* c, *что* $\beta(b, c, i) = k_i$ *для* $0 \leqslant i \leqslant n$.

Доказательство. Пусть $j = \max(n, k_0, k_1, \ldots, k_n)$ и $c = j!$. Рассмотрим числа $u_i = 1 + (i + 1) \cdot c$, где $0 \leqslant i \leqslant n$. Никакие два из них не имеют общих делителей, отличных от 1. В самом деле, если бы

число p было простым делителем каких-нибудь двух чисел $1+(i+1)\cdot c$ и $1+(m+1)\cdot c$, где $0\leqslant i<m\leqslant n$, то p было бы делителем и их разности $(m-i)\cdot c$. Но тогда p не было бы делителем c, ибо в противном случае оно было бы общим делителем чисел $(i+1)\cdot c$ и $1+(i+1)\cdot c$ и, следовательно, делителем числа 1, что невозможно. Следовательно, такое число p должно было бы быть делителем числа $m-i$, что тоже невозможно, ибо $m-i\leqslant n\leqslant j$, и, следовательно, $m-i$ делит $j!=c$, и если бы p делило $m-i$, то делило бы и c. Итак, p не может делить $(m-i)\cdot c$, и потому числа u_i при $0\leqslant i\leqslant m$ попарно взаимно просты. Кроме того, если $0\leqslant i\leqslant n$, то $k_i\leqslant j\leqslant j!=$ $=c<1+(i+1)\cdot c=u_i$. Согласно китайской теореме об остатках (см. Диксон [1929] или упражнение 1 на стр. 151), существует число $b<u_0u_1\ldots u_n$ такое, что $\mathrm{rm}(u_i, b)=k_i$, если $0\leqslant i\leqslant n$. Но $\beta(b, c, i)=$ $=\mathrm{rm}(1+(i+1)\cdot c, b)=\mathrm{rm}(u_i, b)=k_i$, что и требовалось доказать.

Предложения 3.21 и 3.22 позволят нам выражать внутри системы S утверждения о конечных последовательностях натуральных чисел, что существенно важно для доказательства следующей основной теоремы.

Предложение 3.23. *Всякая рекурсивная функция представима в* S.

Доказательство. Исходные функции Z, N, U_i^n представимы в S, согласно примерам (a) — (c) на стр. 133. В силу примера (d) на стр. 133, правило подстановки (IV) не выводит за пределы класса представимых функций. Обратимся к правилу рекурсии (V). Допустим, что функции $\mathrm{g}(\mathrm{x}_1, \ldots, \mathrm{x}_n)$ и $\mathrm{h}(\mathrm{x}_1, \ldots, \mathrm{x}_n, \mathrm{y}, \mathrm{z})$ представимы в S соответственно формулами $\mathscr{A}(x_1, \ldots, x_{n+1})$ и $\mathscr{B}(x_1, \ldots, x_{n+3})$, и пусть

$$(\mathrm{I})\quad \begin{cases} \mathrm{f}(\mathrm{x}_1, \ldots, \mathrm{x}_n, 0) = \mathrm{g}(\mathrm{x}_1, \ldots, \mathrm{x}_n), \\ \mathrm{f}(\mathrm{x}_1, \ldots, \mathrm{x}_n, \mathrm{y}+1) = \mathrm{h}(\mathrm{x}_1, \ldots, \mathrm{x}_n, \mathrm{y}, \mathrm{f}(\mathrm{x}_1, \ldots, \mathrm{x}_n, \mathrm{y})). \end{cases}$$

Идея доказательства заключается в следующем. Равенство $\mathrm{f}(\mathrm{x}_1, \ldots, \mathrm{x}_n, \mathrm{y})=\mathrm{z}$ справедливо тогда и только тогда, когда существует конечная последовательность чисел $b_0, \ldots, b_{\mathrm{y}}$ такая, что $b_0=\mathrm{g}(\mathrm{x}_1, \ldots, \mathrm{x}_n)$, $b_{\mathrm{w}+1}=\mathrm{h}(\mathrm{x}_1, \ldots, \mathrm{x}_n, \mathrm{w}, b_{\mathrm{w}})$ при всяком $\mathrm{w}+1\leqslant\mathrm{y}$ и $b_{\mathrm{y}}=\mathrm{z}$; но, согласно предложению 3.22, всякое высказывание о конечных последовательностях может быть выражено в терминах значений функции β, которая, в силу предложения 3.21, представима в S.

Мы докажем, что функция $\mathrm{f}(\mathrm{x}_1, \ldots, \mathrm{x}_n, \mathrm{x}_{n+1})$ представима в S с помощью формулы $\mathscr{C}(x_1, \ldots, x_{n+2})$:

$$\exists u\exists v[(\exists w(Bt(u, v, 0, w)\,\&\,\mathscr{A}(x_1, \ldots, x_n, w)))\,\&$$
$$\&\,Bt(u, v, x_{n+1}, x_{n+2})\,\&\,\forall w(w<x_{n+1}\supset\exists y\exists z(Bt(u, v, w, y)\,\&$$
$$\&\,Bt(u, v, w', z)\,\&\,\mathscr{B}(x_1, \ldots, x_n, w, y, z)))].$$

(i) Предположим сначала, что $\mathrm{f}(k_1, \ldots, k_n, p)=m$. Докажем $\vdash\mathscr{C}(\bar{k}_1, \ldots, \bar{k}_n, \bar{p}, \bar{m})$. Если $p=0$, то $m=\mathrm{g}(k_1, \ldots, k_n)$. Рассмотрим последовательность, состоящую из одного числа m. Согласно предложению 3.22, существуют такие b, c, что $\mathfrak{R}(b, c, 0)=m$. Следовательно,

в силу предложения 3.21, $\vdash Bt(\bar{b}, \bar{c}, 0, \bar{m})$. Кроме того, так как $m = g(k_1, \ldots, k_n)$, то $\vdash \mathscr{A}(\bar{k}_1, \ldots, \bar{k}_n, \bar{m})$. Отсюда по правилу E4 получаем

$$\vdash \exists w (Bt(\bar{b}, \bar{c}, 0, w) \& \mathscr{A}(\bar{k}_1, \ldots, \bar{k}_n, w)). \quad (*)$$

Перед этим мы только что доказали, что

$$\vdash Bt(\bar{b}, \bar{c}, 0, \bar{m}). \quad (**)$$

Переходя, наконец, к третьему конъюнктивному члену в $\mathscr{C}(\bar{k}_1, \ldots, \bar{k}_n, 0, \bar{m})$, мы видим, что из $\vdash \neg(w < 0)$, на основании соответствующей тавтологии, следует

$$\vdash \forall w (w < 0 \supset \exists y \exists z Bt(\bar{b}, \bar{c}, w, y) \& \& Bt(\bar{b}, \bar{c}, w', z) \& \mathscr{B}(\bar{k}_1, \ldots, \bar{k}_n, w, y, z)). \quad (***)$$

Из (*), (**) и (***) по правилу E4 получаем, наконец, $\vdash \mathscr{C}(\bar{k}_1, \ldots, \bar{k}_n, 0, \bar{m})$. Для $p > 0$ $f(k_1, \ldots, k_n, p)$ вычисляется из равенств (I) за $p+1$ шагов. Пусть $r_i = f(k_1, \ldots, k_n, i)$ при $i = 0, 1, 2, \ldots, p$. Согласно предложению 3.22, для последовательности $r_0, r_1, \ldots, r_p$ существуют числа b, c такие, что $\beta(b, c, i) = r_i$ при $0 \leqslant i \leqslant p$. Тогда, по предложению 3.21, $\vdash Bt(\bar{b}, \bar{c}, \bar{i}, \bar{r}_i)$. Так как, в частности, $\beta(b, c, 0) = r_0 = f(k_1, \ldots, k_n, 0) = g(k_1, \ldots, k_n)$, то $\vdash Bt(\bar{b}, \bar{c}, 0, \bar{r}_0) \& \mathscr{A}(\bar{k}_1, \ldots, \bar{k}_n, \bar{r}_0)$, и, следовательно, по правилу E4

(1) $\vdash \exists w (Bt(\bar{b}, \bar{c}, 0, w) \& \mathscr{A}(\bar{k}_1, \ldots, \bar{k}_n, w))$.

Далее, так как $r_p = f(k_1, \ldots, k_n, p) = m$, то $\beta(b, c, p) = m$. Поэтому

(2) $\vdash Bt(\bar{b}, \bar{c}, \bar{p}, \bar{m})$.

Если же, наконец, $0 \leqslant i \leqslant p-1$, то $\beta(b, c, i) = r_i = f(k_1, \ldots, k_n, i)$ и $\beta(b, c, i+1) = r_{i+1} = f(k_1, \ldots, k_n, i+1) = h(k_1, \ldots, k_n, i, f(k_1, \ldots, k_n, i)) = h(k_1, \ldots, k_n, i, r_i)$. Следовательно, $\vdash Bt(\bar{b}, \bar{c}, \bar{i}, \bar{r}_i) \& \& Bt(\bar{b}, \bar{c}, \bar{i}', \bar{r}_{i+1}) \& \mathscr{B}(\bar{k}_1, \ldots, \bar{k}_n, \bar{i}, \bar{r}_i, \bar{r}_{i+1})$. Теперь по правилу E4 получаем $\vdash \exists y \exists z (Bt(\bar{b}, \bar{c}, \bar{i}, y) \& Bt(\bar{b}, \bar{c}, \bar{i}', z) \& \mathscr{B}(\bar{k}_1, \ldots, \bar{k}_n, \bar{i}, y, z))$. Отсюда, на основании предложения 3.8 (b′), получаем

(3) $\vdash \forall w (w < \bar{p} \supset \exists y \exists z (Bt(\bar{b}, \bar{c}, \bar{i}, y) \& Bt(\bar{b}, \bar{c}, \bar{i}', z) \& \mathscr{B}(\bar{k}_1, \ldots, \bar{k}_n, \bar{i}, y, z)))$.

Применив дважды правило E4 к конъюнкции формул, выводимость которых обозначена через (1), (2) и (3), получаем окончательно $\vdash \mathscr{C}(\bar{k}_1, \ldots, \bar{k}_n, \bar{p}, \bar{m})$. Таким образом, мы доказали, что пункт (1) определения представимости в S (стр. 133) для функции f выполнен.

(ii) Теперь мы должны доказать, что $\vdash \exists_1 x_{n+2} \mathscr{C}(\bar{k}_1, \ldots, \bar{k}_n, \bar{p}, x_{n+2})$ при любых $k_1, \ldots, k_n, p$. Докажем это индукцией по p в метаязыке. Заметим, что, в силу доказанного выше, нам осталось доказать лишь единственность. Случай $p = 0$ легкий, и мы его оставляем читателю

в качестве упражнения. Итак, предположим, что $\vdash \exists_1 x_{n+2} \mathscr{C}(\bar{k}_1, \ldots, \bar{k}_n, \bar{p}, x_{n+2})$. Пусть $\alpha = g(k_1, \ldots, k_n)$, $\beta = f(k_1, \ldots, k_n, p)$ и $\gamma = f(k_1, \ldots, k_n\ p+1) = h(k_1, \ldots, k_n, p, \beta)$. Тогда

(1) $\vdash \mathscr{B}(\bar{k}_1, \ldots, \bar{k}_n, \bar{p}, \bar{\beta}, \bar{\gamma})$

(2) $\vdash \mathscr{A}(\bar{k}_1, \ldots, \bar{k}_n, \bar{\alpha})$

(3) $\vdash \mathscr{C}(\bar{k}_1, \ldots, \bar{k}_n, \bar{p}, \bar{\beta})$

(4) $\vdash \mathscr{C}(\bar{k}_1, \ldots, \bar{k}_n, \overline{p+1}, \bar{\gamma})$

(5) $\vdash \exists_1 x_{n+2} \mathscr{C}(\bar{k}_1, \ldots, \bar{k}_n, \bar{p}, x_{n+2})$

Предположим

(6) $\mathscr{C}(\bar{k}_1, \ldots, \bar{k}_n, \overline{p+1}, x_{n+2})$.

Мы должны доказать, что $x_{n+2} = \bar{\gamma}$. Из (6) по правилу C получаем

(a) $\exists w (Bt(b, c, 0, w) \& \mathscr{A}(\bar{k}_1, \ldots, \bar{k}_n, w))$,

(b) $Bt(b, c, \overline{p+1}, x_{n+2})$,

(c) $\forall w (w < \overline{p+1} \supset \exists y \exists z (Bt(b, c, w, y) \&$
$\& Bt(b, c, w', z) \& \mathscr{B}(\bar{k}_1, \ldots, \bar{k}_n, w, y, z)))$.

Из (c) получаем

(d) $\forall w (w < \bar{p} \supset \exists y \exists z (Bt(b, c, w, y) \&$
$\& Bt(b, c, w', z) \& \mathscr{B}(\bar{k}_1, \ldots, \bar{k}_n, w, y, z)))$.

Из (c) по правилу C следует

(e) $Bt(b, c, \bar{p}, d) \& Bt(b, c, \overline{p+1}, e) \& \mathscr{B}(\bar{k}_1, \ldots, \bar{k}_n, \bar{p}, d, e)$.

Из (a), (d), (e) следует

(f) $\mathscr{C}(\bar{k}_1, \ldots, \bar{k}_n, \bar{p}, d)$.

Из (f) и (5) следует

(g) $d = \bar{\beta}$.

Из (e) и (g) получаем

(h) $\mathscr{B}(\bar{k}_1, \ldots, \bar{k}_n, \bar{p}, \bar{\beta}, e)$.

Так как функция h представима формулой $\mathscr{B}$, то из (1) и (h) следует

(i) $\bar{\gamma} = e$.

Из (e) и (i) следует

(j) $Bt(b, c, \overline{p+1}, \bar{\gamma})$,

и, наконец, из (b) и (j), на основании предложения 3.21, получаем

(k) $x_{n+2} = \bar{\gamma}$.

Индукция завершена.

Перейдем, наконец, к μ-оператору. Допустим, что для любых $x_1, \ldots, x_n$ существует y такое, что $g(x_1, \ldots, x_n, y) = 0$, и предположим, что функция g представима в S формулой $\mathscr{D}(x_1, \ldots, x_{n+2})$. Пусть

$f(x_1, \ldots, x_n) = \mu y (g(x_1, \ldots, x_n, y) = 0)$. Докажем, что тогда функция f представима формулой $\mathscr{E}(x_1, \ldots, x_{n+1})$:

$$\mathscr{D}(x_1, \ldots, x_{n+1}, 0) \& \forall y (y < x_{n+1} \supset \neg \mathscr{D}(x_1, \ldots, x_n, y, 0)).$$

Предположим сначала, что $f(k_1, \ldots, k_n) = m$. Тогда $g(k_1, \ldots, k_n, m) = 0$ и $g(k_1, \ldots, k_n, k) \neq 0$ при $k < m$. Поэтому $\vdash \mathscr{D}(\bar{k}_1, \ldots, \bar{k}_n, \bar{m}, 0)$ и $\vdash \neg \mathscr{D}(\bar{k}_1, \ldots, \bar{k}_n, \bar{k}, 0)$ при $k < m$. В силу предложения 3.8 (b'),

$$\vdash \forall y (y < \bar{m} \supset \neg \mathscr{D}(\bar{k}_1, \ldots, \bar{k}_n, y, 0)).$$

Следовательно, $\vdash \mathscr{E}(\bar{k}_1, \ldots, \bar{k}_n, \bar{m})$. Остается доказать, что $\vdash \exists_1 x_{n+1} \mathscr{E}(\bar{k}_1, \ldots, \bar{k}_n, x_{n+1})$, причем, ввиду уже доказанного, достаточно, очевидно, установить лишь единственность. Допустим, что $\mathscr{D}(\bar{k}_1, \ldots, \bar{k}_n, u, 0) \& \forall y (y < u \supset \neg \mathscr{D}(\bar{k}_1, \ldots, \bar{k}_n, y, 0))$ и $\mathscr{D}(\bar{k}_1, \ldots, \bar{k}_n, v, 0) \& \forall y (y < v \supset \neg \mathscr{D}(\bar{k}_1, \ldots, \bar{k}_n, y, 0))$. Тогда, если $v < u$, то мы получим противоречие $\mathscr{D}(\bar{k}_1, \ldots, \bar{k}_n, v, 0) \& \neg \mathscr{D}(\bar{k}_1, \ldots, \bar{k}_n, v, 0)$, а если $u < v$, то получим противоречие $\mathscr{D}(\bar{k}_1, \ldots, \bar{k}_n, u, 0) \& \neg \mathscr{D}(\bar{k}_1, \ldots, \bar{k}_n, u, 0)$. А так как $\vdash u < v \vee v < u \vee u = v$, то $u = v$.

Таким образом, мы доказали, что все рекурсивные функции представимы в S. Можно также показать, что все примитивно рекурсивные функции сильно представимы в S. Для исходных функций это было показано в примерах (a) — (c) на стр. 133. Кроме того, было также показано, что правило подстановки не выводит за пределы класса сильно представимых функций (там же, пример (d)). Наконец, приведенное только что доказательство того, что правило рекурсии не выводит за пределы класса представимых в S функций, может быть усовершенствовано для получения аналогичного утверждения о сильной представимости, поскольку предложение 3.22 может быть доказано в системе S при любом n, т. е. для каждого $n \geqslant 1$

$$\vdash_S \exists u \exists v (Bt(u, v, 0, x_1) \& Bt(u, v, \bar{1}, x_2) \& \ldots \& Bt(u, v, \bar{n}, x_n)).$$

Следствие 3.24. *Всякое рекурсивное отношение выразимо в* S.

Доказательство. Пусть $R(x_1, \ldots, x_n)$ — рекурсивный предикат *). Характеристическая функция C_R этого предиката рекурсивна. В силу предложения 3.23, функция C_R представима в S и, следовательно, в силу предложения 3.12, предикат R выразим в S.

Упражнения

A1. (a) Показать, что если a и b — взаимно простые натуральные числа, то существует натуральное число c такое, что $ac \equiv 1 \pmod{b}$. ($x \equiv y \pmod{z}$ означает, что x и y имеют один и тот же остаток при делении на z или, иначе говоря, что разность $x - y$ делится на z без остатка. (По сути дела, в настоя-

*) Слово «предикат» употребляется часто как синоним слова «отношение».

щем упражнении речь идет о существовании целых u и v таких, что $1 = au + bv$.)

b) Доказать китайскую теорему об остатках: каковы бы ни были натуральные числа $y_1, \ldots, y_k$ и натуральные попарно взаимно простые числа $x_1, \ldots, x_k$, существует натуральное число z такое, что $z \equiv y_1 \pmod{x_1}, \ldots, z \equiv y_k \pmod{x_k}$, причем любые два таких числа z отличаются друг от друга на число, кратное произведению $x_1 \ldots x_k$ (Указание. Пусть $x = x_1 \ldots x_k$, и пусть $x = w_1 x_1 = \ldots = w_k x_k$ при соответствующих w_i. Тогда, если $1 \leqslant i \leqslant k$, то w_i и x_i взаимно просты, и, в силу предыдущего пункта (a), существует z_i такое, что $w_i z_i \equiv 1 \pmod{x_i}$. Положим теперь $z = w_1 z_1 y_1 + \ldots + w_k z_k y_k$. Тогда $z \equiv w_i z_i y_i \equiv y_i \pmod{x_i}$. Кроме того, разность между любыми двумя такими решениями делится на $x_1, \ldots, x_k$, а следовательно, и на $x_1 x_2 \ldots x_k$.)

2. (a) Назовем предикат $R(x_1, \ldots, x_n)$ *арифметическим*, если он является интерпретацией какой-нибудь формулы $\mathscr{A}(x_1, \ldots, x_n)$ теории S относительно стандартной модели Показать, что всякий рекурсивный предикат является арифметическим (Указание. Использовать следствие 3.24.)

b) Показать, что для всякой рекурсивной функции $f(x_1, \ldots, x_n)$ ее представляющий предикат $f(x_1, \ldots, x_n) = y$ (см. стр. 135, упражнение l) рекурсивен. (Указание Характеристической функцией представляющего предиката является $\operatorname{sg}(|f(x_1, \ldots, x_n) - y|)$.)

(c) Если функция $f(x_1, \ldots, x_n)$ рекурсивна, то ее представляющий предикат является арифметическим.

3. Открытая проблема: всякая ли рекурсивная функция сильно представима в S?

§ 4. Арифметизация. Гёделевы номера

Каждому символу *u* произвольной теории первого порядка K следующим образом поставим в соответствие положительное число $g(u)$, называемое *гёделевым номером* символа *u*:

$$g((\,) = 3;\ g(\,)\,) = 5;\ g(,) = 7;\ g(\neg) = 9;\ g(\supset) = 11;$$
$$g(x_k) = 5 + 8k \text{ для } k = 1, 2, \ldots;$$
$$g(a_k) = 7 + 8k \text{ для } k = 1, 2, \ldots;$$
$$g(f_k^n) = 9 + 8(2^n 3^k) \text{ для } k,\ n \geqslant 1;$$
$$g(A_k^n) = 11 + 8(2^n 3^k) \text{ для } k,\ n \geqslant 1;$$

при этом положим $g((\forall x_i)) = g((x_i))$.

Таким образом, различным символам поставлены в соответствие различные гёделевы номера, являющиеся положительными числами *).

Примеры. $g(x_2) = 21$, $g(a_4) = 39$, $g(f_1^2) = 105$, $g(A_2^1) = 155$.

Пусть дано выражение $u_0 u_1 \ldots u_r$. Гёделев номер $g(u_0 u_1 \ldots u_r)$ этого выражения определим как $2^{g(u_0)} 3^{g(u_1)} \ldots p_r^{g(u_r)}$, где p_i есть *i*-е простое число и $p_0 = 2$. Например,

$$g(A_1^2(x_1, x_2)) = 2^{g(A_1^2)} \cdot 3^{g((\,))} \cdot 5^{g(x_1)} \cdot 7^{g(,)} \cdot 11^{g(x_2)} \cdot 13^{g(\,))} =$$
$$= 2^{107} \cdot 3^3 \cdot 5^{13} \cdot 7^7 \cdot 11^{21} \cdot 13^5.$$

Заметим, что, в силу единственности разложения натуральных чисел в произведения степеней простых чисел, различные выражения получают

*) Эта же самая нумерация была применена в лемме 2.10, стр. 73.

при этом разные гёделевы номера. Кроме того, гёделевы номера выражений четны и потому отличны от гёделевых номеров символов. (Всякий символ можно рассматривать как выражение, и тогда он снабжается гёделевым номером, отличным от того, который становится ему в соответствие как символу. Это не должно, однако, приводить к недоразумению.)

Наконец, гёделев номер произвольной последовательности $e_0, \ldots, e_r$ выражений определим следующим образом: $g(e_0, \ldots, e_r) = 2^{g(e_0)} \cdot 3^{g(e_1)} \times \times \ldots p_r^{g(e_r)}$. Как и прежде, различные последовательности выражений имеют различные гёделевы номера, а так как эти последние четны и, кроме того, имеют четный показатель степени при 2, то они отличны и от гёделевых номеров символов, и от гёделевых номеров выражений.

Таким образом, функция g взаимно однозначно отображает множество всех символов, выражений и конечных последовательностей выражений в множество целых положительных чисел. Множество значений функции g не совпадает, однако, с множеством всех целых положительных чисел; так, число 12 не является гёделевым номером.

Упражнения

1. Построить объекты, имеющие своими гёделевыми номерами числа 1944 и 47.

2. Показать, что если n нечетно, то $4n$ не является гёделевым номером.

3. Найти гёделевы номера выражений:

(a) $f_1^1(a_1)$, (b) $(\neg(A_1^3(a_1, x_3, x_5))) \supset (A_1^1(x_2))$.

Такая нумерация символов, выражений и последовательностей выражений впервые была предпринята Гёделем [1931] с целью *арифметизации* метаматематики *), т. е. с целью замены утверждений о формальной системе эквивалентными высказываниями о натуральных числах с последующим выражением этих высказываний в формальной системе. Идея арифметизации стала ключом к решению многих важных проблем математической логики.

Рассмотренный здесь способ построения гёделевых номеров, разумеется, не является единственным. Другие способы можно найти у Клини [1952, гл. X] и у Шмульяна [1961, гл. I, § 6].

Предложение 3.25. *Пусть для данной теории первого порядка* K *следующие отношения примитивно рекурсивны* (*рекурсивны*): (a) IC(x), *что означает* «x *есть гёделев номер предметной константы теории* K», (b) FL(x), *что означает* «x *есть гёделев номер функциональной буквы теории* K», (c) PL(x), *что означает* «x *есть*

*) Арифметизацией данной теории первого порядка K мы называем всякую функцию g, отображающую взаимно однозначно множество всех символов, выражений и конечных последовательностей выражений теории K в множество целых положительных чисел. При этом требуется: (i) чтобы функция g была эффективно вычислимой, (ii) чтобы существовала эффективная процедура, позволяющая для каждого m определить, является ли m значением функции g, и в случае, если является, то построить тот объект x, для которого $m = g(x)$.

гёделев номер предикатной буквы теории K». *Тогда следующие отношения и функции являются примитивно рекурсивными* (*рекурсивными*). (В (1)—(4) предположения (a)—(c) не используются *).)

(1) EVbl (x): «x есть гёделев номер выражения, состоящего из переменной», что может быть выражено формулой $\exists z_{z<x}(1 \leqslant z \,\&\, x = 2^{5+8z})$. Это отношение примитивно рекурсивно на основании предложения 3.17.

(2) $\mathrm{Arg_T}(x) = (\mathrm{qt}(8,\ x \dot{-} 9))_0$; если x есть гёделев номер функциональной буквы f^n_j, то $\mathrm{Arg_T}(x) = n$.

$\mathrm{Arg_P}(x) = (\mathrm{qt}(8,\ x \dot{-} 11))_0$; если x есть гёделев номер предикатной буквы A^n_j, то $\mathrm{Arg_P}(x) = n$.

(3) MP (x, y, z): «выражение с гёделевым номером z непосредственно следует из выражений с гёделевыми номерами x и y по правилу modus ponens». Формально это отношение выражается равенством $y = 2^3 * x * 2^{11} * z * 2^5$ **).

(4) Gen (x, y): «выражение с гёделевым номером y получается из выражения с гёделевым номером x по правилу обобщения», или формально:

$$\exists v_{v<y}(\mathrm{EVbl}(v) \,\&\, y = 2^3 * 2^3 * v * 2^5 * x * 2^5).$$

(5) EIC (x): «x есть гёделев номер выражения, состоящего из предметной константы», т. е. $\exists y_{y<x}(\mathrm{IC}(y) \,\&\, x = 2^y)$. (Предложение 3.17.)

EFL (x): «x есть гёделев номер выражения, состоящего из функциональной буквы», т. е. $\exists y_{y<x}(\mathrm{FL}(y) \,\&\, x = 2^y)$. (Предложение 3.17.)

EPL (x): «x есть гёделев номер выражения, состоящего из предикатной буквы», т. е. $\exists y_{y<x}(\mathrm{PL}(y) \,\&\, x = 2^y)$. (Предложение 3.17.)

(6) Trm (x): «x есть гёделев номер терма теории K». Это высказывание истинно тогда и только тогда, когда либо x есть гёделев номер выражения, состоящего из предметной константы или из предметной переменной, либо существуют функциональная буква f^n_k и термы $t_1, \ldots, t_n$ такие, что x есть гёделев номер выражения $f^n_k(t_1, \ldots, t_n)$. В этом последнем случае пусть y — гёделев номер последовательности из $n+3$ выражений: f^n_k; $f^n_k($; $f^n_k(t_1$; $f^n_k(t_1, t_2$; $\ldots$; $f^n_k(t_1, t_2, \ldots, t_{n-1}$; $f^n_k(t_1, \ldots, t_{n-1}, t_n$; $f^n_k(t_1, \ldots, t_n)$. Нетрудно видеть, что $y < (p^x_{n+2})^{n+3} < (p^x_x)^x = p^{x^2}_x$. Заметим также, что $n = \mathrm{Arg_T}((x)_0)$, ибо $(x)_0$ есть гёделев номер символа f^n_k. Следовательно, Trm (x) эквивалентно следующему отношению:

$$\mathrm{EVbl}(x) \vee \mathrm{EIC}(x) \vee \exists y_{y<(p_x)^{x^2}}[x = (y)_{\mathrm{lh}(y) \dot{-} 1} \,\&\, \mathrm{EFL}((y)_0) \,\&\, \mathrm{lh}(y) =$$
$$= \mathrm{Arg_T}((x)_0) + 3 \,\&\, (y)_1 = (y)_0 \cdot 3^3 \,\&\, \forall u_{u<\mathrm{lh}(y)}(u > 1 \,\&\, u \leqslant$$
$$\leqslant \mathrm{Arg_T}((x)_0) \supset \exists v_{v<x}((y)_u = (y)_{u \dot{-} 1} * v * 2^7 \,\&\, \mathrm{Trm}(v))) \,\&$$
$$\& \exists v_{v<y}((y)_{\mathrm{lh}(y) \dot{-} 2} = (y)_{\mathrm{lh}(y) \dot{-} 3} * v \,\&\, \mathrm{Trm}(v) \,\&\, (y)_{\mathrm{lh}(y) \dot{-} 1} = (y)_{\mathrm{lh}(y) \dot{-} 2} * 2^5)].$$

Таким образом, в силу следствия 3.20, предикат Trm (x) примитивно

*) Ниже автор перечисляет предикаты и функции одновременно с обоснованием их примитивной рекурсивности (или рекурсивности). (*Прим. перев.*)

**) См. определение приписывающей функции * в примере 4 на стр. 142.

рекурсивен (рекурсивен), так как последняя формула содержит Trm (v) только для $v < x$ *).

(7) Atmf (x): «x есть гёделев номер элементарной формулы теории K». Это высказывание истинно тогда и только тогда, когда существуют термы $t_1, \ldots, t_n$ и предикатная буква A_k^n такие, что x есть гёделев номер $A_k^n(t_1, \ldots, t_n)$. Тогда существует последовательность выражений A_k^n; A_k^n (; $A_k^n(t_1$,; $A_k^n(t_1, t_2$;; ...; $A_k^n(t_1, t_2, \ldots, t_{n-1}$,; $A_k^n(t_1, t_2, \ldots, t_{n-1}, t_n$; $A_k^n(t_1, \ldots, t_{n-1}, t_n)$. Пусть y — гёделев номер этой последовательности, состоящей из $n+3$ выражений. Так же, как и в предыдущем пункте (6), $y < (p_x)^{x^2}$ и $n = \mathrm{Arg_P}((x)_0)$. Поэтому Atmf (x) эквивалентно следующему отношению:

$$(\exists y)_{y<(p_x)^{x^2}}[x = (y)_{\mathrm{lh}\,(y)\dot{-}1} \,\&\, \mathrm{EPL}((y)_0) \,\&\, \mathrm{lh}\,(y) = \mathrm{Arg_P}((x)_0) +$$
$$+ 3 \,\&\, (y)_1 = (y)_0 \cdot 3^3 \,\&\, \forall u_{u<\mathrm{lh}\,(y)}(u > 1 \,\&\, u \leqslant \mathrm{Arg_P}((x)_0) \supset$$
$$\supset \exists v_{v<y}((y)_u = (y)_{u\dot{-}1} * v * 2^7 \,\&\, \mathrm{Trm}\,(v))) \,\&\, \exists v_{v<y}((y)_{\mathrm{lh}\,(y)\dot{-}2} =$$
$$= (y)_{\mathrm{lh}\,(y)\dot{-}3} * v \,\&\, \mathrm{Trm}\,(v)) \,\&\, (y)_{\mathrm{lh}\,(y)\dot{-}1} = (y)_{\mathrm{lh}\,(y)\dot{-}2} * 2^5].$$

Отсюда, на основании предложения 3.17, заключаем, что отношение Atmf (x) примитивно рекурсивно (рекурсивно).

(8) Fml (y): «y есть гёделев номер некоторой формулы теории K».

$$\mathrm{Atmf}\,(y) \vee \exists z_{z<y}[(\mathrm{Fml}\,(z) \,\&\, y = 2^3 * 2^9 * z * 2^5) \vee$$
$$\vee (\mathrm{Fml}\,((z)_0) \,\&\, \mathrm{Fml}\,((z)_1) \,\&\, y = 2^3 * (z)_0 * 2^{11} * (z)_1 * 2^5) \vee$$
$$\vee (\mathrm{Fml}\,((z)_0) \,\&\, \mathrm{EVbl}\,((z)_1) \,\&\, y = 2^3 * 2^3 * (z)_1 * 2^5 * (z)_0 * 2^5)].$$

Здесь применимо следствие 3.20 (возвратная рекурсия) (упражнение).

(9) (a) $\mathrm{Subst}_1(\gamma, u, v)$: «$(\gamma)_0$ есть гёделев номер результата подстановки в формулу с гёделевым номером $(\gamma)_1$ терма с гёделевым номером u вместо всех свободных вхождений переменной с гёделевым номером v».

$$\mathrm{Trm}\,(u) \,\&\, \mathrm{EVbl}\,(v) \,\&\, (((\gamma)_1 = v \,\&\, (\gamma)_0 = u) \vee (\exists w_{w<(\gamma)_1}((\gamma)_1 =$$
$$= 2^w \,\&\, (\gamma)_1 \neq v \,\&\, (\gamma)_0 = (\gamma)_1)) \vee (\exists w_{w<(\gamma)_1}(1 < w \,\&\, (\gamma)_1 =$$
$$= 2^3 * 2^{\cdot} * v * 2^5 * w \,\&\, (\gamma)_1 = (\gamma)_0)) \vee (\mathrm{Atmf}\,((\gamma)_1) \supset$$
$$\supset \exists w_{w<(\gamma)_1}\exists z_{z<(\gamma)_1}\exists \alpha_{\alpha<(\gamma)_0}\exists \beta_{\beta<(\gamma)_0}((\gamma)_1 = w * z \,\&\, (\gamma)_0 =$$
$$= \alpha * \beta \,\&\, \mathrm{Subst}_1(2^\alpha \cdot 3^w, u, v) \,\&\, \mathrm{Subst}_1(2^\beta \cdot 3^z, u, v))) \vee$$
$$\vee (\exists w_{w<(\gamma)_1}\exists z_{z<(\gamma)_1}\exists \alpha_{\alpha<(\gamma)_0}\exists \beta_{\beta<(\gamma)_0}((\gamma)_1 = 2^3 * w * 2^{11} * z * 2^5 \,\&$$
$$\& \,(\gamma)_0 = 2^3 * \alpha * 2^{11} * \beta * 2^5 \,\&\, \mathrm{Subst}_1(2^\alpha \cdot 3^w, u, v) \,\&\, \mathrm{Subst}_1(2^\beta \cdot 3^z, u, v))) \vee$$
$$\vee (\exists w_{w<(\gamma)_1}\exists \alpha_{\alpha<(\gamma)_0}((\gamma)_1 = 2^3 * 2^9 * w * 2^5 \,\&\, (\gamma)_0 =$$
$$= 2^3 * 2^9 * \alpha * 2^5 \,\&\, \mathrm{Subst}_1(2^\alpha \cdot 3^w, u, v))).$$

В силу следствия 3.20 (проверить его применимость), предикат Subst_1 примитивно рекурсивен (рекурсивен).

*) Если мы заменим оба вхождения Trm (v) в вышеприведенную формулу на $(z)_v = 0$, то новая формула определит нам некоторый примитивно рекурсивный (рекурсивный) предикат H (x, z) такой, что $\mathrm{Trm}\,(x) \equiv H(x, (C_{\mathrm{Trm}})_{\neq}(x))$; поэтому здесь и применимо следствие 3.20.

(b) Subst (x, y, u, v): «x есть гёделев номер результата подстановки терма с гёделевым номером u вместо всех свободных вхождений переменной с гёделевым номером v в формулу с гёделевым номером y». Это утверждение эквивалентно $\mathrm{Subst}_1(2^x \cdot 3^y, u, v)$.

(c) Пусть Sub (y, u, v) — гёделев номер результата подстановки терма с гёделевым номером u вместо всех свободных вхождений переменной с гёделевым номером v в формулу с гёделевым номером y. Так как $\mathrm{Sub}(y, u, v) = \mu x_{x < p_{uy}^{uy}} \mathrm{Subst}(x, y, u, v)$, то функция Sub примитивно рекурсивна (рекурсивна), в силу предложения 3.17.

(10) (a) Fr (u, x): «u есть гёделев номер формулы теории K, содержащей свободно переменную с гёделевым номером x».

$$\mathrm{Fml}(u) \,\&\, \mathrm{EVbl}(x) \,\&\, \neg\, \mathrm{Subst}(u, u, 2^5 + 8^u, x)$$

(т. е. подстановка в формулу с гёделевым номером u переменной, отличной от переменной с гёделевым номером x, вместо всех свободных вхождений переменной с номером x приводит к новому выражению).

(b) Fr_1 (u, v, w): «u есть гёделев номер терма, свободного для переменной с гёделевым номером v, в формуле с гёделевым номером w».

$$\mathrm{Trm}(u) \,\&\, \mathrm{EVbl}(v) \,\&\, \mathrm{Fml}(w) \,\&\, [\mathrm{Atfml}(w) \vee \exists y_{y<w}(w = 2^3 * 2^9 * y * 2^5 \,\&\, \mathrm{Fr}_1(u, v, y)) \vee \exists y_{y<w} \exists z_{z<w}(w = 2^3 * y * 2^{11} * z * 2^5 \,\&\, \mathrm{Fr}_1(u, v, y) \,\&\, \mathrm{Fr}_1(u, v, z)) \vee \exists y_{y<w} \exists z_{z<w}(w = 2^3 * 2^3 * z * 2^5 * y * 2^5 \,\&\, \mathrm{EVbl}(z) \,\&\, (\mathrm{Fr}(y, v) \subset \neg\, \exists \alpha_{\alpha<w} \exists \beta_{\beta<w}(u = \alpha * 2^z * \beta)))].$$

Для доказательства применить возвратную рекурсию (следствие 3.20).

(11) (a) Ax_1 (x): «x есть гёделев номер частного случая схемы аксиом (1)».

$$\exists u_{u<x} \exists v_{v<x}(\mathrm{Fml}(u) \,\&\, \mathrm{Fml}(v) \,\&\, x = 2^3 * u * 2^{11} * 2^3 * v * 2^{11} * u * 2^5 * 2^5).$$

(b) Ax_2 (x): «x есть гёделев номер частного случая схемы аксиом (2)».

$$\exists u_{u<x} \exists v_{v<x} \exists w_{w<x}(\mathrm{Fml}(u) \,\&\, \mathrm{Fml}(v) \,\&\, \mathrm{Fml}(w) \,\&\, x = 2^3 * 2^3 * u * 2^{11} * 2^3 * v * 2^{11} * w * 2^5 * 2^5 * 2^{11} * 2^3 * 2^3 * u * 2^{11} * v * 2^5 * 2^{11} * 2^3 * u * 2^{11} * w * 2^5 * 2^5 * 2^5)$$

(c) Ax_3 (x): «x есть гёделев номер частного случая схемы аксиом (3)».

$$\exists u_{u<x} \exists v_{v<x}(\mathrm{Fml}(u) \,\&\, \mathrm{Fml}(v) \,\&\, x = 2^3 * 2^3 * 2^3 * 2^9 * v * 2^5 * 2^{11} * 2^3 * 2^9 * u * 2^5 * 2^5 * 2^{11} * 2^3 * 2^3 * 2^3 * 2^9 * v * 2^5 * 2^{11} * u * 2^5 * 2^{11} * v * 2^5 * 2^5).$$

(d) Ax_4 (x): «x есть гёделев номер частного случая схемы аксиом (4)».

$$\exists u_{u<x} \exists v_{v<x} \exists w_{w<x}(\mathrm{Fml}(u) \,\&\, \mathrm{Trm}(v) \,\&\, \mathrm{EVbl}(w) \,\&\, \mathrm{Fr}_1(v, w, u) \,\&\, x = 2^3 * 2^3 * 2^3 * w * 2^5 * u * 2^5 * 2^{11} * \mathrm{Sub}(u, v, w) * 2^5).$$

(e) $\mathrm{Ax}_5(x)$: «x есть гёделев номер частного случая схемы аксиом (5)».

$$\exists u_{u<x}\exists v_{v<x}\exists w_{w<x}(\mathrm{Fml}(u)\ \&\ \mathrm{Fml}(v)\ \&\ \mathrm{EVbl}(w)\ \&\ \neg\,\mathrm{Fr}(u,\ w)\ \&\ x = 2^3 * 2^3 * 2^3 * w * 2^5 * 2^3 * u * 2^{11} * v * 2^5 * 2^5 * 2^{11} * 2^3 * u * 2^{11} * 2^3 * 2^3 * w * 2^5 * v * 2^5 * 2^5 * 2^5).$$

(f) LAx (y): «y есть гёделев номер логической аксиомы».

$$\mathrm{Ax}_1(y) \vee \mathrm{Ax}_2(y) \vee \mathrm{Ax}_3(y) \vee \mathrm{Ax}_4(y) \vee \mathrm{Ax}_5(y).$$

(11′) Gd (x): «x есть гёделев номер выражения теории K».

$$\mathrm{EVbl}(x) \vee \mathrm{EIC}(x) \vee \mathrm{EFL}(x) \vee \mathrm{EPL}(x) \vee x = 2^3 \vee x = 2^5 \vee x = 2^7 \vee x = 2^9 \vee x = 2^{11} \vee \exists u_{u<x}\exists v_{v<x}(x = u * v\ \&\ \mathrm{Gd}(u)\ \&\ \mathrm{Gd}(v))$$

(следствие 3.20).

Замечание. В предложении 3.25 условия (a) — (c) выполнены для всякой теории K с конечным числом предметных констант, а также функциональных и предикатных букв, ибо для такой теории предикаты IC (x), FL (x) и PL (x) примитивно рекурсивны. Так, например, если предметными константами теории K служат символы $a_{j_1}, a_{j_2}, \ldots, a_{j_n}$, то IC (x) истинно тогда и только тогда, когда $x = 7 + 8j_1 \vee x = 7 + 8j_2 \vee \ldots \vee x = 7 + 8j_n$. В частности, условия (a) — (c) выполнены для S.

Предложение 3.26. *Если теория* K *удовлетворяет условиям* (a) — (c) *предложения* 3.25 *и если, кроме того,* (d) *предикат* PrAx (y): «y *есть гёделев номер собственной аксиомы теории* K», *примитивно рекурсивен* (*рекурсивен*), *то следующие отношения примитивно рекурсивны* (*рекурсивны*).

(12) Ax (y): «y есть гёделев номер аксиомы теории K».

$$\mathrm{LAx}(y) \vee \mathrm{PrAx}(y).$$

(13) (a) Prf (y): «y есть гёделев номер вывода в K». В силу следствия 3.20, предикат

$$\exists w_{w<y}(y = 2^w\ \&\ \mathrm{Ax}(w)) \vee \exists u_{u<y}\exists w_{w<y}\exists v_{v<y}(\mathrm{Prf}(u)\ \&\ y = u * (p_{\mathrm{lh}(u)})^v\ \&\ (\mathrm{Ax}(v) \vee \mathrm{Gen}(v, (u)_w))) \vee \exists z_{z<y}\exists w_{w<y}\exists u_{u<y}\exists v_{v<y}(\mathrm{Prf}(u)\ \&\ y = u * (p_{\mathrm{lh}(u)})^v\ \&\ \mathrm{MP}((u)_z, (u)_w, v)),$$

эквивалентный Prf (y), является примитивно рекурсивным (рекурсивным).

(b) Pf (y, x): «y есть гёделев номер вывода формулы с гёделевым номером x». Pf (y, x) эквивалентно $\mathrm{Prf}(y)\ \&\ x = (y)_{\mathrm{lh}(y) \dot{-} 1}$.

(Заметим, что S удовлетворяет условию (d). В самом деле, пусть $a_1, a_2, \ldots, a_8$ — гёделевы номера аксиом (S1) — (S8), и пусть u есть гёделев номер частного случая схемы аксиом (S9), что возможно тогда и только тогда, когда

$$\exists v_{v<u}\exists y_{y<u}(\mathrm{EVbl}(v)\ \&\ \mathrm{Fml}(y)\ \&\ u = 2^3 * \mathrm{Sub}(y,\ 2^{15},\ v) * 2^{11} * 2^3 * 2^3 * 2^3 * v * 2^5 * 2^3 * y * 2^{11} * \mathrm{Sub}(y,\ 2^{57} * 2^3 * v * 2^5,\ v) * 2^5 * 2^5 * 2^{11} * 2^3 * 2^3 * v * 2^5 * y * 2^5 * 2^5 * 2^5).$$

Обозначим эту последнюю формулу через $A_9(u)$. Тогда x есть гёделев номер собственной аксиомы теории S в том и только в том случае, когда $x = a_1 \vee x = a_2 \vee \ldots \vee x = a_8 \vee A_9(x)$.)

Предложение 3.27. *Для теории* S, *наряду с отношениями и функциями* (a) — (d) *и* (1) — (13), *примитивно рекурсивными являются также следующие отношения и функции.*

(14) (a) Nu (y): «y есть гёделев номер некоторой цифры теории S». $y = 2^{15} \vee \exists x_{x<y}(\mathrm{Nu}(x) \& y = 2^{57} * 2^3 * x * 2^5)$. Применить следствие 3.20.

(b) Num (y) = гёделеву номеру $\bar{y}$.

$$\mathrm{Num}(0) = 2^{15}, \qquad \mathrm{Num}(y+1) = 2^{57} * 2^3 * \mathrm{Num}(y) * 2^5.$$

(15) Bw (u, v, x, y): «u есть гёделев номер некоторой формулы $\mathscr{A}$, v есть гёделев номер переменной, свободной в $\mathscr{A}$, и y есть гёделев номер вывода в S формулы, полученной из $\mathscr{A}$ подстановкой цифры $\bar{x}$ вместо свободных вхождений в $\mathscr{A}$ переменной с гёделевым номером v».

$$\mathrm{Fml}(u) \& \mathrm{EVbl}(v) \& \mathrm{Fr}(u, v) \& \mathrm{Pf}(y, \mathrm{Sub}(u, \mathrm{Num}(x), v)).$$

(16) Пусть $\mathscr{A}(x_1, \ldots, x_n)$ — некоторая фиксированная формула теории S, единственными свободными переменными которой являются $x_1, \ldots, x_n$, и пусть m есть гёделев номер $\mathscr{A}(x_1, \ldots, x_n)$. Обозначим через $\mathrm{Bw}_{\mathscr{A}}(u_1, \ldots, u_n, y)$ высказывание: «y есть гёделев номер вывода в S формулы $\mathscr{A}(\bar{u}_1, \ldots, \bar{u}_n)$». Тогда $\mathrm{Bw}_{\mathscr{A}}(u_1, \ldots, u_n, y)$ эквивалентно

$$\mathrm{Pf}(y, \mathrm{Sub}\ldots(\mathrm{Sub}(\mathrm{Sub}(m, \mathrm{Num}(u_1), 2^{5+8}), \mathrm{Num}(u_2), 2^{5+16}))\ldots).$$

(17) (a) $W_1(u, y)$: «u есть гёделев номер формулы $\mathscr{A}(x_1)$, содержащей свободную переменную x_1, и y есть гёделев номер вывода в S формулы $\mathscr{A}(\bar{u})$». Это утверждение эквивалентно

$$\mathrm{Fml}(u) \& \mathrm{Fr}(u, 2^{13}) \& \mathrm{Pf}(y, \mathrm{Sub}(u, \mathrm{Num}(u), 2^{13})).$$

(b) $W_2(u, y)$: «u есть гёделев номер формулы $\mathscr{A}(x_1)$, содержащей свободную переменную x_1, и y есть гёделев номер вывода в S формулы $\neg\mathscr{A}(\bar{u})$. Это утверждение эквивалентно

$$\mathrm{Fml}(u) \& \mathrm{Fr}(u, 2^{13}) \& \mathrm{Pf}(y, \mathrm{Sub}(2^3 * 2^9 * u * 2^5, \mathrm{Num}(u), 2^{13})).$$

(18) Определим, наконец, функцию D(u) таким образом, чтобы для каждого u, являющегося гёделевым номером формулы $\mathscr{A}(x_1)$ со свободной переменной x_1, D(u) было равно гёделеву номеру формулы $\mathscr{A}(\bar{u})$. Для этого положим $\mathrm{D}(u) = \mathrm{Sub}(u, \mathrm{Num}(u), 2^{13})$.

В дальнейшем символы, служащие для обозначения относящихся к системе S предикатов и функций из предложений 3.25—3.27, мы будем снабжать индексом «S», чтобы указать на зависимость этих предикатов и функций от S. Дело в том, что, рассматривая какую-нибудь другую теорию первого порядка S′ с теми же символами, что и у S, мы можем получить в предложениях 3.25—3.27 предикаты и функции, отличные от предикатов и функций, соответствующих в этих предложениях теории S.

Предложение 3.28. *Всякая функция* $f(x_1, \ldots, x_n)$, *представимая в* S, *рекурсивна.*

Доказательство. Пусть формула $\mathscr{A}(x_1, \ldots, x_n, z)$ представляет f в S. Рассмотрим натуральные числа $k_1, \ldots, k_n$. Пусть $f(k_1, \ldots, k_n) = m$. Тогда $\vdash_S \mathscr{A}(\bar{k}_1, \ldots, \bar{k}_n, \bar{m})$. Пусть j есть гёделев номер вывода $\mathscr{A}(\bar{k}_1, \ldots, \bar{k}_n, m)$ в S. Тогда $\mathrm{Bw}_{\mathscr{A}}(k_1, \ldots, k_n, m, j)$ (см. предложение 3.27 (16)). Итак, для любых $x_1, \ldots, x_n$ существует такое y, что $\mathrm{Bw}_{\mathscr{A}}(x_1, \ldots, x_n, (y)_0, (y)_1)$. Поэтому $f(x_1, \ldots, x_n) = (\mu y \mathrm{Bw}_{\mathscr{A}}(x_1, \ldots, x_n, (y)_0, (y)_1))_0$. Согласно предложению 3.27 (16), предикат $\mathrm{Bw}_{\mathscr{A}}$ примитивно рекурсивен. Отсюда, принимая во внимание правило μ-оператора (VI) в определении рекурсивных функций, заключаем, что функция $\mu y \mathrm{Bw}_{\mathscr{A}}(x_1, \ldots, x_n, (y)_0, (y)_1)$ рекурсивна; следовательно, и функция f рекурсивна.

Предложение 3.28 вместе с предложением 3.23 показывает, что класс рекурсивных функций совпадает с классом функций, представимых в S.

В главе 5 мы приведем доводы в пользу правдоподобности того, что понятие рекурсивной функции есть точный математический эквивалент интуитивной идеи эффективно вычислимой функции.

Следствие 3.29. *Всякий заданный на множестве натуральных чисел предикат* $R(x_1, \ldots, x_n)$ *рекурсивен тогда и только тогда, когда он выразим в теории* S.

Доказательство. Согласно определению, предикат $R(x_1, \ldots, x_n)$ рекурсивен тогда и только тогда, когда рекурсивна функция C_R. С другой стороны, предикат R выразим в S тогда и только тогда, когда функция C_R представима в S (предложение 3.12).

§ 5. Теорема Гёделя для теории S

Пусть K — теория первого порядка с теми же самыми символами, что и S. Теория K называется *ω-непротиворечивой*, если для всякой формулы $\mathscr{A}(x)$ этой теории из того, что при любом n $\vdash_K \mathscr{A}(\bar{n})$, следует невозможность $\vdash_K \exists x \neg \mathscr{A}(x)$. Если мы признаем стандартную интерпретацию теории S в качестве модели этой теории, то тогда теорию S следует признать ω-непротиворечивой. Но, так или иначе, мы будем явно формулировать предположение о ω-непротиворечивости S всякий раз, когда эта ω-непротиворечивость будет использована в доказательстве (см. замечания о непротиворечивости на стр. 121).

Предложение 3.30 *Если теория* K *ω-непротиворечива, то она непротиворечива.*

Доказательство. Пусть теория K ω-непротиворечива. Рассмотрим какую-нибудь выводимую в K формулу $\mathscr{A}(x)$ со свободной переменной, например $x = x \supset x = x$. При любом n имеем, очевидно, $\vdash_K \bar{n} = \bar{n} \supset \bar{n} = \bar{n}$. Поэтому формула $\exists x \neg (x = x \supset x = x)$ невыводима

в K. Следовательно, теория K непротиворечива (ибо, в силу тавтологии $\neg A \supset (A \supset B)$, из противоречивости K следовало бы, что в K выводима любая формула).

Согласно предложению 3.27 (17a), отношение $W_1(u, y)$ примитивно рекурсивно и потому, в силу следствия 3.24, выразимо в S некоторой формулой $\mathcal{W}_1(x_1, x_2)$ с двумя свободными переменными x_1, x_2. Это значит, что если $W_1(k_1, k_2)$ истинно, то $\vdash_S \mathcal{W}_1(\bar{k}_1, \bar{k}_2)$, и если $W_1(k_1, k_2)$ ложно, то $\vdash_S \neg \mathcal{W}_1(\bar{k}_1, \bar{k}_2)$. Рассмотрим теперь формулу

$$\forall x_2 \neg \mathcal{W}_1(x_1, x_2). \qquad (*)$$

Пусть m есть гёделев номер формулы (*). Подставив в (*) $\bar{m}$ вместо x_1, мы получим замкнутую формулу

$$\forall x_2 \neg \mathcal{W}_1(\bar{m}, x_2). \qquad (**)$$

Вспомним, что утверждение $W_1(u, y)$ истинно тогда и только тогда, когда u есть гёделев номер некоторой формулы $\mathscr{A}(x_1)$, содержащей свободно переменную x_1, а y есть гёделев номер вывода в S формулы $\mathscr{A}(\bar{u})$. Следовательно,

(I) $W_1(m, y)$ истинно тогда и только тогда, когда y есть гёделев номер вывода в S формулы (**).

Предложение 3.31. (Теорема Гёделя для теории S [1931].)

(1) *Если теория* S *непротиворечива, то формула* (**) *невыводима в* S.

(2) *Если теория* S *ω-непротиворечива, то формула* $\neg$(**) *невыводима в* S.

(Таким образом, в силу предложения 3.30, если теория S ω-непротиворечива, то замкнутая формула (**) невыводима и неопровержима в S. Замкнутые формулы, обладающие таким свойством, называются *неразрешимыми предложениями* теории S.)

Доказательство. (1) Предположим, что теория S непротиворечива и $\vdash_S \forall x_2 \neg \mathcal{W}_1(\bar{m}, x_2)$. Пусть тогда k — гёделев номер какого-нибудь вывода в S этой последней формулы. В силу (I), справедливо $W_1(m, k)$. Так как $\mathcal{W}_1$ выражает W_1 в S, то $\vdash_S \mathcal{W}_1(\bar{m}, \bar{k})$. Из $\forall x_2 \neg \mathcal{W}_1(\bar{m}, x_2)$ по правилу A4 мы можем вывести $\neg \mathcal{W}_1(\bar{m}, \bar{k})$. Таким образом, в S оказываются выводимыми формулы $\mathcal{W}_1(\bar{m}, \bar{k})$ и $\neg \mathcal{W}_1(\bar{m}, \bar{k})$, что противоречит предположению о непротиворечивости S.

(2) Предположим, что теория S ω-непротиворечива и $\vdash \neg \forall x_2 \neg \mathcal{W}_1(\bar{m}, x_2)$, т. е. $\vdash_S \neg$(**). На основании предложения 3.30, заключаем, что теория S непротиворечива и, следовательно, не $\vdash_S$(**). Поэтому, каково бы ни было натуральное число n, n не есть гёделев номер вывода в S формулы (**), т. е. $W_1(m, n)$ ложно для любого n. А это значит, что $\vdash_S \neg \mathcal{W}_1(\bar{m}, \bar{n})$ для любого n. Взяв в качестве формулы $\mathscr{A}(x_2)$ формулу $\neg \mathcal{W}_1(\bar{m}, x_2)$, мы, на основании предположения о ω-

непротиворечивости теории S, заключаем, что не $\vdash_S \exists x_2 \neg\neg \mathscr{W}_1(\bar{m}, x_2)$ и, следовательно, не $\vdash_S \exists x_2 \mathscr{W}_1(\bar{m}, x_2)$. Мы пришли, таким образом, к противоречию с предположением, что $\vdash_S \exists x_2 \mathscr{W}_1(\bar{m}, x_2)$.

Весьма любопытна стандартная интерпретация неразрешимого предложения (**): $\forall x_2 \neg \mathscr{W}_1(\bar{m}, x_2)$. Так как $\mathscr{W}_1$ выражает в S отношение W_1, то, в соответствии со стандартной интерпретацией, (**) утверждает, что $W_1(m, x_2)$ ложно для каждого натурального числа x_2. Согласно (I), это означает, что не существует вывода формулы (**) в S. Другими словами, формула (**) утверждает свою собственную невыводимость в S *). По теореме же Гёделя, если только теория S непротиворечива, эта формула и в самом деле невыводима в S и потому истинна при стандартной интерпретации. Итак, для натуральных чисел, соответствующих обычной интерпретации, формула (**) верна, но в S невыводима. Это может навести нас на мысль, что теорема Гёделя потому справедлива для теории S, что первоначально выбранная для этой теории система аксиом оказалась слишком слабой и что, если бы мы усилили теорию S, добавив к ней новые аксиомы, то новая теория могла бы оказаться полной. Так, например, чтобы получить некоторую более сильную теорию S_1, мы могли бы добавить к S истинную формулу (**). Однако всякая рекурсивная функция, будучи представимой в S, представима также и в такой теории S_1. Точно так же и предложения 3.25 — 3.27 остаются, очевидно, в силе, если их переформулировать для S_1. Но ведь это и есть все, что требуется для того, чтобы получить результат Гёделя; и потому, если теория S_1 ω-непротиворечива, то и она имеет некоторое неразрешимое предложение $\mathscr{B}$. ($\mathscr{B}$ имеет ту же форму $\forall x_2 \neg (\mathscr{W}_1)_{S_1}(\bar{k}, x_2)$, но, разумеется, будет отличаться от (**), поскольку отношение W_1 для S_1 отлично от отношения W_1 для S, и, следовательно, формула $(\mathscr{W}_1)_{S_1}$ и входящая в $\mathscr{B}$ цифра $\bar{k}$ отличны от формулы $\mathscr{W}_1$ и цифры $\bar{m}$ в (**).)

Упражнения

1. Пусть S_g — расширение теории S, полученное добавлением к последней формулы $\neg$(**) в качестве новой аксиомы. Показать, что если теория S непротиворечива, то теория S_g непротиворечива и ω-противоречива.

2. Теория K, содержащая те же символы, что и теория S, называется ω-*неполной*, если существует такая формула $\mathscr{A}(x)$, что $\vdash_K \mathscr{A}(\bar{n})$ для каждого неотрицательного n, но не $\vdash_K \forall x \mathscr{A}(x)$. Доказать, что если теория S непротиворечива, то она ω-неполна. (Указание. Рассмотреть формулу $\neg \mathscr{W}_1(\bar{m}, x_2)$ и применить предложение 3.31.)

*) Таким образом, (**) является аналогом различных семантических парадоксов, в частности, таких, как парадоксы Ришара, Берри и парадокс лжеца (см. Ван Хао [1955]).

3. Показать, что для непротиворечивой теории ω-противоречивость влечет ω-неполноту.

В теореме Гёделя содержится предположение о ω-непротиворечивости теории S. Однако, как показал Россер [1936 b], ценой некоторого усложнения доказательства можно с тем же успехом ограничиться предположением об обычной непротиворечивости теории S.

Как было доказано, отношение $W_2(u, y)$ из предложения 3.27 (17 b) является примитивно рекурсивным. Следовательно, W_2 выразимо в S с помощью некоторой формулы $\mathcal{W}_2(x_1, x_2)$. Рассмотрим тогда формулу

$$\forall x_2 (\mathcal{W}_1(x_1, x_2) \supset \exists x_3 (x_3 \leqslant x_2 \,\&\, \mathcal{W}_2(x_1, x_3))). \qquad (***)$$

Пусть n — гёделев номер этой формулы. Подставив в нее вместо x_1 цифру $\bar{n}$, получим замкнутую формулу

$$\forall x_2 (\mathcal{W}_1(\bar{n}, x_2) \supset \exists x_3 (x_3 \leqslant x_2 \,\&\, \mathcal{W}_2(\bar{n}, x_3))). \qquad (****)$$

Вспомним, что $W_1(u, y)$ (соответственно $W_2(u, y)$) истинно тогда и только тогда, когда u есть гёделев номер какой-нибудь формулы $\mathscr{A}(x_1)$ со свободной переменной x_1, а y есть гёделев номер вывода в S формулы $\mathscr{A}(\bar{u})$ (соответственно $\neg \mathscr{A}(\bar{u})$). Так как n есть гёделев номер формулы (***), то

(II) $W_1(n, y)$ истинно тогда и только тогда, когда y есть гёделев номер вывода в S формулы (****);

(III) $W_2(n, y)$ истинно тогда и только тогда, когда y есть гёделев номер вывода в S формулы $\neg$ (****).

Предложение 3.32. (Теорема Гёделя в форме Россера [1936 b].) *Если теория* S *непротиворечива, то в ней невыводимы обе формулы* (****) *и* $\neg$ (****) *и, следовательно, существует неразрешимое предложение этой теории.*

Доказательство. Предположим, что теория S непротиворечива и что в S выводима формула (****), т. е.

$$\vdash_S \forall x_2 (\mathcal{W}_1(\bar{n}, x_2) \supset \exists x_3 (x_3 \leqslant x_2 \,\&\, \mathcal{W}_2(\bar{n}, x_3))).$$

Пусть тогда k — гёделев номер какого-нибудь вывода (****) в S. В силу (II), справедливо $W_1(n, k)$. Так как $\mathcal{W}_1$ выражает W_1 в S, то $\vdash_S \mathcal{W}_1(\bar{n}, \bar{k})$. Но из (****) по правилу A4 можно получить $\vdash_S \mathcal{W}_1(\bar{n}, \bar{k}) \supset \exists x_3 (x_3 \leqslant \bar{k} \,\&\, \mathcal{W}_2(\bar{n}, x_3))$ и затем по MP и $\vdash_S \exists x_3 (x_3 \leqslant \bar{k} \,\&\, \mathcal{W}_2(\bar{n}, x_3))$. Так как, согласно предположению, теория S непротиворечива, то в S не существует вывода формулы $\neg$ (****). Поэтому, в силу (III), $W_2(n, y)$ ложно для всякого натурального y. А так как $\mathcal{W}_2$ выражает W_2 в S, то $\vdash_S \neg \mathcal{W}_2(\bar{n}, \bar{j})$ для любого натурального j и, в частности, $\vdash_S \neg \mathcal{W}_2(\bar{n}, \bar{0}) \,\&\, \ldots \,\&\, \neg \mathcal{W}_2(\bar{n}, \bar{k})$. Поэтому, в силу предложения 3.8(a'), $\vdash_S \forall x_3 (x_3 \leqslant \bar{k} \supset \neg \mathcal{W}_2(\bar{n}, x_3))$, и, наконец, по теореме о замене (следствие 2.21), $\vdash_S \neg \exists x_3 (x_3 \leqslant \bar{k} \,\&\, \mathcal{W}_2(\bar{n}, x_3))$. Но тем

самым мы доказали выводимость в S формулы, являющейся отрицанием ранее выведенной уже в S формулы, что противоречит непротиворечивости S.

(2) Допустим $\vdash_S \neg(****)$, т. е. $\vdash_S \neg \forall x_2 (\mathscr{W}_1(n, x_2) \supset \exists x_3 (x_3 \leqslant x_2 \& \mathscr{W}_2(n, x_3)))$. Пусть r — гёделев номер какого-нибудь вывода $\neg(****)$. В силу (III), истинно $W_2(n, r)$, и потому $\vdash_S \mathscr{W}_2(\bar{n}, \bar{r})$. В силу предположения о непротиворечивости теории S, не существует вывода в S формулы (****), т. е. согласно (II), $W_1(n, y)$ ложно для каждого натурального y. Поэтому $\vdash_S \neg \mathscr{W}_1(\bar{n}, \bar{j})$ для каждого натурального числа j. В частности,

$$\vdash_S \neg \mathscr{W}_1(\bar{n}, \bar{0}) \& \neg \mathscr{W}_1(\bar{n}, \bar{1}) \& \ldots \& \neg \mathscr{W}_1(\bar{n}, \bar{r}).$$

Отсюда, в силу предложения 3.8 (a′), получаем

(i) $\vdash_S x_2 \leqslant \bar{r} \supset \neg \mathscr{W}_1(\bar{n}, x_2)$.

Рассмотрим теперь следующий вывод:

(1) $\bar{r} \leqslant x_2$	гипотеза
(2) $\mathscr{W}_2(\bar{n}, \bar{r})$	выводимость доказана выше
(3) $\bar{r} \leqslant x_2 \& \mathscr{W}_2(\bar{n}, \bar{r})$	(1), (2), тавтология
(4) $\exists x_3 (x_3 \leqslant x_2 \& \mathscr{W}_2(\bar{n}, x_3))$	(3), правило E4

Из (1) — (4) с помощью теоремы дедукции получаем

(ii) $\vdash_S \bar{r} \leqslant x_2 \supset \exists x_3 (x_3 \leqslant x_2 \& \mathscr{W}_2(\bar{n}, x_2))$.

Согласно предположению 3.7(p),

(iii) $\vdash_S x_2 \leqslant \bar{r} \vee \bar{r} \leqslant x_2$.

Из (i) — (iii) с помощью подходящей тавтологии получаем

$$\vdash_S \neg \mathscr{W}_1(\bar{n}, x_2) \vee \exists x_3 (x_3 \leqslant x_2 \& \mathscr{W}_2(\bar{n}, x_2)),$$

а затем снова с помощью тавтологии и правил MP и Gen:

$$\vdash_S \forall x_2 (\mathscr{W}_1(\bar{n}, x_2) \supset \exists x_3 (x_3 \leqslant x_2 \& \mathscr{W}_2(\bar{n}, x_2))).$$

Итак, $\vdash_S (****)$. Но это противоречит предположениям о непротиворечивости S и о том, что $\vdash_S \neg (****)$.

Россерово неразрешимое предложение (****) тоже имеет интересную стандартную интерпретацию. Согласно (II) и (III), $W_1(n, x_2)$ означает, что x_2 есть гёделев номер некоторого вывода в S формулы (****), а $W_2(n, x_3)$ означает, что x_3 есть гёделев номер некоторого вывода в S формулы $\neg$ (****). Таким образом, (****) утверждает, что если существует вывод в S формулы (****), то существует, и даже с меньшим гёделевым номером, вывод в S формулы $\neg$ (****). Согласно же предложению 3.32, если теория S непротиворечива, то формула (****)

в ней невыводима; поэтому, если теория S непротиворечива, то формула (****) верна в стандартной интерпретации.

Теорема Гёделя в форме Россера применима не только к теории S. Пусть K — любая теория первого порядка с теми же символами, что и теория S. Анализ проведенного только что доказательства позволяет сформулировать следующие достаточные условия применимости теоремы Гёделя в форме Россера к теории K:

(a) Отношения W_1 и W_2 (см. предложение 3.27(17), в котором всюду в определениях следует заменить S на K) выразимы в K.

(b) Имеется формула $u \leqslant v$ такая, что

(i) для всякой формулы $\mathscr{A}(x)$ и для всякого натурального k:

$$\vdash_K \mathscr{A}(0) \& \mathscr{A}(\bar{1}) \& \ldots \& \mathscr{A}(\bar{k}) \supset \forall x\,(x \leqslant \bar{k} \supset \mathscr{A}(x)),$$

(ii) для всякого натурального числа k:

$$\vdash_K x \leqslant \bar{k} \vee \bar{k} \leqslant x.$$

Заметим, что если K есть теория первого порядка с равенством, то условие (i) может быть заменено условием

(i′) $\vdash_K x \leqslant \bar{k} \supset (x = 0 \vee x = \bar{1} \vee \ldots \vee x = \bar{k})$.

Условие (a), говорящее о выразимости в K отношений W_1 и W_2, выполнено, если эти отношения рекурсивны и если в K выразимо всякое рекурсивное отношение. Из доказательств предложений 3.25 — — 3.27 легко видеть, что W_1 и W_2 рекурсивны, если для теории K выполнено условие (d) из предложения 3.26, т. е. если свойство PrAx_K «быть гёделевым номером собственной аксиомы теории K» рекурсивно (или, иными словами, если множество гёделевых номеров собственных аксиом теории K рекурсивно). Таким образом, мы приходим к следующему результату.

Предложение 3.33. *Пусть* K *есть теория первого порядка с теми же символами, что и теория* S, *и пусть, кроме того,* K *удовлетворяет следующим условиям*:

(1) *всякое рекурсивное отношение выразимо в* K,

(2) *множество гёделевых номеров собственных аксиом теории* K *рекурсивно,*

(3) *выполнены указанные выше условия* (b), (i) — (ii).

Тогда для теории K *справедлива теорема Гёделя в форме Россера, т. е. если теория* K *непротиворечива, то существует неразрешимое в этой теории предложение.* (Заметим, что, согласно предложению 3.12, условие (1) выполняется, если в K представима каждая рекурсивная функция; кроме того, если K есть теория первого порядка с равенством, то условие (3)(b) (i) может быть заменено на (i′).)

Назовем теорию K *рекурсивно аксиоматизируемой*, если существует такая теория K′ с тем же, что и у K, множеством теорем, что множество $\mathrm{PrAx}_{K'}$ гёделевых номеров собственных аксиом K′ рекурсивно.

Следствие 3.34. *Теорема Гёделя в форме Россера справедлива для каждого непротиворечивого рекурсивно аксиоматизируемого расширения теории* S, *т. е. для каждого такого расширения существует предложение, неразрешимое в нем.*

Доказательство. Так как все рекурсивные отношения выразимы в S, то они выразимы и во всяком расширении S. Точно так же и условия (i) — (ii), будучи выполнены в S, выполнены и во всяком расширении S. Поэтому, на основании предложения 3.33, теорема Гёделя в форме Россера применима к любому непротиворечивому рекурсивно аксиоматизируемому расширению теории S.

По прочтении главы 5 читатель сможет оценить всё правдоподобие гипотезы, согласно которой точное понятие рекурсивного множества соответствует интуитивному понятию эффективно разрешимого множества. Гипотеза эта носит название тезиса Чёрча *). Для всякого, кто принимает этот тезис, следствие 3.34 утверждает, что теория S *существенно неполна,* т. е. что любое непротиворечивое эффективно аксиоматизированное расширение теории S имеет неразрешимые предложения. (Напомним, что теория называется эффективно аксиоматизированной, если существует эффективная процедура, позволяющая для каждой формулы этой теории узнавать, является ли она ее аксиомой.)

Упражнения

1. Доказать, что множество Tr гёделевых номеров всех формул теории S, истинных в стандартной модели, не является рекурсивным. (Указание. Рассмотреть теорию первого порядка K, являющуюся расширением теории S и имеющую Tr в качестве множества аксиом, и применить следствие 3.34.)

2. Опираясь на следствие 3.34, показать, что не существует рекурсивно аксиоматизируемой теории, имеющей Tr в качестве множества гёделевых номеров своих теорем.

Пусть $\mathrm{Neg}(x) = 2^3 * 2^9 * x * 2^5$. Тогда, если x есть гёделев номер формулы $\mathscr{A}$, то Neg (x) есть гёделев номер формулы $\neg\mathscr{A}$. Функция Neg, очевидно, рекурсивна и, следовательно, представима в S некоторой формулой $Neg(x_1, x_2)$. Ранее нами был введен предикат Pf (y, x), истинный тогда и только тогда, когда x есть гёделев номер некоторой формулы $\mathscr{A}$ теории S, а y есть гёделев номер некоторого вывода $\mathscr{A}$ в S. В силу предложения 3.26, предикат Pf примитивно рекурсивен, и потому, на основании следствия 3.24, выразим в S с помощью некоторой формулы $Pf(x_1, x_2)$.

Обозначим через Con_S формулу $\forall x_1 \forall x_2 \forall x_3 \forall x_4 \neg (Pf(x_1, x_3) \& Pf(x_2, x_4) \& Neg(x_3, x_4))$. Содержательно, т. е. в соответствии со стандартной интерпретацией, Con_S выражает невозможность вывода в S

*) Позже на стр. 249 тезис Чёрча будет сформулирован следующим образом: всякая арифметическая функция является эффективно вычислимой тогда и только тогда, когда она есть рекурсивная функция. Мы оставляем читателю в качестве упражнения доказать эквивалентность этих двух форм тезиса Чёрча.

какой-либо формулы вместе с ее отрицанием и является истинной в том и только в том случае, когда теория S непротиворечива. Иными словами, формулу Con_S можно интерпретировать как утверждение непротиворечивости теории S. Вспомним теперь, что, в соответствии со стандартной интерпретацией, гёделева неразрешимая формула (**) (см. стр. 159) содержательно выражает свою собственную невыводимость. Тогда формула $Con_S \supset (**)$ содержательно утверждает, что если теория S непротиворечива, то формула (**) в ней невыводима. Но в этом и состоит первая часть теоремы Гёделя. Математические рассуждения, доказывающие теорему Гёделя, могут быть выражены и проведены средствами теории S, так что в результате оказывается возможным получить вывод формулы $Con_S \supset (**)$ в теории S. (Доказательство этого утверждения см. у Гильберта и Бернайса [1939], стр. 285—328; Фефермана [1960].) Итак, $\vdash_S Con_S \supset (**)$. Согласно теореме Гёделя, однако, если теория S непротиворечива, то формула (**) в ней невыводима. Отсюда следует, что если теория S непротиворечива, то в ней невыводима и формула Con_S; иными словами, если теория непротиворечива, то в ней невыводима некоторая формула, содержательно утверждающая непротиворечивость теории S. Этот результат носит название второй теоремы Гёделя (см. Гёдель [1931]). Грубо говоря, эта теорема утверждает, что если теория S непротиворечива, то доказательство непротиворечивости теории не может быть проведено средствами самой теории S, т. е. всякое такое доказательство обязательно должно использовать невыразимые в теории S идеи или методы. Примерами тому могут служить доказательства непротиворечивости теории S, предложенные Генценом [1936], [1938b] и Шютте [1951] (см. Дополнение), в которых применяются понятия и методы (например, один фрагмент теории счетных порядковых чисел), очевидно, не формализуемые средствами теории S.

Рассмотрим следующее утверждение типа второй теоремы Гёделя: пусть Con_K есть арифметизация утверждения о том, что данная теория первого порядка K непротиворечива (при этом предполагается, что теория K содержит все предметные константы теории S); тогда если теория K достаточно сильна и непротиворечива, то формула Con_K невыводима в K. Эта теорема в действительности применима и к многим более общим теориям (не обязательно первого порядка). Однако в сформулированной таким образом второй теореме Гёделя помимо неопределенности, заключенной в словах «достаточно сильна» (которым, впрочем, нетрудно придать точный смысл), неясен также способ построения Con_K. В этом последнем обстоятельстве таится опасность, ибо, как показал Феферман [1960] (следствие 5.10), существует некоторый приемлемый способ построения Con_S, при котором $\vdash_S Con_S$. Итак, следует уточнить формулировку теоремы. Это было сделано Феферманом [1960] приблизительно следующим образом. В ходе доказательства

предложения 3.23 было показано, как для всякой примитивно рекурсивной функции $f(x_1, \ldots, x_n)$ строится формула $\mathscr{A}(x_1, \ldots, x_n, y)$, представляющая f в S. Полученные таким образом формулы $\mathscr{A}(x_1, \ldots, x_n, 0)$ назовем PR-*формулами*. Формулу $\mathscr{B}$, имеющую вид $\exists y_1 \ldots \exists y_k \mathscr{A}$, где $k \geqslant 0$ и $\mathscr{A}$ есть какая-нибудь PR-формула, назовем RE-*формулой*. В частности, всякая PR-формула является RE-формулой. Предположим теперь, что некоторая формула $\mathscr{A}(x)$ представляет теорию K, т. е. что совокупность аксиом теории K совпадает с множеством тех формул, чьи гёделевы номера удовлетворяют $\mathscr{A}$. Тогда следующим образом можно построить предикат выводимости $\mathrm{Prf}_{\mathscr{A}}(x, y)$ для теории K. Рассмотрим выражение

$$x = (y)_{\mathrm{lh}(y) \dot{-} 1} \,\&\, y > 1 \,\&\, \forall z\,(z < \mathrm{lh}(y) \supset$$
$$\supset (\mathrm{Fml}((y)_z) \,\&\, (\mathrm{LAx}((y)_z) \vee \mathscr{A}((y)_z) \vee$$
$$\vee \exists v \exists w\,(v < z \,\&\, w < z \,\&\, (\mathrm{MP}((y)_v, (y)_w, (y)_z) \vee \mathrm{Gen}((y)_v, (y)_z)))))$$

и обозначим через $Prf_{\mathscr{A}}(x, y)$ формулу, которая получится, если в этом выражении примитивно рекурсивные функции и предикаты заменить соответственно представляющими или выражающими их формулами (например, если $\mathscr{C}(u, v)$ представляет lh(y), то $z < \mathrm{lh}(y)$ заменяем на $\exists v(\mathscr{C}(y, v) \,\&\, z < v)$). Формула $Prf_{\mathscr{A}}(x, y)$ выражает в S предикат, истинный для пары (x, y) натуральных чисел тогда и только тогда, когда y есть гёделев номер вывода в теории K формулы с гёделевым номером x. (Определения отношений и функций Fml, lh, $(y)_v$, Gen, MP см. на стр. 141, 142, 153, 154.) Теперь мы можем построить и формулу $Pr_{\mathscr{A}}(x)$, соответствующую понятию теоремы теории K: такой формулой будет формула $\exists y Prf_{\mathscr{A}}(x, y)$. Наконец, через $Con_{\mathscr{A}}$ обозначим следующую формулу, выражающую непротиворечивость теории K: $\forall x\,(Fml(x) \supset \neg Pr_{\mathscr{A}}(x) \vee \exists y\,(Neg(x, y) \,\&\, \neg Pr_{\mathscr{A}}(y)))$. Одним из следствий работы Ферферман [1960] является следующий точный вариант второй теоремы Гёделя.

Пусть K — непротиворечивое расширение теории S, K_1 — любая теория, для которой K является расширением и которая сама служит расширением системы Q Робинсона*) (в частности, K_1 может совпадать с S или K), T_K — множество гёделевых номеров теорем теории K, и пусть некоторая RE-формула $\mathscr{A}(x)$ выражает T_K в K_1; тогда не $\vdash_K Con_{\mathscr{A}}$. (Условие, требующее, чтобы формула $\mathscr{A}(x)$ была RE-формулой, является здесь необходимым; это следует из существования такой формулы $\mathscr{B}(x)$, которая выражает T_S в S и для которой $\vdash_S Con_{\mathscr{B}}$ (Ферферман [1960], следствие 5.10).).

---

*) См. ниже, стр. 169. (*Прим. перев.*)

§ 6. Рекурсивная неразрешимость. Теорема Тарского. Система Робинсона

Пусть K — какая-нибудь теория первого порядка с равенством и с теми же символами, что и теория S. В предложении 3.27(18) была определена функция D(u), которая для всякого u, являющегося гёделевым номером какой-нибудь формулы $\mathscr{A}(x_1)$ со свободной переменной x_1, принимает значение, равное гёделеву номеру формулы $\mathscr{A}(\bar{u})$. Так как $D(u) = \mathrm{Sub}(u, \mathrm{Num}(u), 2^{13})$, то функция D, очевидно, примитивно рекурсивна.

Через T_K обозначим множество гёделевых номеров теорем теории K.

Предложение 3.35. *Если теория* K *непротиворечива, а функция* D *представима в* K, *то* T_K *невыразимо в* K.

Доказательство. Предположим, что функция D представима и множество T_K выразимо в теории K. Тогда существуют такие формулы $\mathscr{D}(x_1, x_2)$ и $\mathscr{T}(x_2)$, что

(1) если $D(k) = j$, то $\vdash_K \mathscr{D}(\bar{k}, \bar{j})$;
(2) $\vdash \exists_1 x_2 \mathscr{D}(\bar{k}, x_2)$;
(3) если $k \in T_K$, то $\vdash_K \mathscr{T}(\bar{k})$;
(4) если $k \notin T_K$, то $\vdash_K \neg\mathscr{T}(\bar{k})$.

Рассмотрим формулу $\mathscr{A}(x_1)$: $\forall x_2(\mathscr{D}(x_1, x_2) \supset \neg\mathscr{T}(x_2))$. Пусть p — гёделев номер этой формулы. Рассмотрим формулу $\mathscr{A}(\bar{p})$:

$$\forall x_2(\mathscr{D}(\bar{p}, x_2) \supset \neg\mathscr{T}(x_2)).$$

Пусть q — гёделев номер формулы $\mathscr{A}(\bar{p})$. Тогда $D(p) = q$. Поэтому, в силу (1), $\vdash_K \mathscr{D}(\bar{p}, \bar{q})$. Одно из двух: либо $\vdash_K \mathscr{A}(\bar{p})$, либо не $\vdash_K \mathscr{A}(\bar{p})$. Если не $\vdash_K \mathscr{A}(\bar{p})$, то $q \notin T_K$ и, согласно (4), $\vdash_K \neg\mathscr{T}(\bar{q})$. С другой стороны, если $\vdash_K \mathscr{A}(\bar{p})$, то $\vdash_K \forall x_2(\mathscr{D}(\bar{p}, x_2) \supset \neg\mathscr{T}(x_2))$. Отсюда по правилу A4 получаем $\vdash_K (\mathscr{D}(\bar{p}, \bar{q}) \supset \neg\mathscr{T}(\bar{q}))$. Однако $\vdash_K \mathscr{D}(\bar{p}, \bar{q})$. Следовательно, $\vdash_K \neg\mathscr{T}(\bar{q})$. Итак, в обоих случаях $\vdash_K \neg\mathscr{T}(\bar{q})$. Из $\vdash_K \mathscr{D}(\bar{p}, \bar{q})$ и (2) следует $\vdash_K \mathscr{D}(\bar{p}, x_2) \supset x_2 = \bar{q}$. Но так как $\vdash_K \neg\mathscr{T}(\bar{q})$, то $\vdash_K x_2 = \bar{q} \supset \neg\mathscr{T}(x_2)$. Следовательно, $\vdash_K \mathscr{D}(\bar{p}, x_2) \supset \supset \neg\mathscr{T}(x_2)$ и по правилу Gen $\vdash_K \forall x_2(\mathscr{D}(\bar{p}, x_2) \supset \neg\mathscr{T}(x_2))$, т. е. $\vdash_K \mathscr{A}(\bar{p})$. Поэтому $q \in T_K$ и, согласно (3), $\vdash_K \mathscr{T}(\bar{q})$. Но так как, кроме того, доказано, что $\vdash_K \neg\mathscr{T}(\bar{q})$, то теория K противоречива.

Следствие 3.36. *Если теория* K *непротиворечива и всякая рекурсивная функция представима в* K, *то* T_K *невыразимо в* K *и, следовательно,* T_K *нерекурсивно.*

Доказательство. Функция D примитивно рекурсивна, следовательно, представима в K. В силу предложения 3.35, множество T_K невыразимо в K. Так же, как при доказательстве предложения 3.12,

можно показать, что характеристическая функция C_{T_K} множества T_K непредставима в K. Следовательно, функция C_{T_K} нерекурсивна, а вместе с ней нерекурсивно и множество T_K.

Мы будем говорить, что теория K *рекурсивно неразрешима*, если множество T_K нерекурсивно. Теорию K назовем *существенно рекурсивно неразрешимой*, если она сама и всякое ее непротиворечивое расширение рекурсивно неразрешимы. (Если мы принимаем тезис Чёрча, то рекурсивная неразрешимость эквивалентна эффективной неразрешимости, т. е. невозможности какой бы то ни было механической разрешающей процедуры для свойства быть теоремой. Невозможность такой механической процедуры означает, что для каждой данной формулы требуются специальные усилия изобретательности для того, чтобы решить вопрос, является ли эта формула теоремой.)

Следствие 3.37. *Если теория* S *непротиворечива, то она существенно рекурсивно неразрешима.*

Доказательство. Пусть K — произвольное непротиворечивое расширение теории S (в том числе, быть может, и сама теория S). Всякая рекурсивная функция представима в S, а следовательно, и в K. Поэтому, в силу следствия 3.36, T_K нерекурсивно.

Следствие 3.38. (Теорема Тарского [1936].) *Множество* Tr *гёделевых номеров формул теории* S, *истинных в стандартной интерпретации, не является арифметическим множеством, т. е. не существует такой формулы* $\mathscr{A}(x)$ *теории* S, *чтобы* Tr *совпадало с множеством чисел* k, *для которых* $\mathscr{A}(\bar{k})$ *истинно в стандартной интерпретации.*

Доказательство. Пусть K — расширение теории S, аксиомами которого являются все те формулы, которые истинны в стандартной интерпретации. Тогда $T_K = \mathrm{Tr}$. Поскольку теория K имеет стандартную модель, мы можем считать эту теорию непротиворечивой. Согласно следствию 3.36, Tr невыразимо в K, так как всякая рекурсивная функция представима в K. Но всякое отношение выразимо в K тогда и только тогда, когда оно является стандартной интерпретацией некоторой формулы теории S. Следовательно, Tr — множество не арифметическое. (Грубо говоря, этот результат означает, что понятие арифметической истины арифметически неопределимо.)

Упражнения

1. (a) Для всякого n, являющегося гёделевым номером какой-нибудь формулы $\mathscr{A}$, определим $\mathrm{Cl}(n)$ как гёделев номер замыкания $\mathscr{A}$; в противном случае положим $\mathrm{Cl}(n) = n$. С помощью предложения 3.25 показать, что функция Cl примитивно рекурсивна.

(b) Показать, что всякая рекурсивно аксиоматизируемая и полная теория первого порядка K рекурсивно разрешима, т. е., иными словами, что для такой теории множество T_K рекурсивно. (Эквивалентное утверждение: если теория первого порядка K рекурсивно аксиоматизируема и рекурсивно неразрешима, то она неполна.) [Указание. Если n есть гёделев номер формулы $\mathscr{A}$, то

существует вывод либо замыкания $\mathscr{A}$, либо отрицания замыкания $\mathscr{A}$, т. е. $\exists y\,(\mathrm{Pf}\,(y,\ \mathrm{Cl}\,(n)) \vee \mathrm{Pf}\,(y,\ 2^3 * 2^9 * \mathrm{Cl}\,(n) * 2^5) \vee \neg\,\mathrm{Fml}\,(n))$. Обозначив последнюю формулу через $\exists y \mathrm{B}\,(y, n)$, замечаем, что, в соответствии с правилом (Vl) для μ-оператора, функция $\mu y\,(\mathrm{B}\,(y, n))$ является рекурсивной. Поэтому рекурсивен и предикат $\mathrm{Pf}\,(\mu y\,(\mathrm{B}\,(y, n)),\ \mathrm{Cl}\,(n))$. Но этот предикат эквивалентен предикату $\mathrm{Cl}\,(n) \in \mathrm{T_K}$, который в свою очередь эквивалентен предикату $n \in \mathrm{T_K}$. Это рассуждение показывает также, что всякая полная эффективно аксиоматизированная теория эффективно разрешима, т. е. что для всякой такой теории существует эффективный способ определять, является ли данная формула теоремой или нет.]

(c) Если теория K непротиворечива и рекурсивно аксиоматизируема и если в ней представима каждая рекурсивная функция, то в K существуют предложения, неразрешимые в ней.

2. Показать, что если теория K не является рекурсивно аксиоматизируемой, то она рекурсивно неразрешима.

Система Робинсона. Рассмотрим теорию первого порядка, имеющую те же символы, что и теория S, и следующее конечное число аксиом:

(1) $x_1 = x_1$;

(2) $x_1 = x_2 \supset x_2 = x_1$;

(3) $x_1 = x_2 \supset (x_2 = x_3 \supset x_1 = x_3)$;

(4) $x_1 = x_2 \supset x_1' = x_2'$;

(5) $x_1 = x_2 \supset (x_1 + x_3 = x_2 + x_3 \,\&\, x_3 + x_1 = x_3 + x_2)$;

(6) $x_1 = x_2 \supset (x_1 \cdot x_3 = x_2 \cdot x_3 \,\&\, x_3 \cdot x_1 = x_3 \cdot x_2)$;

(7) $x_1' = x_2' \supset x_1 = x_2$;

(8) $0 \neq (x_1)'$;

(9) $x_1 \neq 0 \supset \exists x_2 (x_1 = x_2')$;

(10) $x_1 + 0 = x_1$;

(11) $x_1 + (x_2)' = (x_1 + x_2)'$;

(12) $x_1 \cdot 0 = 0$;

(13) $x_1 \cdot (x_2)' = x_1 \cdot x_2 + x_1$;

(14) $(x_2 = x_1 \cdot x_3 + x_4 \,\&\, x_4 < x_1 \,\&\, x_2 = x_1 \cdot x_6 + x_5 \,\&\, x_5 < x_1) \supset x_4 = x_5$ (единственность остатка).

Мы будем называть эту теорию теорией RR. (Система Q аксиом (1)—(13) предложена Рафаэлем Робинсоном [1950]. Аксиома (14) была добавлена с целью упрощения одного из нижеследующих выводов.) Очевидно, теория RR является подтеорией теории S, поскольку все аксиомы теории RR являются теоремами теории S. Кроме того, из предложения 2.26 и наличия аксиом (1)—(6) в теории RR следует, что теория RR является теорией с равенством.

Предложение 3.39. *Следующие формулы являются теоремами теории* RR:

(a) $\bar{n} + \bar{m} = \overline{n + m}$ *для любых натуральных* n *и* m;

(b) $\bar{n} \cdot \bar{m} = \overline{n \cdot m}$ *для любых натуральных* n *и* m;

(c) $\bar{n} \neq \bar{m}$ *для любых натуральных* n *и* m, *если* $n \neq m$;

(d) $x \leqslant \bar{n} \supset x = 0 \vee x = 1 \vee \ldots \vee x = \bar{n}$ *для любого натурального* n;

(e) $x \leqslant \bar{n} \vee \bar{n} \leqslant x$ *для любого натурального* n.

Доказательство. Утверждения (a) — (c) доказываются так же как соответствующие утверждения в предложении 3.6 (a). Утверждения (d) и (e) доказываются индукцией по n в метаязыке с применением аксиомы (9). (Напомним, что выражение $x \leqslant y$, по определению означает формулу

$$x = y \vee \exists z\,(z \neq 0 \,\&\, x + z = y.)$$

Упражнения

1. Показать, что теория RR является собственной подтеорией теории S. (Указание. Рассмотреть в качестве нормальной модели теории RR (но не теории S*)) множество всех полиномов с целыми коэффициентами и неотрицательным старшим коэффициентом. Формула $\exists y\,(x = y + y \vee x = y + y + 1)$ ложна в этой модели, но выводима в теории S.) Заметим, что теория S не только не совпадает с теорией RR, но и вообще не является конечно аксиоматизируемой (т. е. не существует никакой теории с конечным числом собственных аксиом и с тем же, что у S, множеством теорем). Это утверждение было доказано Рылль-Нардзевским [1953] и Рабином [1961].

2. Показать, что аксиома (14) невыводима из аксиом (1)—(13). (Указание. Пусть ∞ — некоторый объект, не являющийся натуральным числом, и пусть $\infty' = \infty$, $\infty + x = x + \infty = \infty$ для всех x, $\infty \cdot 0 = 0 \cdot \infty = 0$ и $\infty \cdot x = x \cdot \infty = \infty$ для всех $x \neq 0$.)

Предложение 3.40. *Всякая рекурсивная функция представима в теории* RR.

Доказательство. Для исходных функций, а также для правил подстановки и μ-оператора остаются полностью в силе соответствующие рассуждения из доказательства предложения 3.23, проведенные там применительно к S. Что касается правила рекурсии, то, повторив внимательно соответствующее рассуждение в доказательстве предложения 3.23, мы убедимся, что и оно остается в силе для теории RR, так как для введенной в предложении 3.21 формулы Bt из $\beta(k_1, k_2, k_3) = m$ следует $\vdash_{RR} Bt(\bar{k}_1, \bar{k}_2, \bar{k}_3, \bar{m})$ и, в силу аксиомы (14), $\vdash_{RR} Bt(u, v, x, y)$ & & $Bt(u, v, x, z) \supset y = z$.

Упражнение

Провести во всех деталях доказательство предложения 3.40.

В той мере, в какой мы согласны считать стандартную интерпретацию моделью для теории RR, следует признать и непротиворечивость теории RR. Впрочем, следуя идеям доказательства Бета [1959, § 84] или Клини [1952, § 79], можно построить более конструктивные доказательства непротиворечивости этой теории RR.

*) См. упражнение 1 на стр. 131. (*Прим. перев.*)

Предложение 3.41.

(a) *Теория* RR *существенно рекурсивно неразрешима.*

(b) *Теория* RR *существенно рекурсивно неполна* *).

Доказательство. Утверждение (a) следует из предложения 3.40 и следствия 3.36. Утверждение (b) следует из предложений 3.33 и 3.40 (или из (a) и упражнения 1(b) на стр. 168).

Эти результаты были уже нами ранее получены для теории S. Однако воспроизвести их для теории RR представляет интерес в связи с тем, что теория RR конечно аксиоматизируема. Можно даже доказать, что предложение 3.40, а следовательно, и предложение 3.41 справедливы также и для системы Q Робинсона (аксиомы (1)—(13)), однако доказательство этого факта (см. Тарский, Мостовский и Робинсон [1953], стр. 56—59) более сложно, чем для теории RR.

Пусть K_1 и K_2 — какие-нибудь две теории первого порядка с одними и теми же символами. Теория K_2 называется *конечным расширением* теории K_1, если существуют множество A формул и конечное множество B формул такие, что (1) множество теорем теории K_1 совпадает с множеством формул, выводимых из A, (2) множество теорем теории K_2 совпадает с множеством формул, выводимых из $A \cup B$.

Две теории K_1 и K_2 называются *совместимыми*, если непротиворечива теория $K_1 \cup K_2$, т. е. теория, множество аксиом которой является объединением множеств аксиом теорий K_1 и K_2.

Предложение 3.42. *Пусть* K_1 *и* K_2 *— какие-нибудь две теории первого порядка с теми же символами, что и теория* S; *тогда если теория* K_2 *является конечным расширением теории* K_1 *и рекурсивно неразрешима, то и теория* K_1 *рекурсивно неразрешима.*

Доказательство. Пусть A — множество аксиом теории K_1 и $A \cup \{\mathscr{A}_1, \ldots, \mathscr{A}_n\}$ — множество аксиом теории K_2. Мы можем предполагать, что формулы $\mathscr{A}_1, \ldots, \mathscr{A}_n$ — замкнутые. Тогда, в силу теоремы дедукции, всякая формула $\mathscr{B}$ выводима в K_2 тогда и только тогда, когда в K_1 выводима формула $(\mathscr{A}_1 \& \ldots \& \mathscr{A}_n) \supset \mathscr{B}$. Пусть c — гёделев номер формулы $\mathscr{A}_1 \& \ldots \& \mathscr{A}_n$. Число b является гёделевым номером некоторой теоремы теории K_2 тогда и только тогда, когда число $2^3 * c * 2^{11} * b * 2^5$ является гёделевым номером какой-то теоремы теории K_1, т. е. предикат $b \in T_{K_2}$ эквивалентен предикату $2^3 * c * 2^{11} * b * 2^5 \in \in T_{K_1}$. Следовательно, если бы множество T_{K_1} было рекурсивно, то рекурсивным было бы и множество T_{K_2}, что противоречит рекурсивной неразрешимости теории K_2.

Предложение 3.43. *Всякая теория первого порядка* K, *имеющая те же символы, что и теория* S, *и совместимая с теорией* RR, *рекурсивно неразрешима.*

Доказательство. Так как теории K и RR совместимы, то теория $K \cup RR$ является непротиворечивым расширением теории RR. Поэтому,

*) Здесь автор, по-видимому, имеет в виду, что RR не имеет непротиворечивых, рекурсивно аксиоматизируемых полных расширений. (*Прим. ред.*)

на основании предложения 3.41, теория $K \cup RR$ рекурсивно неразрешима. Но эта теория является конечным расширением теории K; следовательно, в силу предложения 3.42, теория K рекурсивно неразрешима.

Следствие 3.44. *Всякая теория первого порядка* K *рекурсивно неразрешима, если она имеет те же символы, что и теория* S, *и если ее аксиомы истинны в стандартной модели.*

Доказательство. Стандартная интерпретация является моделью для теории $K \cup RR$, поэтому эта теория непротиворечива, а следовательно, теории K и RR совместимы. Теперь остается применить предложение 3.43.

Следствие 3.45. *Исчисление предикатов* P_S, *имеющее те же символы, что и теория* S, *рекурсивно неразрешимо.*

Доказательство. $P_S \cup RR = RR$. Следовательно, P_S и RR совместимы и потому, в силу предложения 3.43, P_S рекурсивно неразрешимо.

Исчисление предикатов первого порядка, содержащее все предикатные буквы A_j^n, все функциональные буквы f_j^n и все предметные константы a_j, назовем *насыщенным исчислением предикатов* (первого порядка) или исчислением PF. Исчисление предикатов первого порядка, содержащее все предикатные буквы, но не содержащее функциональных букв и предметных констант, назовем *чистым исчислением предикатов* (первого порядка) или исчислением PP.

Лемма 3.46. *Существует рекурсивная функция* h *такая, что если* u *есть гёделев номер некоторой формулы* $\mathscr{A}$ *исчисления* PF, *то* h(u) *есть гёделев номер некоторой формулы* $\mathscr{A}'$ *исчисления* PP, *причем формула* $\mathscr{A}'$ *выводима в* PP *тогда и только тогда, когда формула* $\mathscr{A}$ *выводима в* PF.

Доказательство. Пусть $\mathscr{A}$ — формула исчисления PF. Сопоставим каждой функциональной букве f_j^n из $\mathscr{A}$ какую-нибудь предикатную букву A_r^{n+1}, не входящую в $\mathscr{A}$, так, чтобы различным функциональным буквам соответствовали различные предикатные буквы, а каждой предметной константе a_j из $\mathscr{A}$ сопоставим (соблюдая аналогичное условие) не входящую в $\mathscr{A}$ предикатную букву A_k^1. Пусть a_j — первая входящая в $\mathscr{A}$ предметная константа и z — первая не входящая в $\mathscr{A}$ переменная. Определим $\mathscr{A}^*$ как результат замены каждого вхождения a_j в $\mathscr{A}$ на z. Построим формулу $\mathscr{A}_1$: $\exists z A_k^1(z) \supset \supset \exists z (A_k^1(z) \& \mathscr{A}^*)$, где A_k^1 есть предикатная буква, сопоставленная предметной константе a_j. Нетрудно проверить (см. доказательство предложения 2.29), что формула $\mathscr{A}$ логически общезначима тогда и только тогда, когда логически общезначима формула $\mathscr{A}_1$. Продолжим аналогичные преобразования до тех пор, пока не получим формулу $\mathscr{B}$ без предметных констант, логически общезначимую одновременно с $\mathscr{A}$. Пусть теперь $f_l^n(t_1, \ldots, t_n)$ — самый левый в формуле $\mathscr{B}$ терм такой, что термы $t_1, \ldots, t_n$ не содержат функциональных букв, и пусть w — первая переменная, не входящая в $\mathscr{B}$. Обозначим через $\mathscr{B}^*$ формулу,

получающуюся из формулы $\mathscr{B}$ заменой в ней каждого вхождения терма $f_l^n(t_1, \ldots, t_n)$ переменной w, и построим формулу $\mathscr{B}_1$:

$$\exists w A_r^{n+1}(w, t_1, \ldots, t_n) \supset \exists w \left(A_r^{n+1}(w, t_1, \ldots, t_n) \,\&\, \mathscr{B}^*\right),$$

где A_r^{n+1} — предикатная буква, поставленная в соответствие функциональной букве f_l^n. И в этом случае легко убедиться в том, что формула $\mathscr{B}_1$ логически общезначима тогда и только тогда, когда логически общезначима формула $\mathscr{B}$. Применим теперь аналогичное преобразование к $\mathscr{B}_1$ и т. д., пока не придем к некоторой формуле $\mathscr{A}'$, которая уже не содержит ни предметных констант, ни функциональных букв и, следовательно, является формулой исчисления PP. Формула $\mathscr{A}'$ логически общезначима тогда и только тогда, когда логически общезначима формула $\mathscr{A}$. На основании теоремы Гёделя о полноте (следствие 2.14), формула $\mathscr{A}$ логически общезначима тогда и только тогда, когда $\vdash_{\mathrm{PF}} \mathscr{A}$, а формула $\mathscr{A}'$ логически общезначима тогда и только тогда, когда $\vdash_{\mathrm{PP}} \mathscr{A}'$. Следовательно, $\vdash_{\mathrm{PF}} \mathscr{A}$ тогда и только тогда, когда $\vdash_{\mathrm{PP}} \mathscr{A}'$. Построим теперь функцию h: если u не является гёделевым номером никакой формулы исчисления PF, то положим $\mathrm{h}(\mathrm{u}) = 0$, если же u есть гёделев номер некоторой формулы $\mathscr{A}$ исчисления PF, то пусть $\mathrm{h}(\mathrm{u})$ будет гёделевым номером формулы $\mathscr{A}'$. Функция h, очевидно, эффективно вычислима; доказательство того, что она рекурсивна, мы оставляем в качестве упражнения на долю усердного читателя.

Предложение 3.47 (Теорема Чёрча [1936a].) *Исчисления* PF *и* PP *рекурсивно неразрешимы.*

Доказательство. (1) По теореме Гёделя о полноте всякая формула $\mathscr{A}$ исчисления $\mathrm{P_S}$ выводима в $\mathrm{P_S}$ тогда и только тогда, когда она логически общезначима, и эта же формула $\mathscr{A}$ выводима в PF тогда и только тогда, когда она логически общезначима. Отсюда $\vdash_{\mathrm{P_S}} \mathscr{A}$ тогда и только тогда, когда $\vdash_{\mathrm{PF}} \mathscr{A}$. Заметим, что множество $\mathrm{Fml}_{\mathrm{P_S}}$ гёделевых номеров формул исчисления $\mathrm{P_S}$ рекурсивно. Пусть $\mathrm{T_{P_S}}$ и $\mathrm{T_{PF}}$ обозначают соответственно множества гёделевых номеров теорем исчислений $\mathrm{P_S}$ и PF. Тогда $\mathrm{T_{P_S}} = \mathrm{T_{PF}} \cap \mathrm{Fml_{P_S}}$, и из рекурсивности множества $\mathrm{T_{PF}}$ следовала бы, в противоречие со следствием 3.45, рекурсивность множества $\mathrm{T_{P_S}}$. Таким образом, исчисление PF рекурсивно неразрешимо.

(2) Согласно лемме 3.46, $\mathrm{u} \in \mathrm{T_{PF}}$ тогда и только тогда, когда $\mathrm{h}(\mathrm{u}) \in \mathrm{T_{PP}}$, где h — некоторая рекурсивная функция. Поэтому, если множество $\mathrm{T_{PP}}$ рекурсивно, то рекурсивно и множество $\mathrm{T_{PF}}$, что противоречит предыдущему пункту (1). Таким образом, множество $\mathrm{T_{PP}}$ нерекурсивно, т. е. исчисление PP рекурсивно неразрешимо.

Если мы признаём тезис Чёрча, то слова «рекурсивная неразрешимость» можно всюду заменить на «эффективная неразрешимость».

В частности, предложение 3.47 утверждает, что не существует никакой эффективной разрешающей процедуры ни для чистого исчисления предикатов PP, ни для насыщенного исчисления предикатов PF. Отсюда следует и невозможность какого-либо эффективного способа узнавать, является ли данная формула логически общезначимой.

Упражнение

Показать, что в противовес теореме Чёрча чистое исчисление одноместных предикатов эффективно разрешимо. Под чистым исчислением одноместных предикатов мы здесь понимаем чистое исчисление предикатов, содержащее только одноместные предикатные буквы. [Указание. Пусть $B_1, \ldots, B_k$ — все, и притом без повторений, предикатные буквы, входящие в данную формулу $\mathscr{A}$. Тогда формула $\mathscr{A}$ общезначима в том и только в том случае, когда она истинна в каждой интерпретации, содержащей не более 2^k элементов. В самом деле, предположим, что формула $\mathscr{A}$ истинна в каждой интерпретации с не более чем 2^k элементами, и пусть M — произвольная интерпретация. Всякие два элемента b и c из области D интерпретации M назовем эквивалентными, если истинностные значения $B_1(\mathrm{b})$, $B_2(\mathrm{b})$, ..., $B_k(\mathrm{b})$ в M соответственно те же самые, что и у $B_1(\mathrm{c})$, $B_2(\mathrm{c})$, ..., $B_k(\mathrm{c})$. Введенное таким образом отношение эквивалентности разбивает D на классы эквивалентности, число которых не превышает 2^k. Рассмотрим новую интерпретацию M′ формулы $\mathscr{A}$ с областью, имеющей своими элементами эти классы эквивалентности, на которых очевидным образом определяются значения для $B_1, \ldots, B_k$. Индукцией по построению формулы $\mathscr{A}$ легко доказать, что формула $\mathscr{A}$ истинна в M тогда и только тогда, когда она истинна в M′. Так как формула $\mathscr{A}$ истинна в M′, то она истинна и в M. Итак, формула истинна во всякой интерпретации и, следовательно, в силу следствия 2.14, выводима. К этому остается добавить, что истинность формулы $\mathscr{A}$ в произвольной интерпретации, имеющей не более чем 2^k элементов, проверяется эффективно.]

Содержащийся в этом последнем упражнении результат является в некотором смысле наилучшим из возможных. В самом деле, по теореме Кальмара [1936], существует эффективная процедура, позволяющая по каждой формуле $\mathscr{A}$ чистого исчисления предикатов построить другую формулу $\mathscr{A}^*$ чистого исчисления предикатов, которая содержит единственную и притом двуместную предикатную букву и которая общезначима тогда и только тогда, когда общезначима формула $\mathscr{A}$. (Другое доказательство этого утверждения см. Чёрч [1956, § 47].) Отсюда, на основании теоремы Чёрча, следует, что не существует эффективной разрешающей процедуры для свойства общезначимости (или выводимости) формул, содержащих лишь двуместные предикатные буквы.

[D]Упражнения

(Тарский, Мостовский и Робинсон [1953], I.)

1. Пусть K* — непротиворечивая теория первого порядка, K_1 — существенно рекурсивно неразрешимая теория, всякая теорема которой является также и теоремой теории K*, и пусть понятие $\mathrm{Fml}_{K_1}(x)$ рекурсивно. Показать, что тогда теория K* существенно рекурсивно неразрешима.

2. Пусть K — теория первого порядка с равенством. Если предикатная буква A_j^n, функциональная буква f_j^n и предметная константа a_j не являются символами теории K, то под *допустимыми определениями* A_j^n, f_j^n и a_j в K мы будем понимать соответственно выражения вида

(a) $\forall x_1 \ldots \forall x_n (A_j^n(x_1, \ldots, x_n) \equiv \mathscr{A}(x_1, \ldots, x_n))$;

(b) $\forall x_1 \ldots \forall x_n \forall y (f_j^n(x_1, \ldots, x_n) = y \equiv \mathscr{B}(x_1, \ldots, x_n, y))$;

(c) $\forall y (a_j = y \equiv \mathscr{C}(y))$,

где $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ — формулы теории K, причем последние две формулы таковы, что $\vdash_K \forall x_1 \ldots \forall x_n \exists_1 y \mathscr{B}(x_1, \ldots, x_n, y)$ и $\vdash_K \exists_1 y \mathscr{C}(y)$. Доказать, что если теория K непротиворечива, то добавление к K в качестве новых аксиом любых допустимых определений приводит к непротиворечивой теории K′, которая рекурсивно неразрешима тогда и только тогда, когда рекурсивно неразрешима теория K. (Применить предложение 2.29.)

3. Назовем *нелогической константой* всякую предикатную или функциональную букву или предметную константу. Пусть K_1 — теория первого порядка с равенством и с конечным числом нелогических констант. Будем говорить, что теория K_1 *интерпретируема* в теории первого порядка K с равенством, если всякой нелогической константе теории K_1, которая не является нелогической константой теории K, можно сопоставить допустимое определение в теории K таким образом, чтобы всякая аксиома (и, следовательно, всякая теорема) теории K_1 оказалась выводимой в теории K*, получающейся из теории K добавлением к ней всех этих допустимых определений в качестве новых аксиом. Заметим, что если теория K_1 интерпретируема в теории K, то она интерпретируема во всяком расширении теории K. Если теория K_1 интерпретируема в непротиворечивой теории K и если K_1 существенно рекурсивно неразрешима, то такова же и теория K. (Указание. В силу упражнения 2, теория K* непротиворечива, следовательно, в силу упражнения 1, K* существенно рекурсивно неразрешима. Таким образом, теория K рекурсивно неразрешима на основании упражнения 2.)

4. Пусть K — теория первого порядка с равенством, A_j^1 — одноместная предикатная буква, не принадлежащая теории K, и $\mathscr{A}$ — замкнутая формула. Заменим каждую, начиная с наименьших, подформулу в $\mathscr{A}$ вида $\forall x \mathscr{B}(x)$ на $\forall x (A_j^1(x) \supset \mathscr{B}(x))$. Полученную в результате формулу $\mathscr{A}^{(A_j^1)}$ назовем релятивизацией формулы $\mathscr{A}$ посредством буквы A_j^1. Пусть $K^{A_j^1}$ — теория, аксиомами которой служат релятивизации посредством A_j^1 замыканий всех собственных аксиом теории K. (a) Теория $K^{A_j^1}$ интерпретируема в K. (Указание. Взять формулу $\forall x (A_j^1(x) \equiv x = x)$ в качестве допустимого определения для A_j^1.) (b) Теория $K^{A_j^1}$ непротиворечива тогда и только тогда, когда непротиворечива теория K. (c) Теория $K^{A_j^1}$ существенно рекурсивно неразрешима одновременно с теорией K (Тарский, Мостовский и Робинсон [1953], стр. 28).

5. Теория K называется *относительно интерпретируемой* в теории K′, если существует такая предикатная буква A_j^1, не принадлежащая теории K, что теория $K^{A_j^1}$ интерпретируема в теории K′. Если теория K относительно интерпретируема в теории K′ и существенно рекурсивно неразрешима, то и теория K′ существенно рекурсивно неразрешима. (Применить упражнения 3 и 4.)

6. Всякую теорию первого порядка K, в которой относительно интерпретируема теория RR, назовем *достаточно сильной*. Доказать, что всякая достаточно сильная непротиворечивая теория K существенно рекурсивно неразрешима, а если, кроме того, теория K рекурсивно аксиоматизируема, то она неполна. (Применить предложение 3.41(a) на стр. 170 и упражнение 1(b) на стр. 168.) Грубо говоря, теория K является достаточно сильной, если понятия натурального числа, 0, 1, сложения и умножения «определимы» в K таким образом, чтобы аксиомы теории RR (релятивизованные посредством понятия «натуральное число» в K) оказывались выводимыми. Очевидно, всякая теория, адекватная современной математике, должна быть достаточно сильной, поэтому если такая теория непротиворечива, то она рекурсивно неразрешима, а если она рекурсивно аксиоматизируема, то неполна. Для того, кто принимает тезис Чёрча, это означает, что всякая непротиворечивая достаточно сильная математическая теория эффективно неразрешима, а если она эффективно аксиоматизируема, то она будет неполна. (Аналогичные результаты верны также и для теорий высших порядков, см., например, Гёдель [1931], Хазенъегер и Шольц [1961], §§ 237—238). Все это, по-видимому, лишает нас всякой надежды на полную и непротиворечивую аксиоматизацию математики.

Глава 4

Аксиоматическая теория множеств

§ 1. Система аксиом

Значение математической логики в нашем столетии сильно возросло. Главной причиной этого явилось открытие парадоксов теории множеств и необходимость пересмотра противоречивой интуитивной теории множеств. Было предложено много различных аксиоматических теорий для обоснования теории множеств, но как бы они не отличались друг от друга своими внешними чертами, общее для всех них содержание составляют те фундаментальные теоремы, на которые в своей повседневной работе опираются математики. Выбор той или иной из имеющихся теорий является в основном делом вкуса; мы же не предъявляем к системе, которой будем пользоваться, никаких требований, кроме того, чтобы она служила достаточной основой для построения современной математики.

Мы опишем теорию первого порядка NBG, которая в основном является системой того же типа, что и система, предложенная первоначально фон Нейманом [1925], [1928], а затем тщательно пересмотренная и упрощенная Р. Робинсоном [1937], Бернайсом [1937—1954] и Гёделем [1940]. (Мы будем в основном следовать монографии Гёделя, хотя и с некоторыми важными отклонениями.) Теория NBG имеет единственную предикатную букву A_2^2 и не имеет ни одной функциональной буквы или предметной константы. Чтобы быть ближе к обозначениям Бернайса [1937—1954] и Гёделя [1940], мы будем употреблять в качестве переменных вместо x_1, x_2, ... прописные латинские буквы X_1, X_2, ... (Как обычно, мы используем буквы X, Y, Z, ... для обозначения произвольных переменных.) Мы введем также сокращенные обозначения $X \in Y$ для $A_2^2(X, Y)$ и $X \notin Y$ для $\neg A_2^2(X, Y)$. Содержательно знак $\in$ понимается как символ отношения принадлежности.

Следующим образом определим *равенство*:

Определение. $X = Y$ служит сокращением для формулы $\forall Z(Z \in X \equiv Z \in Y)$.

Таким образом, два объекта равны тогда и только тогда, когда они состоят из одних и тех же элементов.

Определение. $X \subseteq Y$ служит сокращением для формулы $\forall Z(Z \in X \supset Z \in Y)$ (*включение*).

Определение. $X \subset Y$ служит сокращением для $X \subseteq Y \,\&\, X \neq Y$ (*собственное включение*).

Из этих определений легко следует

Предложение 4.1.

(a) $\vdash X = Y \equiv (X \subseteq Y \,\&\, Y \subseteq X)$;
(b) $\vdash X = X$;
(c) $\vdash X = Y \supset Y = X$;
(d) $\vdash X = Y \supset (Y = Z \supset X = Z)$;
(e) $\vdash X = Y \supset (Z \in X \supset Z \in Y)$.

Мы теперь приступим к перечислению собственных аксиом теории NBG, перемежая формулировки самих аксиом различными следствиями из них и некоторыми дополнительными определениями. Предварительно, однако, отметим, что в той «интерпретации», которая здесь подразумевается, значениями переменных являются *классы*. Классы — это совокупности, соответствующие некоторым, однако отнюдь не всем, свойствам *). (Эта «интерпретация» столь же неточна, как и понятия «совокупность», «свойство» и т. д.)

Назовем класс *множеством*, если он является элементом какого-нибудь класса. Класс, не являющийся множеством, назовем *собственным классом*.

Определение. $M(X)$ служит сокращением для $\exists Y(X \in Y)$ (X есть множество).

Определение. $Pr(X)$ служит сокращением для $\neg M(X)$ (X есть собственный класс).

В дальнейшем мы увидим, что обычные способы вывода парадоксов приводят теперь уже не к противоречию, а всего лишь к результату, состоящему в том, что некоторые классы не являются множествами. Множества предназначены быть теми надежными, удобными классами, которыми математики пользуются в своей повседневной деятельности; в то время как собственные классы мыслятся как чудовищно необъятные собрания, которые, если позволить им быть множествами (т. е. быть элементами других классов), порождают противоречия.

Упражнение

$\vdash Y \in X \supset M(Y)$.

Система NBG задумана как теория, трактующая о классах, а не о предметах. Мотивом в пользу этого послужило то обстоятельство, что математика не нуждается в объектах, не являющихся классами, вроде коров или молекул. Все математические объекты и отношения могут быть выражены в терминах одних только классов. Если же ради при-

*) Те свойства, которые фактически определяют классы, будут частично указаны в аксиомах. Эти аксиомы обеспечивают нам существование необходимых в математике классов и являются, как мы надеемся, достаточно скромными, чтобы из них нельзя было вывести противоречие.

ложений в других науках возникает необходимость привлечения «неклассов», то незначительная модификация системы NBG позволяет применить ее равным образом как к классам, так и к «неклассам» (Мостовский [1939]).

Мы введем строчные латинские буквы $x_1, x_2, \ldots$ в качестве специальных, ограниченных множествами, переменных. Иными словами, $\forall x_1 \mathscr{A}(x_1)$ будет служить сокращением для $\forall X(M(X) \supset \mathscr{A}(X))$, что содержательно имеет следующий смысл: «$\mathscr{A}$ истинно для всех множеств», и $\exists x_1 \mathscr{A}(x_1)$ будет служить сокращением для $\exists X(M(X) \& \mathscr{A}(X))$, что содержательно имеет смысл: «$\mathscr{A}$ истинно для некоторого множества». Заметим, что употребленная в этом определении переменная X должна быть отличной от переменных, входящих в $\mathscr{A}(x_1)$. (Как и обычно, буквы $x, y, z, \ldots$ будут употребляться для обозначения произвольных переменных для множеств.)

Пример. Выражение $\forall X \forall x \exists y \exists Z \mathscr{A}(X, x, y, Z)$ служит сокращением для

$$\forall X \forall X_j (M(X_j) \supset \exists Y (M(Y) \& \exists Z \mathscr{A}(X, X_j, Y, Z))).$$

Упражнение

$\vdash X = Y \equiv \forall z (z \in X \equiv z \in Y)$.

Аксиома T. (*Аксиома объемности.*) $X = Y \supset (X \in Z \equiv Y \in Z)$.

Предложение 4.2. *Система* NBG *является теорией первого порядка с равенством.*

Доказательство. Предложение 4.1, аксиома T и замечание на стр. 90 о теориях, в которых равенство может быть определено.

Упражнение

$\vdash M(Z) \& Z = Y \supset M(Y)$.

Аксиома P. (*Аксиома пары.*) $\forall x \forall y \exists z \forall u (u \in z \equiv u = x \vee u = y)$, т. е. для любых множеств x и y существует множество z такое, что x и y являются единственными его элементами.

Упражнения

1. $\vdash \forall x \forall y \exists_1 z \forall u (u \in z \equiv u = x \vee u = y)$, т. е. для любых двух множеств x и y существует единственное множество z, называемое *неупорядоченной парой* элементов x и y, элементами которого являются x и y и только они.

2. $\vdash \forall X (M(X) \equiv \exists y (X \in y))$.

Аксиома N. (*Аксиома пустого множества.*) $\exists x \forall y (y \notin x)$, т. е. существует множество, не содержащее никаких элементов.

Из аксиомы N и аксиомы объемности следует, что существует лишь единственное множество, не содержащее никаких элементов, т. е.

$\vdash \exists_1 x\, \forall y\, (y \notin x)$. Поэтому мы можем ввести предметную константу 0, подчинив ее следующему условию.

Определение. $\forall y\, (y \notin 0)$.

Так как выполнено условие единственности для неупорядоченной пары, то мы можем ввести новую функциональную букву $g(x, y)$ для обозначения неупорядоченной пары x и y. Впрочем вместо $g(x, y)$ мы будем писать $\{x, y\}$. Заметим, что можно однозначно определить пару $\{X, Y\}$ для любых двух классов X и Y, а не только для множеств x и y. Положим $\{X, Y\} = 0$, если один из классов X, Y не является множеством. Можно доказать, что

$$\vdash_{\text{NBG}} \exists_1 Z((M(X) \& M(Y) \& \forall u\, (u \in Z \equiv u = X \vee u = Y)) \vee \vee ((\neg M(X) \vee \neg M(Y)) \& Z = 0)).$$

Этим оправдано введение пары $\{X, Y\}$:

Определение. $(M(X) \& M(Y) \& \forall u\, (u \in \{X, Y\} \equiv \equiv u = X \vee u = Y)) \vee ((\neg M(X) \vee \neg M(Y)) \& \{X, Y\} = 0)$.

Можно доказать, что $\vdash_{\text{NBG}} \forall x\, \forall y\, \forall u\, (u \in \{x, y\} \equiv u = x \vee u = y)$ и $\vdash_{\text{NBG}} \forall x\, \forall y\, (M(\{x, y\}))$.

В связи с этим определением читателю следует вернуться к § 9 гл. 2 и, в частности, к предложению 2.29, которое гарантирует нам, что введение новых предметных констант и функциональных букв, таких как 0 и $\{X, Y\}$, ничего существенно нового к теории NBG не добавляет.

Упражнения

1. $\vdash \{X, Y\} = \{Y, X\}$. (В дальнейшем на протяжении настоящей главы индекс NBG в записи $\vdash_{\text{NBG}}$ опускается.)

2. Определим $\{X\}$ как $\{X, X\}$. Тогда $\vdash \forall x\, \forall y\, (\{x\} = \{y\} \supset x = y)$.

Определение. $\langle X, Y\rangle = \{\{X\}, \{X, Y\}\}$. $\langle X, Y\rangle$ называется *упорядоченной парой* классов X и Y.

Никакого внутреннего интуитивного смысла это определение не имеет. Оно является лишь некоторым удобным способом (его предложил Куратовский) определить упорядоченные пары таким образом, чтобы можно было доказать следующее предложение, выражающее характеристическое свойство упорядоченных пар.

Предложение 4.3.

$\vdash \forall x\, \forall y\, \forall u\, \forall v\, (\langle x, y\rangle = \langle u, v\rangle \supset x = u \& y = v)$.

Доказательство. Пусть $\langle x, y\rangle = \langle u, v\rangle$. Это значит, что $\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$. Так как $\{x\} \in \{\{x\}, \{x, y\}\}$, то $\{x\} \in \{\{u\}, \{u, v\}\}$. Поэтому $\{x\} = \{u\}$ или $\{x\} = \{u, v\}$. В обоих случаях $x = u$. С другой стороны, $\{u, v\} \in \{\{u\}, \{u, v\}\}$ и, следовательно, $\{u, v\} \in \{\{x\}, \{x, y\}\}$. Отсюда $\{u, v\} = \{x\}$ или $\{u, v\} = \{x, y\}$. Подобным же образом, $\{x, y\} = \{u\}$ или $\{x, y\} = \{u, v\}$. Если $\{u, v\} = \{x\}$ и $\{x, y\} = \{u\}$, то $x = u = y = v$; в противном случае $\{u, v\} = \{x, y\}$ и, сле-

довательно, $\{u, v\} = \{u, y\}$. Если при этом $v \neq u$, то $y = v$, если же $v = u$, то тоже $y = v$. Итак, в любом случае, $y = v$.

Мы теперь обобщим понятие упорядоченной пары до понятия упорядоченной n-ки.

Определение

$$\langle X \rangle = X,$$

$$\langle X_1, \ldots, X_{n+1} \rangle = \langle \langle X_1, \ldots, X_n \rangle, X_{n+1} \rangle.$$

Так, например,

$$\langle X, Y, Z \rangle = \langle \langle X, Y \rangle, Z \rangle \text{ и } \langle X, Y, Z, U \rangle = \langle \langle \langle X, Y \rangle, Z \rangle, U \rangle.$$

Нетрудно доказать следующее обобщение предложения 4.3:

$$\vdash \forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n (\langle x_1, \ldots, x_n \rangle = \langle y_1, \ldots, y_n \rangle \supset \supset x_1 = y_1 \& \ldots \& x_n = y_n).$$

Аксиомы существования классов. Эти аксиомы утверждают, что для некоторых свойств, выраженных формулами, существуют соответствующие классы всех множеств, обладающих этими свойствами.

Аксиома B1. $\exists X \forall u \forall v (\langle u, v \rangle \in X \equiv u \in v)$ (*$\in$-отношение*).
Аксиома B2. $\forall X \forall Y \exists Z \forall u (u \in Z \equiv u \in X \& u \in Y)$ (*пересечение*).
Аксиома B3. $\forall X \exists Z \forall u (u \in Z \equiv u \notin X)$ (*дополнение*).
Аксиома B4. $\forall X \exists Z \forall u (u \in Z \equiv \exists v (\langle u, v \rangle \in X))$ (*область определения*).
Аксиома B5. $\forall X \exists Z \forall u \forall v (\langle u, v \rangle \in Z \equiv u \in X)$.
Аксиома B6. $\forall X \exists Z \forall u \forall v \forall w (\langle u, v, w \rangle \in Z \equiv \langle v, w, u \rangle \in X)$.
Аксиома B7. $\forall X \exists Z \forall u \forall v \forall w (\langle u, v, w \rangle \in Z \equiv \langle u, w, v \rangle \in X)$.

С помощью аксиом B2—B4 можно доказать

$$\vdash \forall X \forall Y \exists_1 Z \forall u (u \in Z \equiv u \in X \& u \in Y),$$
$$\vdash \forall X \exists_1 Z \forall u (u \in Z \equiv u \notin X),$$
$$\vdash \forall X \exists_1 Z \forall u (u \in Z \equiv \exists v (\langle u, v \rangle \in X)).$$

Эти результаты оправдывают введение новых функциональных букв $\cap$, $^-$, $\mathscr{D}$.

Определения

$\forall u (u \in X \cap Y \equiv u \in X \& u \in Y)$	(*пересечение классов X и Y*).
$\forall u (u \in \bar{X} \equiv u \notin X)$	(*дополнение к классу X*).
$\forall u (u \in \mathscr{D}(X) \equiv \exists v (\langle u, v \rangle \in X))$	(*область определения класса X*).
$X \cup Y \equiv (\bar{X} \cap \bar{Y})$	(*объединение классов X и Y*).
$V = 0$	(*универсальный класс*).
$X - Y = X \cap \bar{Y}$.	

Упражнения

1. $\vdash \forall u\,(u\in X\cup Y \equiv u\in X \vee u\in Y)$,
$\vdash \forall u\,(u\in V)$.

2.

$\vdash X\cap Y = Y\cap X$	$\vdash X\cup Y = Y\cup X$
$\vdash (X\cap Y)\cap Z = X\cap(Y\cap Z)$	$\vdash (X\cup Y)\cup Z = X\cup(Y\cup Z)$
$\vdash X\cap X = X$	$\vdash X\cup X = X$
$\vdash X\cap 0 = 0$	$\vdash X\cup 0 = X$
$\vdash X\cap V = X$	$\vdash X\cup V = V$
$\vdash X\cap(Y\cup Z) = (X\cap Y)\cup(X\cap Z)$	$\vdash X\cup(Y\cap Z) = (X\cup Y)\cap(X\cup Z)$
$\vdash \overline{X\cup Y} = \bar{X}\cap\bar{Y}$	$\vdash \overline{X\cap Y} = \bar{X}\cup\bar{Y}$
$\vdash X - X = 0$	$\vdash V - X = \bar{X}$
$\vdash \bar{\bar{X}} = X$	$\vdash \bar{V} = 0$

3. (a) $\vdash \forall X\,\exists Z\,\forall u\,\forall v\,(\langle u, v\rangle\in Z \equiv \langle v, u\rangle \in X)$. (Указание. Применить последовательно аксиомы B5, B7, B6, B4.)

(b) $\vdash \forall X\,\exists Z\,\forall u\,\forall v\,\forall w\,(\langle u, v, w\rangle\in Z \equiv \langle u, w\rangle\in X)$. (Указание. Применить B5 и B7.)

(c) $\vdash \forall X\,\exists Z\,\forall v\,\forall x_1 \ldots \forall x_n\,(\langle x_1, \ldots, x_n, v\rangle\in Z \equiv \langle x_1, \ldots, x_n\rangle\in X)$. (Применить B5.)

(d) $\vdash \forall X\exists Z\forall v_1 \ldots \forall v_m\forall x_1 \ldots \forall x_n\,(\langle x_1, \ldots, x_n, v_1, \ldots, v_m\rangle\in Z \equiv \langle x_1, \ldots, x_n\rangle\in X)$. (Указание. Итерация (c).)

(e) $\vdash \forall X\exists Z\forall v_1 \ldots \forall v_m\forall x_1 \ldots \forall x_n\,(\langle x_1, \ldots, x_{n-1}, v_1, \ldots, v_m, x_n\rangle\in Z \equiv \equiv \langle x_1, \ldots, x_n\rangle\in X)$. (Указание. При $m = 1$ из (b) подстановкой $\langle x_1, \ldots, x_{n-1}\rangle$ вместо u и x_n вместо w, а затем общий случай — итерацией.)

(f) $\vdash \forall X\exists Z\forall x\forall v_1 \ldots \forall v_m\,(\langle v_1, \ldots, v_m, x\rangle\in Z \equiv x\in X)$. (Указание. Использовать B5 и пункт (a).)

(g) $\vdash \forall X\exists Z\forall x_1 \ldots \forall x_n\,(\langle x_1, \ldots, x_n\rangle\in Z \equiv \exists y\,(\langle x_1, \ldots, x_n, y\rangle\in X))$. (Указание. Следует из B4 подстановкой $\langle x_1, \ldots, x_n\rangle$ вместо u и y вместо v.)

(h) $\vdash \forall X\exists Z\forall u\forall v\forall w\,(\langle v, u, w\rangle\in Z \equiv \langle u, w\rangle\in X)$. (Указание. Подставить $\langle u, w\rangle$ вместо u в аксиому B5 и применить аксиому B6.)

(i) $\vdash \forall X\exists Z\forall v_1 \ldots \forall v_k\forall u\forall w\,(\langle v_1, \ldots, v_k, u, w\rangle\in Z \equiv \langle u, w\rangle\in X)$. (Указание. Подставить $\langle v_1, \ldots, v_k\rangle$ вместо v в (h).)

Мы теперь можем доказать некоторую общую теорему о существовании классов.

Предложение 4.4. *Пусть* $\varphi(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$ *— формула, переменные которой берутся лишь из числа* $X_1, \ldots, X_n, Y_1, \ldots, Y_m$. *Назовем такую формулу* предикативной, *если в ней связанными являются только переменные для множеств (т. е. если она может быть приведена к такому виду с помощью принятых сокращений). Для всякой предикативной формулы* $\varphi(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$

$$\vdash \exists Z\forall x_1 \ldots \forall x_n\,(\langle x_1, \ldots, x_n\rangle \in Z \equiv \varphi(x_1, \ldots, x_n, Y_1, \ldots, Y_m)).$$

Доказательство. Мы можем ограничиться рассмотрением только таких формул φ, которые не содержат подформул вида $Y_i \in W$, так как всякая такая подформула может быть заменена на $\exists x\,(x = Y_i \,\&\, x \in W)$, что в свою очередь эквивалентно формуле $\exists x\,(\forall z\,(z \in x \equiv z \in Y_i)\,\&$

$\& x \in W$). Можно также предполагать, что в φ не содержатся подформулы вида $X \in X$, которые могут быть заменены на $\exists u (u = X \,\&\, u \in X)$, последнее же эквивалентно $\exists u (\forall z (z \in u \equiv z \in X) \,\&\, u \in X)$. Доказательство проведем теперь индукцией по числу k логических связок и кванторов, входящих в формулу φ (записанную с ограниченными переменными для множеств).

1. Пусть $k = 0$. Формула φ имеет вид $x_i \in x_j$, или $x_j \in x_i$, или $x_i \in Y_l$, где $1 \leqslant i < j \leqslant n$. В первом случае, по аксиоме B1, существует некоторый класс W_1 такой, что

$$\forall x_i \forall x_j (\langle x_i, x_j \rangle \in W_1 \equiv x_i \in x_j).$$

Во втором случае, по той же аксиоме, существует класс W_2 такой, что

$$\forall x_i \forall x_j (\langle x_j, x_i \rangle \in W_2 \equiv x_j \in x_i),$$

и тогда, в силу упражнения 3 (a) на стр. 182, существует класс W_3 такой, что

$$\forall x_i \forall x_j (\langle x_i, x_j \rangle \in W_3 \equiv x_j \in x_i).$$

Итак, в любом из первых двух случаев существует класс W такой, что

$$\forall x_i \forall x_j (\langle x_i, x_j \rangle \in W \equiv \varphi (x_1, \ldots, x_n, Y_1, \ldots, Y_m)).$$

Тогда, заменив в упражнении 3 (i) на стр. 182 X на W, получим, что существует некоторый класс Z_1 такой, что

$$\forall x_1 \ldots \forall x_{i-1} \forall x_i \forall x_j (\langle x_1, \ldots, x_{i-1}, x_i, x_j \rangle \in Z_1 \equiv \equiv \varphi (x_1, \ldots, x_n, Y_1, \ldots, Y_m)).$$

Далее, на основании упражнения 3 (e) там же при $Z_1 = X$, заключаем, что существует класс Z_2 такой, что

$$\forall x_1 \ldots \forall x_i \forall x_{i+1} \ldots \forall x_j (\langle x_1, \ldots, x_j \rangle \in Z_2 \equiv \varphi (x_1, \ldots, x_n, Y_1, \ldots, Y_m)).$$

Наконец, применяя упражнение 3 (d) там же при $Z_2 = X$, получаем, что существует класс Z такой, что

$$\forall x_1 \ldots \forall x_n (\langle x_1, \ldots, x_n \rangle \in Z \equiv \varphi (x_1, \ldots, x_n, Y_1, \ldots, Y_m)).$$

Для остающегося случая $x_i \in Y_l$ теорема следует из упражнений 3 (f) и 3 (d).

2. Предположим, что теорема доказана для любого $k < s$ и что φ содержит s логических связок и кванторов.

(a) φ есть $\neg \psi$. По индуктивному предположению, существует класс W такой, что

$$\forall x_1 \ldots \forall x_n (\langle x_1, \ldots, x_n \rangle \in W \equiv \psi (x_1, \ldots, x_n, Y_1, \ldots, Y_m)).$$

Теперь остается положить $Z = \overline{W}$.

(b) φ есть $\psi \supset \theta$. По индуктивному предположению, существуют классы Z_1 и Z_2 такие, что

$$\forall x_1 \ldots \forall x_n (\langle x_1, \ldots, x_n \rangle \in Z_1 \equiv \psi (x_1, \ldots, x_n, Y_1, \ldots, Y_m))$$

и

$$\forall x_1 \ldots \forall x_n (\langle x_1, \ldots, x_n \rangle \in Z_2 \equiv \theta(x_1, \ldots, x_n, Y_1, \ldots, Y_m)).$$

Искомым классом Z в этом случае будет класс $\overline{(Z_1 \cap \overline{Z_2})}$.

(c) φ есть $\forall x \psi$. По индуктивному предположению, существует класс W такой, что

$$\forall x_1 \ldots \forall x_n \forall x (\langle x_1, \ldots, x_n, x \rangle \in W \equiv \psi(x_1, \ldots, x_n, x, Y_1, \ldots, Y_m)).$$

Применим сперва упражнение 3(g) при $X = \overline{W}$ и получим класс Z_1 такой, что

$$\forall x_1 \ldots \forall x_n (\langle x_1, \ldots, x_n \rangle \in Z_1 \equiv \exists x \neg \psi(x_1, \ldots, x_n, x, Y_1, \ldots, Y_m)).$$

Теперь положим окончательно $Z = \overline{Z_1}$, замечая, что $\forall x \psi$ эквивалентно $\neg \exists x \neg \psi$.

Примеры. 1. Пусть $\varphi(X, Y_1, Y_2)$ есть формула $\exists u \exists v (X = \langle u, v \rangle \& u \in Y_1 \& v \in Y_2)$. Здесь кванторы связывают только переменные для множеств. Поэтому, в силу теоремы о существовании классов, $\vdash \exists Z \forall x (x \in Z \equiv \exists u \exists v (x = \langle u, v \rangle \& u \in Y_1 \& v \in Y_2))$, а на основании аксиомы объемности, $\vdash \exists_1 Z \forall x (x \in Z \equiv \exists u \exists v (x = \langle u, v \rangle \& u \in Y_1 \& v \in Y_2))$. Поэтому возможно следующее определение, вводящее новую функциональную букву $\times$:

Определение. $\forall x (x \in Y_1 \times Y_2 \equiv \exists u \exists v (x = \langle u, v \rangle \& u \in Y_1 \& v \in Y_2)$. (*Декартово произведение* классов Y_1 и Y_2.)

Определения.

X^2 обозначает $X \times X$ (в частности, V^2 обозначает класс всех упорядоченных пар).

. . . . . .

X^n обозначает $X^{n-1} \times X$ (в частности, V^n обозначает класс всех упорядоченных n-ок).

$Rel(X)$ служит сокращением для $X \subseteq V^2$ (X есть отношение).

2. Пусть $\varphi(X, Y)$ обозначает $X \subseteq Y$. По теореме о существовании классов и на основании аксиомы объемности, $\vdash \exists_1 Z \forall x (x \in Z \equiv x \subseteq Y)$. Таким образом, существует класс Z, элементами которого являются все подмножества класса Y.

Определение. $\forall x (x \in \mathcal{P}(Y) \equiv x \subseteq Y)$. ($\mathcal{P}(Y)$: *класс всех подмножеств класса* Y.)

3. Рассмотрим в качестве $\varphi(X, Y)$ формулу $\exists v (X \in v \& v \in Y)$. По теореме о существовании классов и на основании аксиомы объемности, $\vdash \exists_1 Z \forall x (x \in Z \equiv \exists v (x \in v \& v \in Y))$, т. е. существует единственный класс Z, элементами которого являются все элементы элементов класса Y и только они.

Определение. $\forall x (x \in \bigcup(Y) \equiv \exists v (x \in v \& v \in Y))$. ($\bigcup(Y)$: *объединение всех элементов класса* Y.)

4. Пусть $\varphi(X)$ есть $\exists u (X = \langle u, u \rangle)$. По теореме о существовании классов и на основании аксиомы объемности, существует единственный класс Z такой, что $\forall x (x \in Z \equiv \exists u (x = \langle u, u \rangle))$.

Определение. $\forall x (x \in I \equiv \exists u (x = \langle u, u \rangle))$. (*Отношение тождества.*)

Следствие 4.5. *Для всякой предикативной формулы* $\varphi(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$

$$\vdash \exists_1 W (W \subseteq V^n \,\&\, \forall x_1 \ldots \forall x_n (\langle x_1, \ldots, x_n \rangle \in W \equiv \equiv \varphi(x_1, \ldots, x_n, Y_1, \ldots, Y_m)).$$

Доказательство. В силу предложения 4.4, существует класс Z, для которого $\forall x_1 \ldots \forall x_n (\langle x_1, \ldots, x_n \rangle \in Z \equiv \varphi(x_1, \ldots, x_n, Y_1, \ldots, Y_m))$. Очевидно, искомым классом W является класс $W = Z \cap V^n$; его единственность вытекает из аксиомы объемности.

Определение. Для всякой предикативной формулы $\varphi(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$ через $\hat{x}_1 \ldots \hat{x}_n \varphi(x_1, \ldots, x_n, Y_1, \ldots, Y_m)$ обозначается класс всех n-ок $\langle x_1, \ldots, x_n \rangle$, удовлетворяющих формуле $\varphi(x_1, \ldots, x_n, Y_1, \ldots, Y_m)$, т. е. $\forall u (u \in \hat{x}_1 \ldots \hat{x}_n \varphi(x_1, \ldots, x_n, Y_1, \ldots, Y_m) \equiv \exists x_1 \ldots \exists x_n (u = \langle x_1, \ldots, x_n \rangle \,\&\, \varphi(x_1, \ldots, x_n, Y_1, \ldots, Y_m)))$. Следствие 4.5 оправдывает такое определение. В частности, при $n = 1$ получим $\vdash \forall u (u \in \hat{x} \varphi(x, Y_1, \ldots, Y_m) \equiv \varphi(u, Y_1, \ldots, Y_m))$ *).

Примеры. 1. Пусть φ есть $\langle x_2, x_1 \rangle \in Y$. Обозначим $\hat{x}_1 \hat{x}_2 (\langle x_2, x_1 \rangle \in Y)$ сокращенно через $\breve{Y}$, тогда $\vdash \breve{Y} \subseteq V^2 \,\&\, \forall x_1 \forall x_2 (\langle x_1, x_2 \rangle \in \breve{Y} \equiv \langle x_2, x_1 \rangle \in Y)$. Назовем $\breve{Y}$ *обратным отношением* класса Y.

2. Пусть φ есть $\exists v (\langle v, x \rangle \in Y)$. Обозначим через $\mathscr{R}(Y)$ выражение $\hat{x} (\exists v (\langle v, x \rangle \in Y))$. Тогда $\vdash \forall u (u \in \mathscr{R}(Y) \equiv \exists v (\langle v, u \rangle \in Y))$. Класс $\mathscr{R}(Y)$ называется *областью значений* класса Y. Очевидно, $\vdash \mathscr{R}(Y) = \mathscr{D}(\breve{Y})$.

Заметим, что аксиомы B1—B7 являются частными случаями теоремы о существовании классов, т. е. предложения 4.4. Иными словами, вместо того, чтобы выдвигать предложение 4.4 в качестве схемы аксиом, можно с тем же результатом ограничиться лишь некоторым конечным числом его частных случаев. Вместе с тем, хотя предложение 4.4 и позволяет доказывать существование большого числа самых разнообразных классов, нам, однако, ничего еще не известно о существовании каких-либо множеств, кроме самых простых множеств таких, как 0, $\{0\}$, $\{0, \{0\}\}$, $\{\{0\}\}$ и т. д. Чтобы обеспечить существование множеств более сложной структуры, мы введем дальнейшие аксиомы.

Аксиома U. (*Аксиома объединения.*)

$$\forall x \exists y \forall u (u \in y \equiv \exists v (u \in v \,\&\, v \in x)).$$

Эта аксиома утверждает, что объединение $\bigcup(x)$ всех элементов множества x (см. пример 3 на стр. 184) является также множеством, т. е. $\vdash \forall x (M(\bigcup(x)))$. Множество $\bigcup(x)$ обозначают также через $\bigcup\limits_{v \in x} v$.

---

*) Иногда вместо $\hat{x}_1 \ldots \hat{x}_n \varphi(x_1, \ldots, x_n, Y_1, \ldots, Y_m)$ применяют запись $\{\langle x_1, \ldots, x_n \rangle \mid \varphi(x_1, \ldots, x_n, Y_1, \ldots, Y_m)\}$.

Упражнения

1. Показать, что $\vdash \forall x \forall y (\mathbf{U}(\{x, y\}) = x \cup y)$ и, следовательно, $\vdash \forall x \forall y (M(x \cup y))$.
2. (a) $\vdash \mathbf{U}(0) = 0$. (b) $\vdash \mathbf{U}(\{0\}) = 0$. (c) $\vdash \forall x (\mathbf{U}(\{x\}) = x)$. (d) $\vdash \forall x \forall y (\mathbf{U}(\langle x, y\rangle) = \{x, y\})$.
3. Определим по индукции $\{x_1, \ldots, x_n\}$ как $\{x_1, \ldots, x_{n-1}\} \cup \{x_n\}$. Тогда $\vdash \forall x_1 \ldots \forall x_n \forall u (u \in \{x_1, \ldots, x_n\} \equiv u = x_1 \vee \ldots \vee u = x_n)$. Таким образом, для любых данных множеств $x_1, \ldots, x_n$ существует множество, элементами которого являются множества $x_1, \ldots, x_n$ и только они.

Другим средством порождения новых множеств из уже имеющихся является образование множества всех подмножеств данного множества.

Аксиома W. (*Аксиома множества всех подмножеств.*)

$$\forall x \exists y \forall u (u \in y \equiv u \subseteq x).$$

Эта аксиома утверждает, что класс всех подмножеств множества x (см. пример 2 на стр. 184) есть также множество; мы его будем называть *множеством всех подмножеств множества* x. В силу этой аксиомы, $\vdash \forall x (M(\mathscr{P}(x)))$.

Примеры.

$$\vdash \mathscr{P}(0) = \{0\}.$$
$$\vdash \mathscr{P}(\{0\}) = \{0, \{0\}\}.$$
$$\vdash \mathscr{P}(\{0, \{0\}\}) = \{0, \{0\}, \{0, \{0\}\}, \{\{0\}\}\}.$$

Значительно более общим средством построения новых множеств является следующая *аксиома выделения.*

Аксиома S. $\forall x \forall Y \exists z \forall u (u \in z \equiv u \in x \,\&\, u \in Y)$.

Таким образом, для любого множества x и для любого класса Y существует множество, состоящее из элементов, общих для x и Y. Следовательно, $\vdash \forall x \forall Y (M(x \cap Y))$, т. е. пересечение множества с классом есть множество.

Предложение 4.6. $\vdash \forall x \forall Y (Y \subseteq x \supset M(Y))$ (т. е. подкласс множества есть множество).

Доказательство. $\vdash \forall x (Y \subseteq x \supset Y \cap x = Y)$ и $\vdash \forall x (M(Y \cap x))$.

Так как всякая предикативная формула $\mathscr{A}(y)$ порождает соответствующий класс (предложение 4.4), то из аксиомы S следует, что для любого множества x класс всех его элементов, удовлетворяющих данной предикативной формуле $\mathscr{A}(y)$, есть множество.

Однако для полного развития теории множеств нам потребуется аксиома, более сильная, чем аксиома S. Введем предварительно несколько определений.

Определения

$Un(X)$ означает $\forall x \forall y \forall z (\langle x, y\rangle \in X \,\&\, \langle x, z\rangle \in X \supset y = z)$. (*$X$ однозначен.*)

$Fnc(X)$ означает $X \subseteq V^2 \,\&\, Un(X)$. (*$X$ есть функция.*)

$Y \restriction X$ означает $X \cap (Y \times V)$. (*Ограничение X областью Y.*)

$Un_1(X)$ означает $Un(X) \& Un(\breve{X})$. (*X взаимно однозначен.*)

$$X`Y = \begin{cases} z, & \text{если } \forall u(\langle Y, u\rangle \in X \equiv u = z), \\ 0 & \text{в противном случае.} \end{cases}$$

Если существует единственное z такое, что $\langle y, z\rangle \in X$, то $z = X`y$; в противном случае $X`y = 0$. Если X есть функция, а y — множество из области определения X, то $X`y$ есть значение этой функции, примененной к y *).

$X``Y = \mathscr{R}(Y \restriction X)$. (Если $X$ есть функция, то $X``Y$ есть область значений класса X, ограниченного областью Y.)

Аксиома R. (*Аксиома замещения.*)

$$\forall x(Un(X) \supset \exists y \forall u(u \in y \equiv \exists v(\langle v, u\rangle \in X \& v \in x))).$$

Аксиома замещения утверждает, что если класс X однозначен, то класс вторых компонент тех пар из X, первые компоненты которых принадлежат x, является множеством (эквивалентное утверждение: $M(\mathscr{R}(x \restriction X))$). Из этой аксиомы следует, что если X есть функция, то область значений результата ограничения X посредством всякой области, являющейся множеством, также есть множество.

Упражнения

1. Показать, что аксиома замещения (R) влечет аксиому выделения (S). (Указание. Пусть X есть класс всех упорядоченных пар $\langle u, u\rangle$ таких, что $u \in Y$, т. е. $X = \hat{y}_1\hat{y}_2(y_1 = y_2 \& y_1 \in Y)$. Очевидно, $Un(X)$ и $(\exists v(\langle v, u\rangle \in X \& v \in x)) \equiv u \in Y \cap x$.)

2. $\vdash \forall x(M(\mathscr{D}(x)) \& M(\mathscr{R}(x)))$. (Указание. Показать, что $\mathscr{D}(x) \subseteq \subseteq \mathsf{U}(\mathsf{U}(x))$ и $\mathscr{R}(x) \subseteq \mathsf{U}(\mathsf{U}(x))$; применить предложение 4.6 и аксиому U.)

3. $\vdash \forall x \forall y(M(x \times y))$. (Указание. Показать, что $x \times y \subseteq \mathscr{P}(\mathscr{P}(x \cup y))$; применить предложение 4.6 и аксиому W.)

4. (a) $\vdash M(\mathscr{D}(X)) \& M(\mathscr{R}(X)) \& Rel(X) \supset M(X)$. (Указание. $X \subseteq \subseteq \mathscr{D}(X) \times \mathscr{R}(X)$.)

(b) $\vdash \forall y(Fnc(X) \supset M(y \restriction X))$. (Указание. $Fnc(y \restriction X) \& \mathscr{D}(y \restriction X) \subseteq y$, откуда, в силу аксиомы R и утверждения (a), следует $M(X``y)$.)

Следующая аксиома обеспечивает существование бесконечных множеств.

Аксиома I. (*Аксиома бесконечности.*)

$$\exists x(0 \in x \& \forall u(u \in x \supset u \cup \{u\} \in x)).$$

Аксиома бесконечности утверждает, что существует такое множество x, что $0 \in x$, и если $u \in x$, то $u \cup \{u\}$ также принадлежит x. Для такого множества x, очевидно, $\{0\} \in x$, $\{0, \{0\}\} \in x$, $\{0, \{0\}, \{0, \{0\}\}\} \in x$

*) В дальнейшем мы будем по мере необходимости вводить новые функциональные буквы и предметные константы, как только будет ясно, что соответствующее определение может быть обосновано теоремой о единственности. В настоящем случае происходит введение некоторой новой функциональной буквы h с сокращенным обозначением $X`Y$ вместо $h(X, Y)$.

и т. д. Если мы теперь положим $1 = \{0\}$, $2 = \{0, 1\}$, ..., $n = \{0, 1, \ldots, n-1\}$, то для любого целого $n \geqslant 0$ будет выполнено $n \in x$, и при этом $0 \neq 1$, $0 \neq 2$, $1 \neq 2$, $0 \neq 3$, $1 \neq 3$, $2 \neq 3$, ...

Упражнение

Доказать, что аксиома I влечет аксиому N*). Доказать также, что если некоторая формула влечет $\exists X(M(X))$, то вместе с аксиомой S та же формула влечет аксиому N.

Список аксиом теории NBG завершен. Мы видим, что NBG имеет лишь конечное число аксиом, а именно: аксиому T (объемности), аксиому P (пары), аксиому N (пустого множества), аксиому S (выделения), аксиому U (объединения), аксиому W (множества всех подмножеств), аксиому R (замещения), аксиому I (бесконечности) и семь аксиом существования классов B1 — B7. Мы видели также, что аксиомы N и S выводимы из остальных аксиом, однако они включены в общий список аксиом, так как представляют интерес при изучении некоторых более слабых подтеорий теории NBG.

Убедимся теперь в том, что парадокс Рассела невыводим в NBG. Пусть $Y = \hat{x}(x \notin x)$, т. е. $\forall x (x \in Y \equiv x \notin x)$. (Такой класс Y существует, в силу теоремы о существовании классов (предложение 4.4), так как формула $x \notin x$ предикативна.) В первоначальной, т. е. не сокращенной, символике эта последняя формула записывается так: $\forall X (M(X) \supset \supset (X \in Y \equiv X \notin X))$. Допустим $M(Y)$. Тогда $Y \in Y \equiv Y \notin Y$, что, в силу тавтологии $(A \equiv \neg A) \supset A \& \neg A$, влечет $Y \in Y \& Y \notin Y$. Отсюда по теореме дедукции получаем $\vdash M(Y) \supset (Y \in Y \& Y \notin Y)$, а затем, в силу тавтологии $(B \supset (A \& \neg A)) \supset \neg B$, получаем и $\neg M(Y)$. Таким образом, рассуждения, с помощью которых обычно выводится парадокс Рассела, в теории NBG приводят всего лишь к тому результату, что Y есть собственный класс, т. е. не множество. Здесь мы имеем дело с типичным для теории NBG способом избавления от обычных парадоксов (например, парадоксов Кантора и Бурали-Форти).

Упражнение

$\vdash \neg M(V)$. (Универсальный класс не есть множество.) (Указание. $V = \hat{x}(x = x)$; для расселовского класса $Y = \hat{x}(x \notin x)$ уже показано, что $\neg M(Y)$, остается применить предложение 4.6, принимая во внимание, что $Y \subseteq V$.)

§ 2. Порядковые числа

Определим сначала некоторые привычные понятия, связанные с отношениями.

---

*) Чтобы в самой формулировке аксиомы I не предполагать аксиомы N, надлежит в аксиоме I «$0 \in x$» заменить на «$\exists v (v \in x \& \forall u (u \notin v))$».

Определения

$X\ Irr\ Y$ означает $\forall y\,(y \in Y \supset \langle y, y\rangle \notin X)\ \&\ Rel\,(X)$.
(X есть *иррефлексивное* отношение на Y.)

$X\ Tr\ Y$ означает $Rel\,(X)\ \&\ \forall u \forall v \forall w\,(u \in Y\ \&\ v \in Y\ \&\ w \in Y\ \&\ \&\ \langle u, v\rangle \in X\ \&\ \langle v, w\rangle \in X \supset \langle u, w\rangle \in X)$.
(X есть *транзитивное* отношение на Y.)

$X\ Part\ Y$ означает $(X\ Irr\ Y)\ \&\ (X\ Tr\ Y)$.
(X *частично упорядочивает* Y.)

$X\ Con\ Y$ означает $Rel\,(X)\ \&\ \forall u \forall v\,(u \in Y\ \&\ v \in Y\ \&\ u \neq v \supset \langle u, v\rangle \in \in X \vee \langle v, u\rangle \in X)$.
(X есть *связное* на Y отношение.)

$X\ Tot\ Y$ означает $(X\ Irr\ Y)\ \&\ (X\ Tr\ Y)\ \&\ (X\ Con\ Y)$.
(X *упорядочивает* Y.)

$X\ We\ Y$ служит обозначением для $Rel\,(X)\ \&\ (X\ Irr\ Y)\ \&\ \forall Z\,(Z \subseteq Y\ \&\ \&\ Z \neq 0 \supset \exists y\,(y \in Z\ \&\ \forall v\,(v \in Z\ \&\ v \neq y \supset \langle y, v\rangle \in X\ \&\ \&\ \langle v, y\rangle \notin X)))$.
(X *вполне упорядочивает* Y, т. е. отношение X иррефлексивно на Y, и всякий непустой подкласс класса Y имеет наименьший в смысле отношения X элемент.)

Упражнения

1. $\vdash (X\ We\ Y) \supset (X\ Tot\ Y)$. (Указание. Чтобы доказать $X\ Con\ Y$, рассмотрим такие x и y, что $x \in Y$, $y \in Y$ и $x \neq y$; очевидно, $\{x, y\}$ имеет наименьший элемент, пусть это будет, например x, тогда $\langle x, y\rangle \in X$; чтобы показать, что $X\ Tr\ Y$, рассмотрим x, y и z, для которых $x \in Y$, $y \in Y$, $z \in Y$ и $\langle x, y\rangle \in X\ \&\ \langle y, z\rangle \in X$; множество $\{x, y, z\}$ имеет наименьший элемент, которым обязан в данном случае быть x.)

2. $\vdash (X\ We\ Y)\ \&\ (Z \subseteq Y) \supset (X\ We\ Z)$.

Примеры (из наивной теории множеств). 1. Отношение $<$ на множестве P всех целых положительных чисел вполне упорядочивает P.

2. Отношение $<$ на множестве всех целых чисел упорядочивает, но не вполне упорядочивает это множество.

3. Отношение $\subset$ на множестве W всех подмножеств множества всех целых чисел частично упорядочивает W, но не упорядочивает W. (Например, $\{1\} \not\subset \{2\}$ и $\{2\} \not\subset \{1\}$.)

Определение. $Sim\,(Z, W_1, W_2)$ служит сокращением для $\exists x_1 \exists x_2 \exists r_1 \exists r_2\,(Rel\,(r_1)\ \&\ Rel\,(r_2)\ \&\ W_1 = \langle r_1, x_1\rangle\ \&\ W_2 = \langle r_2, x_2\rangle\ \&\ Fnc\,(Z)\ \&\ \&\ Un_1\,(Z)\ \&\ \mathscr{D}\,(Z) = x_1\ \&\ \mathscr{R}\,(Z) = x_2\ \&\ \forall u \forall v\,(u \in x_1\ \&\ v \in x_1 \supset \langle u, v\rangle \in \in r_1 \equiv \langle Z'u, Z'v\rangle \in r_2))$. ($Z$ есть *подобное отображение*, отображающее отношение r_1, определенное на x_1, на отношение r_2, определенное на x_2.).

Определение. $Sim\,(W_1, W_2)$ служит сокращением для $\exists z\ Sim\,(z, W_1, W_2)$. ($W_1$ и W_2 — *подобно упорядоченные структуры*.)

Пример. Пусть r_1 — отношение $<$ на множестве Nn всех неотрицательных целых чисел, а r_2 — отношение $<$ на множестве P всех

положительных целых чисел; пусть, далее, z есть множество всех упорядоченных пар $\langle x, x+1\rangle$, где x пробегает Nn. Тогда z есть подобное отображение $\langle r_1, \mathrm{Nn}\rangle$ на $\langle r_2, \mathrm{P}\rangle$.

Упражнения

1. $\vdash Sim(Z, X, Y) \supset Sim(\check{Z}, X, Y)$.
2. $\vdash Sim(Z, X, Y) \supset M(Z) \,\&\, M(X) \,\&\, M(Y)$.

Определения

$Fld(X)$ означает $\mathscr{D}(X) \cup \mathscr{R}(X)$. (*Поле* класса X.)
$TOR(X)$ означает $Rel(X) \,\&\, (X\ Tot\ (Fld(X)))$.
(X есть *отношение порядка*.)
$WOR(X)$ означает $Rel(X) \,\&\, (X\ We\ (Fld(X)))$.
(X есть *вполне упорядочивающее отношение*.)

Упражнения

1. $\vdash (Sim(X, Y) \supset Sim(Y, X)) \,\&\, (Sim(X, Y) \,\&\, Sim(Y, U) \supset Sim(X, U))$.
2. $\vdash Sim(\langle X, Fld(X)\rangle, \langle Y, Fld(Y)\rangle) \supset (TOR(X) \equiv TOR(Y)) \,\&\, (WOR(X) \equiv WOR(Y))$.

Если x есть отношение порядка, то класс всех отношений порядка, подобных x, называется *порядковым типом* отношения x. В дальнейшем нас будут специально интересовать порядковые типы вполне упорядочивающих отношений. Оказывается, однако, что в теории NBG все порядковые типы (кроме порядкового типа $\{0\}$ отношения 0) являются собственными классами. В связи с этим представляется удобным найти класс W вполне упорядоченных структур такой, чтобы всякое вполне упорядочивающее отношение было подобно некоторому и притом единственному элементу из W. Таким образом, мы подходим к изучению порядковых чисел.

Определения

E означает $\hat{x}\hat{y}(x \in y)$. (*Отношение принадлежности*.)
$Trans(X)$ означает $\forall u(u \in X \supset u \subseteq X)$. (Класс X *транзитивен*.)
$Sect_Y(X, Z)$ означает $Z \subseteq X \,\&\, \forall u \forall v(u \in X \,\&\, v \in Z \,\&\, \langle u, v\rangle \in Y \supset u \in Z)$.
(Класс Z является *Y-сечением* класса X.)
$Seg_Y(X, U) = \hat{x}(x \in X \,\&\, \langle x, U\rangle \in Y)$.
(*Y-сегмент* класса X, определенный классом U.)

Упражнения

1. $\vdash Trans(X) \equiv \mathsf{U}(X) \subseteq X$.
2. $\vdash Trans(X) \,\&\, Trans(Y) \supset Trans(X \cup Y) \,\&\, Trans(X \cap Y)$.
3. $\vdash Seg_E(X, u) = \hat{x}(x \in X \,\&\, x \in u) \,\&\, Seg_E(Y, u) \subseteq Y \cap u \,\&\, M(Seg_E(Y, u))$.

4. $\vdash Trans(X) \equiv \forall u\,(u \in X \supset Seg_E(X, u) = u)$.

5. $\vdash (E\ We\ X)\ \&\ Sect_E(X, Z)\ \&\ Z \neq X \supset \exists u\,(u \in X\ \&\ Z = Seg_E(X, u))$. (Указание. Взять в качестве u $\in$-наименьший элемент класса $X - Z$.)

Определения

$Ord(X)$ означает $(E\ We\ X)\ \&\ Trans(X)$. (X является *порядковым классом* тогда и только тогда, когда $\in$-отношение вполне упорядочивает X и всякий элемент X является также и подмножеством X.)

On означает $\hat{x}(Ord(x))$ (т. е. $\vdash \forall x\,(x \in On \equiv Ord(x))$). Порядковый класс, являющийся множеством, называется *порядковым числом*. On есть класс всех порядковых чисел. Заметим, что формула $x \in On$ эквивалентна некоторой предикативной формуле, а именно конъюнкции формул

(a) $\forall u\,(u \in x \supset u \notin u)$;

(b) $\forall u\,(u \subseteq x\ \&\ u \neq 0 \supset \exists v\,(v \in u\ \&\ \forall w\,(w \in u\ \&\ w \neq v \supset v \in w\ \&\ \&\ w \notin v)))$;

(c) $\forall u\,(u \in x \supset u \subseteq x)$.

(Первая из этих формул эквивалентна $(E\ Irr\ x)$, вторая — $(E\ We\ x)$ и третья — $Trans(x)$.) Поэтому всякая формула, предикативная, если не обращать внимания на вхождения On, эквивалентна некоторой предикативной формуле и, следовательно, может рассматриваться в качестве φ в теореме существования классов (предложение 4.4). Здесь следует добавить, что всякая формула $On \in Y$ может быть заменена на $\exists y\,(y \in Y\ \&\ \&\ \forall z\,(z \in y \equiv z \in On))$.)

Примеры. 1. $\vdash 0 \in On$.

2. Обозначим $\{0\}$ через 1, тогда $\vdash 1 \in On$.

Мы будем употреблять малые греческие буквы α, β, γ, δ, ... в качестве переменных, ограниченных порядковыми числами; например, $\forall \alpha \mathscr{A}(\alpha)$ означает $\forall x\,(x \in On \supset \mathscr{A}(x))$ и $\exists \alpha \mathscr{A}(\alpha)$ означает $\exists x\,(x \in On\ \&\ \mathscr{A}(x))$.

Предложение 4.7.

(1) $\vdash Ord(X) \supset (X \notin X\ \&\ \forall u\,(u \in X \supset u \notin u))$;

(2) $\vdash Ord(X)\ \&\ Y \subset X\ \&\ Trans(Y) \supset Y \in X$;

(3) $\vdash (Ord(X)\ \&\ Ord(Y)) \supset (Y \subset X \equiv Y \in X)$;

(4) $\vdash Ord(X)\ \&\ Ord(Y) \supset (X \in Y \vee X = Y \vee Y \in X)\ \&\ \neg(X \in Y\ \&\ \&\ Y \in X)\ \&\ \neg(X \in Y\ \&\ X = Y)$;

(5) $\vdash Ord(X)\ \&\ Y \in X \supset Y \in On$;

(6) $\vdash E\ We\ On$;

(7) $\vdash Ord(On)$;

(8) $\vdash \neg M(On)$;

(9) $\vdash Ord(X) \supset X = On \vee X \in On$.

Доказательство. (1) Если $Ord(X)$, то отношение E иррефлексивно на X, т. е. $\forall u\,(u \in X \supset u \notin u)$, следовательно, если $X \in X$, то $X \notin X$. Поэтому $X \notin X$.

(2) Пусть $Ord(X) \& Y \subset X \& Trans(Y)$. Легко видеть, что Y является собственным E-сечением класса X. Поэтому, в силу упражнений 4—5 (стр. 191), $Y \in X$.

(3) Пусть $Ord(X) \& Ord(Y)$. Если $Y \in X$, то $Y \subseteq X$, так как X транзитивно; но, в силу (1), $Y \neq X$; следовательно, $Y \subset X$. Обратно, если $Y \subset X$, то, в силу (2), имеем $Y \in X$, так как Y транзитивно.

(4) Предположим $Ord(X) \& Ord(Y) \& X \neq Y$. Справедливы включения $X \cap Y \subseteq X$ и $X \cap Y \subseteq Y$. Так как X и Y транзитивны, то транзитивен и класс $X \cap Y$. Если $X \cap Y \subset X$ и $X \cap Y \subset Y$, то, в силу (2), $X \cap Y \in X$ и $X \cap Y \in Y$, и потому $X \cap Y \in X \cap Y$, что противоречит иррефлексивности E на X. Следовательно, или $X \cap Y = X$ или $X \cap Y = Y$, т. е. или $X \subseteq Y$, или $Y \subseteq X$. Но $X \neq Y$. Поэтому, согласно (3), $X \in Y$ или $Y \in X$. На основании того же пункта (3), $X \in Y$ и $Y \in X$ невозможно, ибо это влечет $X \subset Y$ и $Y \subset X$. Очевидно, в силу (1), невозможно и $X \in Y \& X = Y$.

(5) Пусть $Ord(X) \& Y \in X$. Мы должны доказать $E\ We\ Y$ и $Trans(Y)$. Так как $Y \in X$ и $Trans(X)$, то $Y \subset X$. Поэтому из $E\ We\ X$ следует $E\ We\ Y$. Далее, если $u \in Y$ и $v \in u$, то, по $Trans(X)$, $v \in X$. Так как $E\ Con\ X$ и $Y \in X \& v \in X$, то $v \in Y$, или $Y \in v$, или $v = Y$. Если бы при этом оказалось, что $v = Y$ или $Y \in v$, то, так как $E\ Tr\ X$ и $u \in Y \& v \in u$, мы получили бы $u \in u$, что противоречит пункту (1). Следовательно, $v \in Y$. Итак, если $u \in Y$, то $u \subseteq Y$, т. е. справедливо $Trans(Y)$.

(6) На основании (1), $E\ Irr\ On$. Пусть класс X таков, что $X \subseteq On \& X \neq 0$, и пусть $\alpha \in X$. Если α — наименьший в X элемент, то пункт (6) доказан. (Под *наименьшим элементом* класса X понимается такой элемент $v \in X$, что $\forall u\,(u \in X \& u \neq v \supset v \in u)$.) В противном случае рассуждаем следующим образом: так как $E\ We\ \alpha$ и $X \cap \alpha \neq 0$, то должен существовать элемент β, наименьший в $X \cap \alpha$. В силу (4), ясно, что β есть наименьший элемент в X.

(7) Требуется доказать $E\ We\ On$ и $Trans(On)$. Но $E\ We\ On$ есть (6) и, стало быть, доказано. Пусть теперь $u \in On$ и $v \in u$. Тогда, в силу (5), $v \in On$. Итак, $Trans(On)$ доказано.

(8) Из $M(On)$, согласно (7), следует $On \in On$, что противоречит (1).

(9) Пусть $Ord(X)$. Тогда $X \subseteq On$. Если $X \neq On$, то, в силу (3), $X \in On$.

Из предложения 4.7 (9) следует, что класс On — это единственный порядковый класс, не являющийся порядковым числом.

Определение. $x <_0 y$ означает $x \in On \& y \in On \& x \in y$;
$x \leqslant_0 y$ означает $y \in On \& (x = y \vee x <_0 y)$.

Таким образом, для порядковых чисел отношения $<_0$ и $\in$ совпадают, и $<_0$ вполне упорядочивает On. В частности, из предложения 4.7 (5) мы видим, что всякое порядковое число x равно множеству всех порядковых чисел, меньших x.

Предложение 4.8. (*Трансфинитная индукция.*)

$$\vdash \forall\beta\,(\forall\alpha\,(\alpha\in\beta\supset\alpha\in X)\supset\beta\in X)\supset On\subseteq X$$

(т. е. если для всякого β из того, что все порядковые числа $<_0\beta$ принадлежат X, следует, что и β принадлежит X, то в X находятся все порядковые числа).

Доказательство. Предположим, что $\forall\beta\,(\forall\alpha\,(\alpha\in\beta\supset\alpha\in X)\supset\beta\in X)$. Предположим также, что существует порядковое число, принадлежащее $On-X$. Тогда так как On вполне упорядочен отношением E, то в $On-X$ существует и некоторый наименьший элемент β. Итак, все порядковые числа $<_0\beta$ принадлежат X. Согласно предположению, отсюда следует, что и β принадлежит X, и мы пришли к противоречию.

Предложение 4.8 применяется для доказательства утверждений, говорящих о том, что все порядковые числа обладают тем или иным свойством $P(\alpha)$. При этом обычно полагают $X=\hat{x}\,(P(x)\,\&\,x\in On)$ и доказывают, что $\forall\beta\,(\forall\alpha\,(\alpha\in\beta\supset P(\alpha))\supset P(\beta))$.

Определение. x' служит сокращением для $x\cup\{x\}$.

Предложение 4.9.

(1) $\vdash \forall x\,(x\in On\equiv x'\in On)$;

(2) $\vdash \forall\alpha\neg\exists\beta\,(\alpha<_0\beta<_0\alpha')$;

(3) $\vdash \forall\alpha\forall\beta\,(\alpha'=\beta'\supset\alpha=\beta)$.

Доказательство. (1) Очевидно, $x\in x'$. Поэтому, если $x'\in On$, то, на основании предложения 4.7(5), и $x\in On$. Обратно, пусть $x\in On$. Следует доказать $E\,We(x\cup\{x\})$ и $Trans(x\cup\{x\})$. Так как $E\,We\,x$ и $x\notin x$, то $E\,Irr(x\cup\{x\})$. Кроме того, если $y\neq 0\,\&\,y\subseteq x\cup\{x\}$, то либо $y=\{x\}$ и тогда x есть наименьший элемент y, либо $y\cap x\neq 0$ и тогда наименьшим элементом y является наименьший элемент $y\cap x$. Таким образом, $E\,We(x\cup\{x\})$. Наконец, если $y\in x\cup\{x\}$ и $u\in y$, то, очевидно, $u\in x$, откуда получаем $Trans(x\cup\{x\})$.

(2) Предположим $\alpha<_0\beta<_0\alpha'$. Тогда $\alpha\in\beta$ и $\beta\in\alpha'$. Из $\alpha\in\beta$, в силу предложения 4.7(4), следует $\beta\notin\alpha$ и $\beta\neq\alpha$, что, согласно определению x', противоречит $\beta\in\alpha'$.

(3) Пусть $\alpha'=\beta'$. Тогда $\beta<_0\alpha'$, и, по предыдущему пункту (2), $\beta\leqslant_0\alpha$. Аналогично, $\alpha\leqslant_0\beta$. Следовательно, $\alpha=\beta$.

Определение. $Suc(X)$ служит обозначением для $X\in On\,\&\,\&\,\exists\alpha\,(X=\alpha')$. ($X$ есть *непосредственно следующее порядковое число.*)

Определение. K_1 служит обозначением для $\hat{x}\,(x=0\vee Suc(x))$. ($K_1$ есть класс всех *порядковых чисел первого рода.*)

Определение. ω служит обозначением для

$$\hat{x}\,(x\in K_1\,\&\,\forall u\,(u\in x\supset u\in K_1)).$$

ω есть класс всех порядковых чисел α первого рода и таких, что все порядковые числа $<_0\alpha$ тоже суть порядковые числа первого рода.

Примеры. $0\in\omega$, $1=\{0\}\in\omega$.

Предложение 4.10.

(1) $M(\omega)$;

(2) $\forall\alpha\,(\alpha \in \omega \equiv \alpha' \in \omega)$;

(3) $0 \in X \,\&\, \forall u\,(u \in X \supset u' \in X) \supset \omega \subseteq X$;

(4) $\forall\alpha\,(\alpha \in \omega \,\&\, \beta <_0 \alpha \supset \beta \in \omega)$.

Доказательство. (1) По аксиоме бесконечности I, существует такое множество x, что $0 \in x$ и $\forall u\,(u \in x \supset u' \in x)$. В силу предложения 4.6, достаточно показать $\omega \subseteq x$. Допустим, что $\omega \not\subseteq x$. Пусть тогда α — наименьшее в $\omega - x$ порядковое число. Очевидно, $\alpha \neq 0$, ибо $0 \in x$. Следовательно, $Suc(\alpha)$, т. е. $\exists\beta\,(\alpha = \beta')$. Пусть δ — порядковое число такое, что $\alpha = \delta'$. Тогда $\delta <_0 \alpha$, и потому $\delta \in x$. Но тогда и $\delta' \in x$, т. е. $\alpha \in x$, что приводит к противоречию. Итак, $\omega \subseteq x$ и, следовательно, $M(\omega)$.

(2) Пусть $\alpha \in \omega$. Тогда $\alpha' \in K_1$, ибо заведомо $Suc(\alpha')$. Кроме того, если $\beta \in \alpha'$, то $\beta \in \alpha$ или $\beta = \alpha$, и потому $\beta \in K_1$. Итак, $\alpha' \in \omega$. Обратно, если $\alpha' \in \omega$, то $\alpha \in \omega$ следует из $\alpha \in \alpha'$ и $\forall\beta\,(\beta \in \alpha \supset \beta \in \alpha')$.

Пункт (3) доказывается рассуждениями, подобными тем, которые применялись при доказательстве пункта (1), а доказательство пункта (4) мы предоставляем читателю в качестве легкого упражнения.

Элементы множества ω называются *конечными порядковыми числами*. Мы будем применять обычную форму для их обозначения: 1 для $0'$, 2 для $1'$, 3 для $2'$ и т. д. Таким образом, $0 \in \omega$, $1 \in \omega$, $2 \in \omega$, $3 \in \omega$, ...

Порядковые числа, отличные от нуля и не являющиеся порядковыми числами первого рода, назовем *предельными порядковыми числами* или *порядковыми числами второго рода*.

Определение. $Lim(x)$ означает $x \in On \,\&\, x \notin K_1$.

Упражнение

$\vdash Lim(\omega)$.

Предложение 4.11.

(1) $\vdash \forall x\,(x \subseteq On \supset (\bigcup(x) \in On \,\&\, \forall\alpha\,(\alpha \in x \supset \alpha \leqslant_0 \bigcup(x)) \,\&$
$\& \,\forall\beta\,(\forall\alpha\,(\alpha \in x \supset \alpha \leqslant_0 \beta) \supset \bigcup(x) \leqslant_0 \beta)))$.

(Каково бы ни было множество x порядковых чисел, множество $\bigcup(x)$ является порядковым числом и притом наименьшей верхней гранью для x.)

(2) $\vdash \forall x\,(x \subseteq On \,\&\, x \neq 0 \,\&\, \forall\alpha\,(\alpha \in x \supset \exists\beta\,(\beta \in x \,\&\, \alpha <_0 \beta)) \supset$
$\supset Lim(\bigcup(x)))$.

(Если x есть непустое множество порядковых чисел без наибольшего элемента, то $\bigcup(x)$ есть предельное порядковое число.)

Доказательство. (1) Пусть $x \subseteq On$. $\bigcup(x)$, будучи множеством порядковых чисел, вполне упорядочено отношением E. Кроме того, если

$\alpha \in \mathsf{U}(x) \,\&\, \beta \in \alpha$, то существует γ такое, что $\gamma \in x \,\&\, \alpha \in \gamma$, что вместе с $\beta \in \alpha$ дает, по свойству транзитивности порядковых чисел, $\beta \in \gamma$ и, следовательно, $\beta \in \mathsf{U}(x)$. Таким образом, $\mathsf{U}(x)$ транзитивно, и потому $\mathsf{U}(x) \in On$. Если теперь $\alpha \in x$, то $\alpha \subseteq \mathsf{U}(x)$ и, по предложению 4.7(3), $\alpha \leqslant_0 \mathsf{U}(x)$. Предположим, наконец, что $\forall \alpha (\alpha \in x \supset \alpha \leqslant_0 \beta)$. Для любого δ, если $\delta \in \mathsf{U}(x)$, то существует γ такое, что $\delta \in \gamma \,\&\, \gamma \in x$. При этом $\gamma \leqslant_0 \beta$, и потому $\delta \leqslant_0 \beta$. Таким образом, $\mathsf{U}(x) \subseteq \beta$ и, по предложению 4.7(3), $\mathsf{U}(x) \leqslant_0 \beta$.

(2) Пусть $x \neq 0 \,\&\, x \subseteq On \,\&\, \forall \alpha (\alpha \in x \supset \exists \beta (\beta \in x \,\&\, \alpha <_0 \beta))$. Если $\mathsf{U}(x) = 0$, то из $\alpha \in x$ следует $\alpha = 0$. Тогда $x = 0$ или $x = 1$, чего не может быть, в силу наших условий. Итак, $\mathsf{U}(x) \neq 0$. Допустим $Suc(\mathsf{U}(x))$. Тогда $\mathsf{U}(x) = \gamma'$ при некотором γ. Так как, в силу первой части доказываемого предложения, $\mathsf{U}(x)$ является наименьшей верхней гранью для x, то γ не является верхней гранью для x, следовательно, существует $\delta \in x$ такое, что $\gamma <_0 \delta$. Но тогда $\delta = \mathsf{U}(x)$, поскольку $\mathsf{U}(x)$ есть верхняя грань для x. Таким образом, в противоречие с условием, $\mathsf{U}(x)$ оказывается наибольшим в x элементом. Следовательно, $\neg Suc(\mathsf{U}(x))$, и остается принять $Lim(x)$.

Упражнение

$\vdash \forall \alpha ((Suc(\alpha) \supset (\mathsf{U}(\alpha))' = \alpha) \,\&\, (Lim(\alpha) \supset \mathsf{U}(\alpha) = \alpha))$.

Теперь мы можем сформулировать и доказать принцип трансфинитной индукции в другой форме.

Предложение 4.12. (*Трансфинитная индукция*, вторая форма.)

(1) $\vdash 0 \in X \,\&\, \forall \alpha (\alpha \in X \supset \alpha' \in X) \,\&\, \forall \alpha (Lim(\alpha) \,\&\, \forall \beta (\beta <_0 \alpha \supset \beta \in X) \supset \alpha \in X) \supset On \subseteq X$;

(2) (Индукция до δ.) $\vdash 0 \in X \,\&\, \forall \alpha (\alpha' <_0 \delta \,\&\, \alpha \in X \supset \alpha' \in X) \,\&\, \forall \alpha (\alpha <_0 \delta \,\&\, Lim(\alpha) \,\&\, \forall \beta (\beta <_0 \alpha \supset \beta \in X) \supset \alpha \in X) \supset \delta \subseteq X$.

Доказательство. (1) Пусть $Y = \hat{x} (x \in On \,\&\, \forall \alpha (\alpha \leqslant_0 x \supset \alpha \in X))$. В предположении, что верна посылка доказываемой формулы, легко показать, что $\forall \alpha (\alpha <_0 \gamma \supset \alpha \in Y) \supset \gamma \in Y$. Следовательно, по предложению 4.8, $On \subseteq Y$. А так как $Y \subseteq X$, то и $On \subseteq X$.

(2) Предоставляется в качестве упражнения читателю.

В теории множеств существенную роль играют определения по трансфинитной индукции. Эти определения могут быть оправданы с помощью следующих теорем.

Предложение 4.13.

(1) $\vdash \forall X \exists_1 Y (Fnc(Y) \,\&\, \mathscr{D}(Y) = On \,\&\, \forall \alpha (Y`\alpha = X`(\alpha \restriction Y)))$.

(Для любого X существует единственная функция Y, определенная на всех порядковых числах и такая, что значение Y на α равно значению X, примененного к ограничению Y множеством порядковых чисел $<_0 \alpha$.)

(2) $\vdash \forall x \forall X_1 \forall X_2 \exists_1 Y (Fnc(Y) \,\&\, \mathscr{D}(Y) = On \,\&\, Y`0 = x \,\&\, \forall \alpha (Y`(\alpha') = X_1`(Y`\alpha)) \,\&\, \forall \alpha (Lim(\alpha) \supset Y`\alpha = X_2`(\alpha \restriction Y)))$;

(3) (Индукция до δ.) $\vdash \forall x \forall X_1 \forall X_2 \exists_1 Y (Fnc(Y) \& \mathscr{D}(Y) = \delta \& Y`0 = x \& \forall \alpha (\alpha' <_0 \delta \supset Y`(\alpha') = X_1`(Y`\alpha)) \& \forall \alpha (Lim(\alpha) \& \alpha <_0 \delta \supset Y`\alpha = X_2`(\alpha \restriction Y)))$.

Доказательство. (1) Пусть $Y_1 = \hat{u}(Fnc(u) \& \mathscr{D}(u) \in On \& \forall \alpha (\alpha \in \mathscr{D}(u) \supset u`\alpha = X`(\alpha \restriction u)))$. Докажем сначала, что если $u_1 \in Y_1$ и $u_2 \in Y_1$, то $u_1 \subseteq u_2$ или $u_2 \subseteq u_1$. В самом деле, пусть $\gamma_1 = \mathscr{D}(u_1)$ и $\gamma_2 = \mathscr{D}(u_2)$, тогда либо $\gamma_1 \leqslant_0 \gamma_2$, либо $\gamma_2 \leqslant_0 \gamma_1$. Пусть, например, $\gamma_1 \leqslant_0 \gamma_2$, и пусть w есть множество всех таких порядковых чисел $\alpha <_0 \gamma_1$, что $u_1`\alpha \neq u_2`\alpha$. Допустим, что $w \neq 0$, и пусть η — наименьший элемент в w. Тогда из $\beta <_0 \eta$ следует $u_1`\beta = u_2`\beta$. Следовательно, $\eta \restriction u_1 = \eta \restriction u_2$. Но $u_1`\eta = X`(\eta \restriction u_1)$ и $u_2`\eta = X`(\eta \restriction u_2)$, и, таким образом, $u_1`\eta = u_2`\eta$, что противоречит допущению о том, что непусто множество w, в котором η есть наименьший элемент. Поэтому $w = 0$, т. е. $u_1`\alpha = u_2`\alpha$ для всех $\alpha <_0 \gamma_1$. Отсюда получаем $u_1 = \gamma_1 \restriction u_1 = \gamma_1 \restriction u_2 \subseteq u_2$. Таким образом, любые две функции из Y_1 совпадают на общей части их областей определения. Положим $Y = \bigcup(Y_1)$. Читателю предоставляется самому доказать, что Y есть функция, область определения которой есть либо порядковое число, либо On, и что $\forall \alpha (Y`\alpha = X`(\alpha \restriction Y))$. После этого уже нетрудно доказать, что $\mathscr{D}(Y) = On$. Если бы было $\mathscr{D}(Y) = \delta$, то, положив $W = Y \cup \{\langle \delta, X`Y \rangle\}$, мы имели бы $W \in Y_1$ и, следовательно, $W \subseteq Y$, откуда в свою очередь $\delta \in \mathscr{D}(Y) = \delta$, чего не может быть из-за $\delta \notin \delta$. Единственность Y легко доказывается с помощью трансфинитной индукции (предложение 4.12). Доказательство (2) аналогично доказательству (1), а (3) легко следует из (2).

С помощью предложения 4.13 можно вводить новые функциональные буквы по трансфинитной индукции.

Примеры. 1. *Сложение порядковых чисел.* В предложении 4.13(2) положим $x = \beta$, $X_1 = \hat{u}\hat{v}(v = u')$, $X_2 = \hat{u}\hat{v}(v = \bigcup(\mathscr{R}(u)))$. Получаем, что для всякого порядкового числа β существует единственная функция Y_β такая, что $Y_\beta`0 = \beta \& \forall \alpha (Y_\beta`(\alpha') = (Y_\beta`\alpha)') \& \forall \alpha (Lim(\alpha) \supset Y_\beta`\alpha = \bigcup(Y_\beta``\alpha))$. Следовательно, существует и притом единственная функция $+_0$, областью определения которой служит On^2 и такая, что для любых двух порядковых чисел β и γ $+_0(\beta, \gamma) = Y_\beta`\gamma$. Впрочем, мы тотчас же перейдем к привычной записи $\beta +_0 \gamma$ вместо $+_0(\beta, \gamma)$.

Отметим, что

$$\beta +_0 0 = \beta,$$
$$\beta +_0 (\gamma') = (\beta +_0 \gamma)',$$
$$Lim(\alpha) \supset \beta +_0 \alpha = \bigcup_{\tau <_0 \alpha} (\beta +_0 \tau).$$

В частности, $\beta +_0 1 = \beta +_0 (0') = (\beta +_0 0)' = \beta'$.

2. *Умножение порядковых чисел.* В предложении 4.13(2) положим $x = 0$, $X_1 = \hat{u}\hat{v}(v = u +_0 \beta)$, $X_2 = \hat{u}\hat{v}(v = \bigcup(\mathscr{R}(u)))$. Тогда так же, как

и в предыдущем примере 1, заключаем, что существует функция $\beta \overset{\cdot}{\times}_0 \gamma$ со свойствами

$$\beta \times_0 0 = 0,$$
$$\beta \times_0 (\gamma') = (\beta \times_0 \gamma) +_0 \beta,$$
$$Lim(\alpha) \supset \beta \times_0 \alpha = \bigcup_{\tau <_0 \alpha} (\beta \times_0 \tau).$$

Упражнение

Обосновать операцию возведения в степень для порядковых чисел:

$$\beta^0 = 1,$$
$$\beta^{(\gamma')} = (\beta^\gamma) \times_0 \beta,$$
$$Lim(\alpha) \supset \beta^\alpha = \bigcup_{\tau <_0 \alpha} (\beta^\tau).$$

Для произвольного множества X обозначим через E_X отношение принадлежности, ограниченное множеством X: $E_X = \hat{x}\hat{y}\,(x \in y \,\&\, x \in X \,\&\, y \in X)$.

Предложение 4.14 *). *Пусть R — вполне упорядочивающее отношение на множестве x, т. е. R We x. Пусть, далее, f — функция, отображающая x в x, такая, что для любых u, v в x из $\langle u, v\rangle \in R$ следует $\langle f'u, f'v\rangle \in R$. Тогда для любого u в x: $u = f'u$ или $\langle u, f'u\rangle \in R$.*

Доказательство. Пусть $X = \hat{u}\,(\langle f'u, u\rangle \in R)$. Мы хотим доказать, что $X = 0$. Допустим, что $X \neq 0$. Так как $X \subseteq x$ и R вполне упорядочивает x, то в X существует наименьший относительно порядка R элемент u_0. Очевидно, $\langle f'u_0, u_0\rangle \in R$. Отсюда $\langle f'(f'u_0), f'u_0\rangle \in R$, т. е. $f'u_0 \in X$. Тогда соотношение $\langle f'u_0, u_0\rangle \in R$ противоречит определению u_0.

Следствие 4.15. *Если $\alpha \in \beta$ и $y \subseteq \alpha$, т. е. если y есть подмножество некоторого сегмента порядкового числа β, то $\langle E_\beta, \beta\rangle$ и $\langle E_y, y\rangle$ не подобны.*

Доказательство. Предположим, что существует такая функция f, отображающая β на y, что всякий раз из $u \in \beta$, $v \in \beta$ и $u \in v$ следует $f'u \in f'v$. Так как область значений f совпадает с y, то $f'\alpha \in y$. По условию же $y \subseteq \alpha$. Поэтому $f'\alpha \in \alpha$. Но мы находимся в условиях предложения 4.14, в силу которого, следовательно (полагая $\beta = x$), имеем $f'\alpha = \alpha$ или $\alpha \in f'\alpha$, что несовместимо с $f'\alpha \in \alpha$.

Следствие 4.16. (1) *Если $\alpha \neq \beta$, то $\langle E_\alpha, \alpha\rangle$ и $\langle E_\beta, \beta\rangle$ не подобны.* (2) *Каково бы ни было порядковое число α, всякое отображение f*

*) Начиная с этого места, многие теоремы теории NBG будут формулироваться на русском языке как результаты соответствующего перевода с формального языка этой теории. Это делается с целью избежать выписывания непомерно длинных формул, ввиду трудности их расшифровки. Впрочем, мы будем так поступать только в тех случаях, когда читатель без особого труда смог бы сам построить соответствующую формулу теории NBG по неформальной «русской» версии теоремы.

подобия $\langle E_\alpha, \alpha\rangle$ *на* $\langle E_\alpha, \alpha\rangle$ *является тождественным отображением, т. е.* $f'\beta = \beta$ *при любом* $\beta <_0 \alpha$.

Доказательство. (1) Следует из следствия 4.15. (2) В силу предложения 4.14, $\beta \leqslant_0 f'\beta$ и $\beta \leqslant_0 \breve{f}'\alpha$ при любом $\beta <_0 \alpha$. Поэтому $\beta \leqslant_0 f'\beta \leqslant_0 (\breve{f})'(f'\beta) = \beta$, откуда $f'\beta = \beta$.

Предложение 4.17. *Каковы бы ни были непустое множество и и вполне упорядочивающее это множество отношение* R (*т. е. если* R *We* u & $u = Fld(R)$ & $u \neq 0$), *существует единственное порядковое число* γ *и единственная функция* f *такие, что* f *есть отображение подобия* $\langle E_\gamma, \gamma\rangle$ *на* $\langle R, u\rangle$. (*То есть всякое вполне упорядоченное множество подобно некоторому и притом единственному порядковому числу.*)

Доказательство. Пусть $Z = \hat{v}\hat{w}(w \in u - v \,\&\, \forall z(z \in u - v \supset \supset \neg\langle z, w\rangle \in R))$. Очевидно, Z есть функция и притом такая, что если $v \subseteq u$ и $u - v \neq 0$, то $Z'v$ есть наименьший относительно R элемент в $u - v$. Пусть $X = \hat{v}\hat{w}(\langle \mathcal{R}(v), w\rangle \in Z)$. Пусть затем Y — функция, определяемая по трансфинитной индукции (предложение 4.13), область определения которой есть On и такая, что $\forall\alpha(Y'\alpha = X'(\alpha \upharpoonright Y))$. Наконец, пусть $W = \hat{\alpha}(Y''\alpha \subseteq u \,\&\, u - Y''\alpha \neq 0)$. Ясно, что если $\alpha \in W$ и $\beta \in \alpha$, то и $\beta \in W$. Следовательно, либо $W = On$, либо W есть некоторое порядковое число γ. (Если $W \neq On$, то этим порядковым числом γ является наименьшее порядковое число в классе $On - W$.) Если $\alpha \in W$, то $Y'\alpha = X'(\alpha \upharpoonright Y)$ есть наименьший относительно R элемент в $u - Y''\alpha$, поэтому $Y'\alpha \in u$, и если $\beta \in \alpha$, то $Y'\alpha \neq Y'\beta$. Таким образом, Y есть взаимно однозначная функция на W, и область значений функции Y, ограниченной классом W, является подмножеством u. Положим теперь $f = \breve{(W \upharpoonright Y)}$, т. е. определим f как функцию, обратную к функции Y, ограниченной классом W. Функция f является взаимно однозначной функцией, область определения которой совпадает с некоторым подмножеством множества u, а областью значений служит W. Поэтому, на основании аксиомы замещения R (стр. 187), W есть множество и, следовательно, равно некоторому порядковому числу γ. Пусть $g = \gamma \upharpoonright Y$. Очевидно, что g есть взаимно однозначная функция с областью определения, равной γ, и областью значений, равной некоторому подмножеству u_1 множества u. Мы должны показать, что $u_1 = u$ и что если α и β взяты из γ и $\beta \in \alpha$, то $\langle g'\beta, g'\alpha\rangle \in R$. Итак, допустим, что $\alpha \in \gamma$, $\beta \in \gamma$, $\beta \in \alpha$. Так как $g'\beta$ является наименьшим относительно R элементом множества $u - g''\beta$, $\beta \in \alpha$ и функция g взаимно однозначна, то $g'\alpha \in \in u - g''\beta$. Следовательно, $\langle g'\beta, g'\alpha\rangle \in R$. Остается доказать, что $u_1 = u$. Очевидно, $u_1 = Y''\gamma$. Допустим, что $u - u_1 \neq 0$. Тогда $\gamma \in W$. Но $W = \gamma$, что приводит к противоречию. Итак, $u = u_1$. Единственность γ следует из утверждения 4.16.

Предложение 4.18. *Пусть отношение* R *вполне упорядочивает собственный класс* X *таким образом, что для любого* $y \in X$

класс всех предшественников элемента y относительно отношения R в X (т. е. R-сегмент в X, определенный элементом y) является множеством. Тогда R подобно E_{On}, т. е. существует взаимно однозначное подобное отображение h On на X такое, что из $\alpha \in \beta$ следует $\langle h`\alpha, h`\beta\rangle \in R$.

Доказательство. Рассуждая так же, как и при доказательстве предложения 4.17, приходим, однако, к тому, что W теперь совпадает с On. Кроме того, из условия, что всякий R-сегмент X является множеством, следует $\mathscr{R}(Y) = X$. (Если бы было $X - \mathscr{R}(Y) \neq 0$, то в противоречие с аксиомой замещения мы получили бы, что On есть область значений для функции $\breve{Y}$, областью определения которой служит R-сегмент X, определенный наименьшим относительно R элементом w в $X - \mathscr{R}(Y)$.)

§ 3. Равномощность. Конечные и счетные множества

Мы будем говорить, что два класса X и Y *равномощны*, если существует взаимно однозначная функция, областью определения которой является X, а областью значений Y. Следующими определениями вводится обозначение $X \simeq Y$ для сокращенной записи утверждения о равномощности классов X и Y.

Определения

$X \underset{F}{\simeq} Y$ означает $(Fnc(F) \,\&\, Un_1(F) \,\&\, \mathscr{D}(F) = X \,\&\, \mathscr{R}(F) = Y)$,

$X \simeq Y$ означает $\exists F\left(X \underset{F}{\simeq} Y\right)$.

Отметим, что $\vdash \forall x \forall y \left(x \simeq y \equiv \exists z \left(x \underset{z}{\simeq} y\right)\right)$. Поэтому формула $x \simeq y$ предикативна (т. е. эквивалентна некоторой формуле, содержащей кванторы только по переменным для множеств). Очевидно, что если $X \underset{F}{\simeq} Y$, то $X \underset{\breve{F}}{\simeq} Y$, и что если $X \underset{F}{\simeq} Y$ и $Y \underset{G}{\simeq} Z$, то $X \underset{H}{\simeq} Z$, где H есть *композиция* функций F и G (это значит, что $H = \hat{x}\hat{y}(\exists z(\langle x, z\rangle \in F \,\&\, \langle z, y\rangle \in G)$). Итак, мы имеем следующую теорему.

Предложение 4.19. (1) $X \simeq X$, (2) $X \simeq Y \supset Y \simeq X$, (3) $X \simeq Y \,\&\, Y \simeq Z \supset X \simeq Z$.

Предложение 4.20. (1) $((X \simeq Y) \,\&\, (X_1 \simeq Y_1) \,\&\, (X \cap X_1 = 0) \,\&\, (Y \cap Y_1 = 0)) \supset (X \cup X_1 \simeq Y \cup Y_1)$.

(2) $((X \simeq Y) \,\&\, (X_1 \simeq Y_1)) \supset (X \times X_1 \simeq Y \times Y_1)$.

(3) $X \times \{y\} \simeq X$.

(4) $X \times Y \simeq Y \times X$.

(5) $(X \times Y) \times Z \simeq X \times (Y \times Z)$.

Доказательство. (1) Пусть $X \underset{F}{\simeq} Y$ и $X_1 \underset{G}{\simeq} Y_1$. Тогда $X \cup X_1 \underset{F \cup G}{\simeq} Y \cup Y_1$.

(2) Пусть $X \underset{F}{\simeq} Y$ и $X_1 \underset{G}{\simeq} Y_1$. Положим $W = \hat{u}\hat{v}\,(\exists x \exists y\,(x \in X \,\&\, y \in X_1 \,\&\, u = \langle x, y\rangle \,\&\, v = \langle F`x, G`y\rangle))$. Тогда $X \times X_1 \underset{W}{\simeq} Y \times Y_1$.

(3) Пусть $F = \hat{u}\hat{v}\,(u \in X \,\&\, v = \langle u, y\rangle)$. Тогда $X \underset{F}{\simeq} X \times \{y\}$.

(4) Пусть $F = \hat{u}\hat{v}\,(\exists x \exists y\,(x \in X \,\&\, y \in Y \,\&\, u = \langle x, y\rangle \,\&\, v = \langle y, x\rangle))$. Тогда $X \times Y \underset{F}{\simeq} Y \times X$.

(5) Положим $F = \hat{u}\hat{v}\,(\exists x \exists y \exists z\,(x \in X \,\&\, y \in Y \,\&\, z \in Z \,\&\, u = \langle\langle x, y\rangle, z\rangle \,\&\, v = \langle x, \langle y, z\rangle\rangle))$. Тогда $(X \times Y) \times Z \underset{F}{\simeq} X \times (Y \times Z)$.

Упражнение

Доказать $\vdash \forall X \forall Y \exists X_1 \exists Y_1\,(X \simeq X_1 \,\&\, Y \simeq Y_1 \,\&\, X_1 \cap Y_1 = 0)$.

Определение. $X^Y = \hat{u}\,(Fnc\,(u) \,\&\, \mathscr{D}\,(u) = Y \,\&\, \mathscr{R}\,(u) \subseteq X)$. Таким образом, X^Y есть класс всех множеств, являющихся функциями, отображающими Y в X. Напомним, что $2 = \{0, 1\}$. Отсюда получаем, что $\mathscr{P}(x) \simeq 2^x$ для любого множества x. (Для всякого $u \subseteq x$ характеристической функцией C_u назовем такую функцию с областью определения x, что если $y \in u$, то $C`y = 0$, а если $y \notin u$, то $C`y = 1$. Пусть F — функция, определенная на $\mathscr{P}(x)$ и ставящая в соответствие каждому $u \subseteq x$ функцию C_u. Тогда $\mathscr{P}(x) \underset{F}{\simeq} 2^x$.)

Упражнения

1. $\vdash \neg M\,(Y) \supset X^Y = 0$.
2. $\vdash \forall x \forall y M\,(x^y)$. (Указание. $u \in x^y \supset u \subseteq y \times x$.)
3. $\vdash X^0 = \{0\} = 1$.
4. $\vdash Y \neq 0 \supset 0^Y = 0$.
5. $\vdash X \simeq Y \,\&\, Z \simeq Z_1 \supset X^Z \simeq Y^{Z_1}$.
6. $\vdash X \cap Y = 0 \supset Z^{X \cup Y} \simeq Z^X \times Z^Y$.
7. $\vdash (X^Y)^Z \simeq X^{Y \times Z}$. (Указание. Положить $F = \hat{u}\hat{v}\,(Fnc\,(u) \,\&\, \mathscr{D}\,(u) = Z \,\&\, \mathscr{R}\,(u) \subseteq X^Y \,\&\, Fnc\,(v) \,\&\, \mathscr{D}\,(v) = Y \times Z \,\&\, \mathscr{R}\,(v) \subseteq X \,\&\, \forall y \forall z\,(y \in Y \,\&\, z \in Z \supset v`\langle y, z\rangle = (u`z)`z))$.)

Можно ввести такое отношение частичного упорядочения $\preceq$ для классов, что $X \preceq Y$ тогда и только тогда, когда X содержит такое же, как в Y, или меньшее, чем в Y, количество элементов.

Определение. $X \preceq Y$ служит сокращением для $\exists Z\,(Z \subseteq Y \,\&\, X \simeq Z)$ (т. е. X равномощно некоторому подклассу Y)

Определение. $X \prec Y$ означает $X \preceq Y \,\&\, \neg(X \simeq Y)$. Очевидно, $\vdash X \preceq Y \equiv (X \prec Y \vee X \simeq Y)$.

Упражнение

$\vdash X \preceq Y \,\&\, \neg M\,(X) \supset \neg M\,(Y)$.

Предложение 4.21

(1) $\vdash X \preceq X \,\&\, \neg(X \prec X)$;

(2) $\vdash X \subseteq Y \supset X \preceq Y$;

(3) $\vdash X \preceq Y \,\&\, Y \preceq Z \supset X \preceq Z$;

(4) (Шрёдер — Бернштейн.) $\vdash X \preceq Y \,\&\, Y \preceq X \supset X \simeq Y$.

Доказательство. (3) Пусть $X \underset{F}{\simeq} Y_1 \,\&\, Y_1 \subseteq Y \,\&\, Y \underset{G}{\simeq} Z_1 \,\&\, Z_1 \subseteq Z$, и пусть H есть композиция F и G. Тогда $\mathscr{R}(H) \subseteq Z \,\&\, X \underset{H}{\simeq} \mathscr{R}(H)$.

(4) Известно много доказательств этой нетривиальной теоремы. Мы приведем здесь одно новое доказательство, принадлежащее Хеллману [1961].

Лемма. *Если* $X \cap Y = X \cap Z = Y \cap Z = 0$ *и* $X \underset{F}{\simeq} X \cup Y \cup Z$, *то существует такая функция* G, *что* $X \underset{G}{\simeq} X \cup Y$. (Для доказательства этой леммы построим сначала некоторую функцию H с областью определения, равной $X \times \omega$: $\langle\langle u, k\rangle, v\rangle \in H$ тогда и только тогда, когда $u \in X$, $k \in \omega$ и существует такая функция f с областью определения, равной k', что $f\,'0 = F\,'u$ и $f\,'j \in X \,\&\, f\,'(j') = F\,'(f\,'j) \,\&\, f\,'k = v$ для каждого $j \in k$. Таким образом, $H\,'(\langle u, 0\rangle) = F\,'u$; $H\,'(\langle u, 1\rangle) = F\,'(F\,'u)$, если $F\,'u \in X$; $H\,'(\langle u, 2\rangle) = F\,'(F\,'(F\,'u))$, если $F\,'u$ и $F\,'(F\,'u)$ принадлежат X, и т. д. Пусть теперь X^* — класс всех таких u, что $u \in X$ и $\exists y\,(y \in \omega \,\&\, \langle u, y\rangle \in \mathscr{D}(H) \,\&\, H\,'(\langle u, v\rangle) \in Z)$, и Y^* — класс всех таких u, что $u \in X$ и $\forall y\,(y \in \omega \,\&\, \langle u, y\rangle \in \mathscr{D}(H) \supset H\,'(\langle u, y\rangle) \notin Z)$. Тогда $X = X^* \cup Y^*$. Определим теперь G следующим образом: $\mathscr{D}(G) = X$, и если $u \in X^*$, то положим $G\,'u = u$, если же $u \in Y^*$, то положим $G\,'u = F\,'u$. Читатель сам докажет, что $X \underset{G}{\simeq} X \cup Y$.)

Теперь для доказательства теоремы Шрёдера—Бернштейна предположим, что $X \underset{F}{\simeq} Y_1 \,\&\, Y_1 \subseteq Y \,\&\, Y \underset{G}{\simeq} X_1 \,\&\, X_1 \subseteq X$. Пусть $A = G\,``\, Y_1 \subseteq X_1 \subseteq X$. Очевидно, $A \cap (X_1 - A) = 0$, $A \cap (X - X_1) = 0$ и $(X - X_1) \cap (X_1 - A) = 0$. Кроме того, $X = (X - X_1) \cup (X_1 - A) \cup A$, и композиция H функций F и G является взаимно однозначной функцией с областью определения, равной X, и областью значений, равной A. Следовательно, $A \underset{H}{\simeq} X$. Согласно лемме, существует взаимно однозначная функция D такая, что $A \underset{D}{\simeq} X_1$ (ибо $(X_1 - A) \cup A = X_1$). Пусть, наконец, T есть композиция функций H, D, $\breve{G}$, т. е. такая функция, что $T\,'u = (\breve{G})\,'(D\,'(H\,'u))$. Тогда $X \underset{T}{\simeq} Y$, так как $X \underset{H}{\simeq} A$, $A \underset{D}{\simeq} X_1$ и $X_1 \underset{\breve{G}}{\simeq} Y$.

Упражнение

Провести во всех деталях следующее, принадлежащее Уиттекеру, доказательство теоремы Шрёдера — Бернштейна для случая, когда X и Y суть множества. Итак, пусть $X \underset{F}{\simeq} Y_1 \,\&\, Y_1 \subseteq Y \,\&\, Y \underset{G}{\simeq} X_1 \,\&\, X_1 \subseteq X$. Для доказательства $X \simeq Y$ достаточно найти множество $Z \subseteq X$ такое, чтобы результат ограничения функции G множеством $Y - F\,``\, Z$ был взаимно однозначной функцией, отображающей $Y - F\,``\, Z$ на $X - Z$. (В самом деле, имея такое множество, мы далее

положим $H = (Z \mathbin{1} F) \cup ((X - Z) \mathbin{1} \breve{G})$, что означает, что $H`x = F`x$, если $x \in Z$, и $H`x = G`x$, если $x \in X - Z$. Но тогда, очевидно, $X \underset{H}{\simeq} Y$.) Искомым множеством Z является множество $\hat{x}\,(\exists u\,(u \subseteq X \,\&\, x \in u \,\&\, G``(Y - F`` u) \subseteq X - u))$. Заметим, что это доказательство не использует определения ω и вообще не зависит от теории порядковых чисел. Еще одно доказательство имеется у Клини [1952, § 4].

Предложение 4.22. *Если* $X \preceq Y$ *и* $A \preceq B$, *то*

(1) $Y \cap B = 0 \supset X \cup A \preceq Y \cup B$;

(2) $X \times A \preceq Y \times B$;

(3) $\vdash X^A \preceq Y^B$.

Доказательство. (1) Допустим, что $X \underset{F}{\simeq} Y_1 \subseteq Y$ и $A \underset{G}{\simeq} B_1 \subseteq B$. Функцию H с областью определения, равной $X \cup A$, определим таким образом, чтобы выполнялось $H`x = F`x$ для $x \in X$ и $H`x = G`x$ для $x \in A - X$. Тогда $X \cup A \underset{H}{\simeq} H``(X \cup A) \subseteq Y \cup B$. Читателю предоставляется самому доказать пункты (2) и (3).

Упражнения

1. $\vdash X \preceq X \cup Y$.

2. $\vdash X \prec Y \supset \neg (Y \preceq X)$.

3. $\vdash X \prec Y \,\&\, Y \preceq Z \supset X \prec Z$.

Предложение 4.23. (Теорема Кантора.) $\vdash \forall x (x \prec \mathscr{P}(x))$ *и, следовательно,* $\vdash \forall x (x \prec 2^x)$.

Доказательство. (1) Пусть область определения функции F равна x и $F`u = \{u\}$ для любого $u \in x$. Тогда, очевидно, $F`` x \subseteq \mathscr{P}(x)$ и функция F взаимно однозначна. Таким образом, $x \preceq \mathscr{P}(x)$.

(2) Теперь следует доказать, что $\neg (x \simeq \mathscr{P}(x))$. Допустим, что $x \underset{G}{\simeq} \mathscr{P}(x)$ при некотором G. Пусть $y = \hat{u}\,(u \in x \,\&\, u \notin G`u)$. Ясно, что $y \in \mathscr{P}(x)$. Следовательно, существует и притом единственное $z$ в $x$ такое, что $G`z = y$. Так как $\forall u (u \in y \equiv u \in x \,\&\, u \notin G`u)$, то $\forall u (u \in y \equiv u \in x \,\&\, u \notin G`z \equiv u \in x \,\&\, u \notin G`u)$. Отсюда по правилу А4 следует $z \in G`z \equiv z \in x \,\&\, z \notin G`z$. Так как $z \in x$, то мы получаем $z \in G`z \equiv z \notin G`z$ и приходим, таким образом, к противоречию.

Заметим, что мы не доказали $\vdash \forall x \forall y (x \preceq y \vee y \preceq x)$. На самом же деле это предложение и не может быть выведено, ибо, как оказывается, оно эквивалентно аксиоме выбора.

Упражнение

Если теория NBG непротиворечива, то, по предложению 2.12, она имеет счетную модель. Объяснить, почему этот факт не противоречит теореме Кантора, из которой следует, что существуют несчетные бесконечные множества (например, 2^ω)? Это кажущееся — но не настоящее! — противоречие называют иногда парадоксом Сколема.

Отношение равномощности обладает всеми свойствами отношения эквивалентности. Это склоняет нас к тому, чтобы разбить класс всех

множеств на классы эквивалентности по этому отношению. Классом эквивалентности данного множества x является класс всех множеств, равномощных множеству x. Эти классы эквивалентности называются *кардинальными числами* (или *мощностями*). Если, например, u есть множество и $x = \{u\}$, то классом эквивалентности множества x является класс всех одноэлементных множеств $\{v\}$, он называется кардинальным числом 1_c. Аналогично, если $u \neq v$ и $y = \{u, v\}$, то классом эквивалентности для y будет класс всех двухэлементных, т. е. содержащих в точности по два элемента, множеств. Этот класс называется кардинальным числом 2_c, иначе говоря, $2_c = \hat{z}(\exists x_1 \exists y_1 (x_1 \neq y_1 \,\&\, z = \{x_1, y_1\}))$. Следует отметить, что все кардинальные числа, кроме кардинального числа класса 0 (которое равно $\{0\}$), являются собственными классами. Так, например, $V \simeq 1_c$, где V есть универсальный класс. В самом деле, пусть $F`x = x$ для каждого $x \in V$. Тогда, очевидно, $V \underset{F}{\simeq} 1_c$. Но так как $\neg M(V)$, то, по аксиоме замещения, и $\neg M(1_c)$.

Упражнение

$\vdash \neg M(2_c)$.

Поскольку кардинальные числа являются собственными классами, мы не имеем возможности рассматривать классы кардинальных чисел. Это обстоятельство делает трудным или даже невозможным формулирование и доказательство многих интересных фактов о кардинальных числах. По этой причине дальнейшее обсуждение кардинальных чисел на этом уровне мы прекращаем. Большинство утверждений, которые можно было бы сделать о кардинальных числах, могут быть перефразированы в терминах $\simeq$ и $\preceq$. Кроме того, в дальнейшем мы увидим, что если воспользоваться некоторыми дополнительными, содержательно правдоподобными, аксиомами, то открываются иные пути для определения понятия, которое может с успехом заменить понятие кардинального числа.

Упражнение

Доказать $\vdash \forall x \forall R (R\ We\ x \supset \exists \alpha (x \simeq \alpha))$. (Всякое вполне упорядоченное множество равномощно некоторому порядковому числу. Указание. Применить предложение 4.17.)

Конечные множества. Напомним (стр. 193), что ω есть множество всех порядковых чисел α таких, что α и все порядковые числа, меньшие α, являются порядковыми числами первого рода (т. е. являются непосредственно следующими или 0). Элементы ω называются *конечными порядковыми числами*. Множество называется *конечным*, если оно равномощно какому-нибудь конечному порядковому числу.

Определение. $Fin(X) \equiv \exists \alpha (\alpha \in \omega \,\&\, X \simeq \alpha)$. В силу аксиомы замещения R, очевидно, $\vdash Fin(X) \supset M(X)$. Ясно, что все конечные

порядковые числа являются конечными множествами, и $\vdash Fin(X) \& X \simeq Y \supset Fin(Y)$.

Предложение 4.24.

(1) $\vdash \forall\alpha(\alpha \in On - \omega \supset \alpha \simeq \alpha')$.

(2) $\vdash \forall\alpha\forall\beta(\alpha \in \omega \& \alpha \neq \beta \supset \neg \alpha \simeq \beta)$.

(*Никакое конечное порядковое число не равномощно порядковому числу, ему не равному. Отсюда следует, что всякое конечное множество равномощно одному и только одному конечному порядковому числу, и любое бесконечное порядковое число* (*т. е. всякий элемент* $On - \omega$) *не равномощно никакому конечному порядковому числу*.)

(3) $\vdash \forall\alpha\forall x(\alpha \in \omega \& x \subset \alpha \supset \neg \alpha \simeq x)$. (*Никакое конечное порядковое число не может быть равномощно своему собственному подмножеству*.)

Доказательство. (1) Предположим, что $\alpha \in On - \omega$. Определим функцию f следующим образом: $\mathscr{D}(f) = \alpha'$; если $\delta \in \omega$, то $f'\delta = \delta'$, если $\delta \notin \omega$ и $\delta \neq \alpha$, то $f'\delta = \delta$; наконец, $f'\alpha = 0$. Тогда $\alpha' \underset{f}{\simeq} \alpha$.

(2) Предположим противное, и пусть α — наименьшее порядковое число из ω, для которого существует β такое, что $\beta \neq \alpha$ и $\alpha \simeq \beta$. Тогда $\alpha <_0 \beta$. (В противном случае не α, а β было бы наименьшим порядковым числом из ω, равномощным с порядковым числом, ему не равным.) Пусть $\alpha \underset{f}{\simeq} \beta$. Если $\alpha = 0$, то $f = 0$ и $\beta = 0$, что противоречит предположению $\alpha \neq \beta$. Таким образом, $\alpha \neq 0$. Так как $\alpha \in \beta$, то $\alpha = \delta'$ при некотором $\delta \in \omega$. Мы можем также предполагать, что $\beta = \gamma'$ при некотором γ. (Действительно, если $\beta \in \omega$, то так как $\beta \neq 0$, существует такое γ, что $\beta = \gamma'$; если же $\beta \notin \omega$, то, в силу пункта (1), $\beta \simeq \beta'$ и вместо β мы могли бы рассматривать β'.) Итак, $\delta' = \alpha \underset{f}{\simeq} \gamma'$. Так как $\alpha \neq \beta$, то $\delta \neq \gamma$. Рассмотрим два случая. 1) $f'\delta = \gamma$. Тогда, очевидно, $\delta \underset{\delta 1 f}{\simeq} \gamma$. 2) $f'\delta \neq \gamma$. В этом случае существует такое $\mu \in \delta$, что $f'\mu = \gamma$. Пусть $h = ((\delta 1 f) - \{\langle \mu, \gamma\rangle\}) \cup \{\langle \mu, f'\delta\rangle\}$. Имеем $h'\tau = f'\tau$, если $\tau \notin \{\delta, \mu\}$; $h'\mu = f'\delta$. Поэтому $\delta \underset{h}{\simeq} \gamma$. В обоих случаях δ есть конечное порядковое число, меньшее, чем α, и равномощное отличному от него порядковому числу, что противоречит определению α.

(3) Допустим, что существуют такие $\beta \in \omega$, что $\exists x(x \subset \beta \& \beta \simeq x)$. Пусть α — наименьшее из таких β. Очевидно, $\alpha \neq 0$. Следовательно, $\alpha = \gamma'$ при некотором γ. Теперь так же, как и при доказательстве предыдущего пункта, можно показать, что γ равномощно некоторой своей собственной части, чего, разумеется, не может быть из-за минимальности α.

Предложение 4.25.

(1) $\vdash Fin(X) \& Y \subseteq X \supset Fin(Y)$.

(2) $\vdash Fin(X) \& Fin(Y) \supset Fin(X \cup Y)$.

(3) Назовем множество *конечным по Дедекинду*, если оно не равномощно никакому собственному своему подмножеству. *Всякое конечное множество конечно по Дедекинду.* (Обратное утверждение невыводимо без применения дополнительной аксиомы — аксиомы выбора.)

Доказательство. (1) Предположим $Fin(X) \& Y \subseteq X$. Тогда существуют f и α такие, что $\alpha \in \omega$ и $X \underset{f}{\simeq} \alpha$. Положим $g = Y\restriction f$ и $W = g\text{“}Y$. Справедливо $W \subseteq \alpha$. Так как W является множеством порядковых чисел, то отношение E_W вполне упорядочивает W. В силу предложения 4.17, $\langle E_W, W\rangle$ подобно $\langle E_\beta, \beta\rangle$ при некотором β. Следовательно, $W \simeq \beta$. Кроме того, $\beta \leqslant_0 \alpha$. (Ибо в противном случае подобие $\langle E_W, W\rangle$ и $\langle E_\beta, \beta\rangle$ противоречило бы следствию 4.15.) Так как $\alpha \in \omega$, то и $\beta \in \omega$; а так как $W \underset{g}{\simeq} Y$, то получаем окончательно, что $Fin(Y)$.

(2) Рассмотрим множество $Z = \hat{u}(u \in \omega \& \forall x \forall y \forall f(x \underset{f}{\simeq} u \& Fin(y) \supset \supset Fin(x \cup y)))$. Для доказательства этого пункта, очевидно, достаточно показать, что $Z = \omega$. Прежде всего, $0 \in Z$, ибо если $x \simeq 0$, то $x = 0$ и $x \cup y = y$. Рассмотрим теперь произвольное α и допустим, что $\alpha \in Z$. Предположим также, что $x \underset{f}{\simeq} \alpha'$ и $Fin(y)$. Пусть $\alpha = f\text{‘}w$ и $x_1 = x - \{w\}$. Тогда $x_1 \simeq \alpha$. Так как, по предположению, $\alpha \in Z$, то $Fin(x_1 \cup y)$. Но $x \cup y = (x_1 \cup y) \cup \{w\}$. Поэтому $Fin(x \cup y)$ (ибо $\vdash \forall v \forall v_1 (Fin(v) \supset Fin(v \cup \{v_1\}))$). Таким образом, $\alpha' \in Z$. Отсюда, на основании предложения 4.10(3), $Z = \omega$.

(3) Этот пункт следует из предложения 4.24(3).

Определения

Inf (X) означает $\neg Fin(X)$. (Класс X бесконечен.)

Den (X) означает $X \simeq \omega$. (Класс X счетен.)

Нетрудно видеть, что $\vdash Inf(X) \& X \simeq Y \supset Inf(Y)$ и $\vdash Den(X) \& X \simeq \simeq Y \supset Den(Y)$. Так как ω есть множество, то, на основании аксиомы замещения R, получаем $\vdash Den(X) \supset M(X)$.

Предложение 4.26.

(1) $\vdash Inf(X) \& X \subseteq Y \supset Inf(Y)$.

(2) $\vdash Inf(X) \equiv Inf(X \cup \{y\})$.

(3) Класс называется *бесконечным по Дедекинду*, если он равномощен некоторому своему собственному, т. е. отличному от него самого, подмножеству. *Всякий бесконечный по Дедекинду класс бесконечен.*

(4) $\vdash Inf(\omega)$.

Доказательство. Пункт (1) следует из предложения 4.25(1). В силу (1), $\vdash Inf(X) \supset Inf(X \cup \{y\})$, а на основании предложения 4.25(2), $\vdash Inf(X \cup \{y\}) \supset Inf(X)$, что и доказывает пункт (2). Пункт (3) следует из предложения 4.25(3), а пункт (4) следует из $\vdash \omega \notin \omega$.

Предложение 4.27. $\vdash Den(v) \& z \subseteq v \supset (Den(z) \vee Fin(z))$.

Доказательство. Достаточно доказать, что $z \subseteq \omega \supset (Den(z) \vee Fin(z))$. Допустим, что $z \subseteq \omega \,\&\, \neg Fin(z)$. Из $\neg Fin(z)$ следует, что для любого $\alpha \in z$ существует $\beta \in z$ такое, что $\alpha <_0 \beta$ (в противном случае мы имели бы $z \subseteq \alpha'$, а так как справедливо $Fin(\alpha')$, то и $Fin(z)$). Пусть X — функция такая, что $X`\alpha$ для любого $\alpha \in \omega$ есть наименьшее порядковое число $\beta$ в $z$, для которого $\alpha <_0 \beta$. Тогда, согласно предложению 4.13(3) (при $\delta = \omega$), существует функция $Y$, область определения которой совпадает с $\omega$ и такая, что $Y`0$ есть наименьшее порядковое число в z, и $Y`(\gamma')$ для любого $\gamma$ из $\omega$ есть наименьшее порядковое число $\beta$ в $z$ с условием $(Y`\gamma) <_0 \beta$. Функция Y взаимно однозначна, $\mathscr{D}(Y) = \omega$ и $Y``\omega \subseteq z$. Предположим, однако, что $z - Y``\omega \neq 0$ и δ — наименьший элемент в $z - Y``\omega$. Пусть $\tau$ — наименьшее порядковое число в $Y``\omega$, для которого выполнено $\delta <_0 \tau$; тогда $\tau = Y`\sigma$ при некотором $\sigma$ из $\omega$. Так как $\delta <_0 \tau$, то $\sigma \neq 0$ и, следовательно, существует такое $\mu \in \omega$, что $\sigma = \mu'$. Поэтому $\tau$ или, что то же, $Y`\sigma$ есть наименьший элемент в z из тех, которые больше $Y`\mu$. Но $Y`\mu <_0 \delta$, ибо τ есть наименьший элемент в $Y``\omega$ из тех, которые больше $\delta$. Следовательно, $\tau = \delta$, и мы пришли к противоречию. Поэтому допущение $z - Y``\omega \neq 0$ неверно, и, следовательно, $Y``\omega = z$, т. е. $Den(z)$.

Упражнения.

1. $\vdash Fin(x) \supset Fin(\mathscr{P}(x))$. (Указание. Индукцией по α доказать $\forall x\,(x \simeq \alpha \,\&\, \alpha \in \omega \supset Fin(\mathscr{P}(x)))$.)

2. $\vdash Fin(x) \,\&\, \forall y\,(y \in x \supset Fin(y)) \supset Fin(\mathsf{U}(x))$. (Указание. Индукция по α таким, что $x \simeq \alpha$).

3. $\vdash x \preceq y \,\&\, Fin(y) \supset Fin(x)$.

4. $\vdash Fin(\mathscr{P}(x)) \supset Fin(x)$.

5. $\vdash Fin(\mathsf{U}(x)) \supset (Fin(x) \,\&\, \forall y\,(y \in x \supset Fin(y)))$.

6. $\vdash Fin(x) \supset (x \preceq y \vee y \preceq x)$.

7. $\vdash Fin(x) \,\&\, Inf(Y) \supset x \prec Y$.

8. $\vdash Fin(x) \,\&\, y \subset x \supset y \prec x$.

9. $\vdash Fin(x) \,\&\, Fin(y) \supset Fin(x \times y)$.

10. $\vdash Fin(x) \,\&\, Fin(y) \supset Fin(x^y)$.

11. $\vdash Fin(x) \,\&\, y \notin x \supset x \prec (x \cup \{y\})$.

12. Назовем x *минимальным* (соответственно *максимальным*) *элементом класса* Y, если $x \in Y$ и $\forall y\,(y \in Y \supset \neg y \subset x)$ (соответственно $\forall y\,(z \in Y \supset \neg x \subset y)$). Доказать, что класс Z конечен тогда и только тогда, когда всякое непустое множество подмножеств класса Z имеет минимальный (соответственно максимальный) элемент (Тарский [1925]).

13. (a) $\vdash Fin(x) \,\&\, Den(y) \supset Den(x \cup y)$. (Указание. Индукция по α, где $\alpha \simeq x$.)

(b) $\vdash Fin(x) \,\&\, Den(y) \,\&\, x \neq 0 \supset Den(x \times y)$.

(c) Всякое множество y содержит счетное подмножество тогда и только тогда, когда y бесконечно по Дедекинду. (Указание. (i) Предположим, что $x \subseteq y$ и $Den(x)$. Пусть $x \underset{f}{\simeq} \omega$. Определим функцию g на y следующим образом:

$g`u = u$, если $u \in y - x$, и $g`u = (\bar{f})`((f`u)')$ для $u \in x$. (ii) Допустим, что y бесконечно по Дедекинду, т. е. что существует такое x, что $x \subset y$ и $y \underset{f}{\simeq} x$. Пусть $v \in y - x$. Определим функцию h на ω таким образом, чтобы выполнялись равенства $h`0 = v$ и $h`(\alpha') = f`(h`\alpha)$ для любого $\alpha \in \omega$. Функция h взаимно однозначна. В результате имеем $Den(h``\omega)$ и $h``\omega \subseteq y$.)

§ 4. Теорема Хартогса. Начальные порядковые числа. Арифметика порядковых чисел

Мы теперь приступаем к изложению теоремы Хартогса, которой незаслуженно пренебрегают и которая, однако, несет в себе возможности многочисленных применений в теории множеств.

Предложение 4.28. (Хартогс [1915].) *Для любого множества x существует порядковое число, которое не равномощно никакому подмножеству x (существует, следовательно, и наименьшее среди таких порядковых чисел).*

Доказательство. Предположим, что всякое порядковое число α равномощно некоторому подмножеству y множества x. Это значит, что $y \underset{f}{\simeq} \alpha$ при некотором f. На множестве y определим отношение R таким образом, чтобы $\langle u, v\rangle \in R$ выполнялось тогда и только тогда, когда $(f`u) \in (f`v)$. Тогда R вполне упорядочивает y, причем $\langle R, y\rangle$ подобно $\langle E_\alpha, \alpha\rangle$. Определим теперь функцию F с областью определения On и такую, что для любого α $F`\alpha$ есть множество w всех пар $\langle z, y\rangle$, удовлетворяющих условиям: $y \subseteq x$, z вполне упорядочивает y и $\langle E_\alpha, \alpha\rangle$ подобно $\langle z, y\rangle$. (w является множеством, ибо $w \subseteq \mathcal{P}(x \times x) \times \mathcal{P}(x)$.) Для такой функции F выполнено соотношение $F``(On) \subseteq \mathcal{P}(\mathcal{P}(x \times x) \times \times \mathcal{P}(x))$, и, следовательно, $F``(On)$ есть множество. F, кроме того, — функция взаимно однозначная. Поэтому $On = \breve{F}``(F``(On))$, и, следовательно, по аксиоме замещения R, On должно быть множеством, что противоречит предложению 4.7(8).

Пусть $\mathcal{H}$ — функция, которая каждому множеству x сопоставляет порядковое число α, являющееся наименьшим в классе порядковых чисел, не равномощных никакому подмножеству множества x.

Назовем *начальным порядковым числом* всякое порядковое число α, которое не равномощно никакому порядковому числу, меньшему α. В силу предложения 4.24 (2), всякое конечное порядковое число является начальным, а ω есть наименьшее из бесконечных начальных чисел. Для всякого множества x $\mathcal{H}`x$ есть также начальное порядковое число.

В силу принципа трансфинитной индукции (предложение 4.13 (2)), существует такая функция G, у которой областью определения служит On и которая удовлетворяет условиям:

$$G`0 = \omega;$$
$$G`(\alpha') = \mathcal{H}`(G`\alpha);$$
$$G`\lambda = \bigcup(G``\lambda), \text{ если } \lambda \text{ — предельное порядковое число.}$$

Функция G возрастает, т. е. из $\alpha \in \beta$ следует $G`\alpha \in G`\beta$; поэтому, если λ есть предельное порядковое число и всякое значение $G`\alpha$ для $\alpha <_0 \lambda$ является начальным порядковым числом, то таково же и $\bigcup(G``\lambda)$. (В самом деле, порядковое число $\delta = \bigcup(G``\lambda)$ является наименьшей верхней гранью для $G``\lambda$. Допустим, что $\delta \simeq \gamma$ при каком-нибудь $\gamma <_0 \delta$. Тогда существует α, меньшее λ и такое, что $\gamma <_0 G`\alpha$. Но $G`(\alpha') <_0 \delta$. Таким образом, имеем $G`\alpha \preceq G`(\alpha')$ и $G`(\alpha') \preceq \delta \preceq \gamma \preceq G`(\alpha)$, откуда, по теореме Шрёдера—Бернштейна (предложение 4.21 (4)), получаем $G`\alpha \simeq G`(\alpha') = \mathscr{K}`(G`\alpha)$, что противоречит определению функции $\mathscr{K}$.) Итак, доказано, что $G`\alpha$ для любого $\alpha$ есть начальное порядковое число. С другой стороны, верно и то, что всякое бесконечное начальное порядковое число есть $G`\alpha$ при некотором α. (Предположим, что это не так. Пусть тогда σ — наименьшее бесконечное начальное порядковое число, не принадлежащее $G``On$. По аксиоме замещения R, $G``On$ не есть множество, следовательно, в $G``On$ имеются порядковые числа, бо́льшие σ. Пусть μ — наименьшее из них, и пусть $\mu = G`\beta$. Очевидно, $\beta \neq 0$. Если $\beta = \gamma'$ для некоторого $\gamma$, то $G`\gamma <_0 \sigma <_0 G`(\gamma') = \mathscr{K}`(G`\gamma)$, что противоречит определению $\mathscr{K}$. Если же $\beta$ — предельное, то существует $\alpha <_0 \beta$ такое, что $\sigma <_0 G`\alpha <_0 G`\beta$, что противоречит определению β.) Таким образом, G является сохраняющим отношение $\in$ «изоморфизмом» между On и классом всех бесконечных начальных порядковых чисел.

Обозначим $G`\alpha$ через ω_α. Тогда $\omega_0 = \omega$; $\omega_{\alpha'}$ есть наименьшее из начальных порядковых чисел, превосходящих ω_α, и ω_λ для предельного порядкового числа λ есть начальное порядковое число, являющееся наименьшей верхней гранью множества всех ω_α при $\alpha <_0 \lambda$. Из предложения 4.14 следует, что $\alpha \leqslant_0 \omega_\alpha$ для всех α. При этом любое порядковое число α равномощно с единственным начальным порядковым числом $\omega_\beta \leqslant_0 \alpha$, а именно, с наименьшим из порядковых чисел, равномощных с α.

Обратимся теперь к арифметике порядковых чисел. Выше (стр. 196—197) были уже определены сложение, умножение и возведение в степень:

(I)
$$\beta +_0 0 = \beta,$$
$$\beta +_0 \gamma' = (\beta +_0 \gamma)',$$
$$Lim(\alpha) \supset \beta +_0 \alpha = \bigcup_{\tau <_0 \alpha} (\beta +_0 \tau);$$

(II)
$$\beta \times_0 0 = 0,$$
$$\beta \times_0 (\gamma') = (\beta \times_0 \gamma) +_0 \beta,$$
$$Lim(\alpha) \supset \beta \times_0 \alpha = \bigcup_{\tau <_0 \alpha} (\beta \times_0 \tau);$$

(III)
$$\beta^0 = 1,$$
$$\beta^{\gamma'} = (\beta^\gamma) \times_0 \beta,$$
$$Lim(\alpha) \supset \beta^\alpha = \bigcup_{\tau <_0 \alpha} (\beta^\tau).$$

Предложение 4.29. *Следующие формулы являются теоремами:*

(1) $\beta +_0 1 = \beta'$;
(2) $0 +_0 \beta = \beta$;
(3) $0 <_0 \beta \supset \alpha <_0 \alpha +_0 \beta \,\&\, \beta \leqslant_0 \alpha +_0 \beta$;
(4) $\beta <_0 \gamma \supset \alpha +_0 \beta <_0 \alpha +_0 \gamma$;
(5) $\alpha +_0 \beta = \alpha +_0 \delta \supset \beta = \delta$;
(6) $\alpha <_0 \beta \supset \exists_1 \delta\, (\alpha +_0 \delta = \beta)$;
(7) $x \subseteq On \supset \alpha +_0 \bigcup\limits_{\beta \in x} \beta = \bigcup\limits_{\beta \in x} (\alpha +_0 \beta)$;
(8) $0 <_0 \alpha \,\&\, 1 <_0 \beta \supset \alpha <_0 \alpha \times_0 \beta$;
(9) $0 <_0 \alpha \,\&\, 0 <_0 \beta \supset \beta \leqslant_0 \alpha \times_0 \beta$;
(10) $\gamma <_0 \beta \,\&\, 0 <_0 \alpha \supset \alpha \times_0 \gamma <_0 \alpha \times_0 \beta$;
(11) $x \subseteq On \supset \alpha \times_0 \bigcup\limits_{\beta \in x} \beta = \bigcup\limits_{\beta \in x} (\alpha \times_0 \beta)$.

Доказательство. (1) $\beta +_0 1 = \beta +_0 (0') = (\beta +_0 0)' = (\beta)'$.

(2) Воспользуемся трансфинитной индукцией (предложение 4.12). Пусть $X = \hat{\beta}\,(0 +_0 \beta = \beta)$. Прежде всего $0 \in X$, так как $0 +_0 0 = 0$. Если же $0 +_0 \gamma = \gamma$, то $0 +_0 (\gamma') = (0 +_0 \gamma)' = \gamma'$. Наконец, если $Lim\,(\alpha)$ и $0 +_0 \tau = \tau$ для любого $\tau <_0 \alpha$, то $0 +_0 \alpha = \bigcup\limits_{\tau <_0 \alpha} (0 +_0 \tau) = \bigcup\limits_{\tau <_0 \alpha} \tau = \alpha$, потому что $\bigcup\limits_{\tau <_0 \alpha} \tau$ есть наименьшая верхняя грань множества всех τ, меньших α.

(3) Пусть $X = \hat{\beta}\,(0 <_0 \beta \supset \alpha <_0 \alpha +_0 \beta)$. Докажем $X = On$ с помощью трансфинитной индукции. Очевидно, $0 \in X$. Если $\gamma \in X$, то $\alpha \leqslant_0 \alpha +_0 \gamma$; отсюда получаем $\alpha \leqslant_0 \alpha +_0 \gamma < (\alpha +_0 \gamma)' = \alpha +_0 (\gamma')$. Если, наконец, $Lim\,(\lambda)$ и $\tau \in X$ для всех $\tau <_0 \lambda$, то $\alpha <_0 \alpha' = \alpha +_0 1 \leqslant_0 \bigcup\limits_{\tau <_0 \lambda} (\alpha +_0 \tau) = \alpha +_0 \lambda$. Доказательство второй части этого пункта оставляем читателю в качестве упражнения.

(4) Снова применяем трансфинитную индукцию. Пусть $X = \hat{\gamma}(\forall \alpha \forall \beta(\beta <_0 <_0 \gamma \supset \alpha +_0 \beta <_0 \alpha +_0 \gamma))$. Очевидно, $0 \in X$. Пусть $\gamma \in X$ и $\beta <_0 \gamma'$. Тогда $\beta <_0 \gamma$ или $\beta = \gamma$. Если $\beta <_0 \gamma$, то, в силу $\gamma \in X$, $\alpha +_0 \beta <_0 \alpha +_0 +_0 \gamma <_0 (\alpha +_0 \gamma)' = \alpha +_0 \gamma'$. Если $\beta = \gamma$, то $\alpha +_0 \beta = \alpha +_0 \gamma <_0 (\alpha +_0 \gamma)' = = \alpha +_0 \gamma'$. Следовательно, $\gamma' \in X$. Пусть $Lim\,(\lambda)$ и $\tau \in X$ при любом $\tau <_0 \lambda$. Предположим $\beta <_0 \lambda$. Тогда $\beta <_0 \tau$ при некотором $\tau <_0 \lambda$, в силу $Lim\,(\lambda)$. Следовательно, так как $\tau \in X$, то $\alpha +_0 \beta <_0 \alpha +_0 \tau \leqslant_0 \leqslant_0 \bigcup\limits_{\tau <_0 \lambda} (\alpha +_0 \tau) = \alpha +_0 \lambda$. Отсюда имеем $\lambda \in X$.

(5) Допустим $\alpha +_0 \beta = \alpha +_0 \delta$. Справедливо одно из трех: $\beta <_0 \delta$, $\delta <_0 \beta$ или $\beta = \delta$. Если $\beta <_0 \delta$, то $\alpha +_0 \beta <_0 \alpha +_0 \delta$, а если $\delta <_0 \beta$, то $\alpha +_0 \delta <_0 \alpha +_0 \beta$ — и то и другое следует из предыдущего пункта (4) и противоречит предположению, согласно которому $\alpha +_0 \beta = \alpha +_0 \delta$ Остается принять, что $\beta = \delta$.

(6) Единственность δ следует из (5). Докажем существование. Положим $X = \hat{\beta}(\alpha <_0 \beta \supset \exists_1 \delta(\alpha +_0 \delta = \beta))$. Ясно, что $0 \in X$. Пусть $\gamma \in X$, и пусть $\alpha <_0 \gamma'$. Тогда $\alpha <_0 \gamma$ или $\alpha = \gamma$. Если $\alpha <_0 \gamma$, то $\exists_1 \delta(\alpha +_0 \delta = \gamma)$, и пусть σ — какое-нибудь порядковое число такое, что $\alpha +_0 \sigma = \gamma$. Тогда $(\alpha +_0 \sigma') = (\alpha +_0 \sigma)' = \gamma'$. Таким образом, $\exists \delta(\alpha +_0 \delta = \gamma')$, и, следовательно, $\gamma' \in X$. Предположим, наконец, что $Lim(\lambda)$ и $\tau \in X$ при всяком $\tau <_0 \lambda$. Пусть $\alpha <_0 \lambda$. Рассмотрим функцию f такую, что для любого μ, удовлетворяющего неравенствам $\alpha <_0 \mu <_0 \lambda$, $f'\mu$ есть (единственное) порядковое число δ, для которого $\alpha +_0 \delta = \mu$. Заметим, что $\lambda = \bigcup\limits_{\alpha <_0 \mu <_0 \lambda} \mu = \bigcup\limits_{\alpha <_0 \mu <_0 \lambda} (\alpha +_0 f'\mu)$, и если $\alpha <_0 \mu <_0 \lambda$, то $f'\mu <_0 f'(\mu')$. Отсюда, положив $\rho = \bigcup\limits_{\alpha <_0 \mu <_0 \lambda} (f'\mu)$, получаем

$$\lambda = \bigcup_{\alpha <_0 \mu <_0 \lambda} (\alpha +_0 f'\mu) = \bigcup_{\sigma <_0 \rho} (\alpha +_0 \sigma) = \alpha +_0 \rho.$$

(7) Пусть $x \subseteq On$. В силу предыдущего пункта (6), существует такое δ, что $\alpha +_0 \delta = \bigcup\limits_{\beta \in x} (\alpha +_0 \beta)$. Мы должны доказать, что $\delta = \bigcup\limits_{\beta \in x} \beta$. Если $\beta \in x$, то $\alpha +_0 \beta \leqslant_0 \alpha + \delta$. Следовательно, $\beta \leqslant_0 \delta$, в силу пункта (4). Таким образом, δ есть верхняя грань множества всех $\beta \in x$. Отсюда $\bigcup\limits_{\beta \in x} \beta \leqslant_0 \delta$. С другой стороны, если $\beta \in x$, то $\alpha +_0 \beta \leqslant_0 \alpha +_0 \bigcup\limits_{\beta \in x} \beta$. Следовательно, $\alpha +_0 \delta = \bigcup\limits_{\beta \in x} (\alpha +_0 \beta) \leqslant_0 \alpha +_0 \bigcup\limits_{\beta \in x} \beta$ и, таким образом, в силу пункта (4), $\delta \leqslant_0 \bigcup\limits_{\beta \in x} \beta$. Отсюда окончательно получаем $\delta = \bigcup\limits_{\beta \in x} \beta$.

Пункты (8)—(11) оставляются читателю в качестве упражнений.

Предложение 4.30. *Следующие формулы являются теоремами*:

(1) $\beta \times_0 1 = \beta \,\&\, 1 \times_0 \beta = \beta$;
(2) $0 \times_0 \beta = 0$;
(3) $(\alpha +_0 \beta) +_0 \gamma = \alpha +_0 (\beta +_0 \gamma)$;
(4) $(\alpha \times_0 \beta) \times_0 \gamma = \alpha \times_0 (\beta \times_0 \gamma)$;
(5) $\alpha \times_0 (\beta +_0 \gamma) = (\alpha \times_0 \beta) +_0 (\alpha \times_0 \gamma)$;
(6) $\beta^1 = \beta \,\&\, 1^\beta = 1$;
(7) $(\beta^\gamma)^\delta = \beta^{\gamma \times_0 \delta}$;
(8) $\beta^{\gamma +_0 \delta} = \beta^\gamma \times_0 \beta^\delta$;
(9) $1 <_0 \alpha \,\&\, \beta <_0 \gamma \supset \alpha^\beta <_0 \alpha^\gamma$.

Доказательство. (1) В силу предложения 4.29 (2), $\beta \times_0 1 = \beta \times_0 0' = (\beta \times_0 0) +_0 \beta = 0 +_0 \beta = \beta$. Равенство же $1 \times_0 \beta = \beta$ легко доказывается трансфинитной индукцией по β.

(2) Равенство $0 \times_0 \beta = 0$ также легко доказывается с помощью трансфинитной индукции.

(3) Пусть $X = \hat{\gamma}(\forall\alpha\,\forall\beta\,((\alpha +_0 \beta) +_0 \gamma = \alpha +_0 (\beta +_0 \gamma)))$. Как легко видеть, $(\alpha +_0 \beta) +_0 0 = \alpha +_0 \beta = \alpha +_0 (\beta +_0 0)$, т. е. $0 \in X$. Пусть $\gamma \in X$. Тогда $(\alpha +_0 \beta) +_0 \gamma' = ((\alpha +_0 \beta) +_0 \gamma)' = (\alpha +_0 (\beta +_0 \gamma))' = \alpha +_0 (\beta +_0 \gamma)' = \alpha +_0 (\beta +_0 \gamma')$, т. е. $\gamma' \in X$. Наконец, пусть $Lim(\lambda)$ и $\tau \in X$ при любом $\tau <_0 \lambda$. Тогда, применив предложение 4.29 (7), получаем $(\alpha +_0 \beta) +_0 +_0 \lambda = \bigcup\limits_{\tau <_0 \lambda} ((\alpha +_0 \beta) +_0 \tau) = \bigcup\limits_{\tau <_0 \lambda} (\alpha +_0 (\beta +_0 \tau)) = \alpha +_0 \bigcup\limits_{\tau <_0 \lambda} (\beta +_0 \tau) = \alpha +_0 +_0 (\beta +_0 \lambda)$.

Доказательства пунктов (4)—(9) оставляем читателю в качестве упражнений.

Мы хотели бы теперь особо остановиться на свойствах операций сложения и умножения порядковых чисел, ограниченных областью ω.

Предложение 4.31. *Пусть* α, β, γ *суть элементы* ω. *Тогда*

(1) $\alpha +_0 \beta \in \omega$;
(2) $\alpha \times_0 \beta \in \omega$;
(3) $\alpha^\beta \in \omega$;
(4) $\alpha +_0 \beta = \beta +_0 \alpha$;
(5) $\alpha \times_0 \beta = \beta \times_0 \alpha$;
(6) $(\alpha +_0 \beta) \times_0 \gamma = (\alpha \times_0 \gamma) +_0 (\beta \times_0 \gamma)$;
(7) $(\alpha \times_0 \beta)^\gamma = \alpha^\gamma \times_0 \beta^\gamma$.

Доказательство. (1) Индукция по β. Пусть $X = \hat{\beta}(\forall\alpha(\alpha \in \omega \supset \supset \alpha +_0 \beta \in \omega))$. Очевидно, $0 \in X$. Предположим, что $\beta \in X$ и $\alpha \in \omega$; тогда, согласно определению X, $\alpha +_0 \beta \in \omega$. Отсюда, на основании предложения 4.10 (2), получаем $\alpha +_0 (\beta') = (\alpha +_0 \beta)' \in \omega$. Следовательно, по предложению 4.10 (3), $\omega \subseteq X$.

Читатель сам докажет пункты (2) и (3).

(4) Лемма. $\vdash \alpha \in \omega \,\&\, \beta \in \omega \supset \alpha' +_0 \beta = \alpha +_0 \beta'$.

Пусть $Y = \hat{\beta}(\beta \in \omega \,\&\, \forall\alpha(\alpha \in \omega \supset \alpha' +_0 \beta = \alpha +_0 \beta'))$. Легко видеть, что $0 \in Y$. Предположим, что $\beta \in Y$ и $\alpha \in \omega$. Согласно определению Y, $\alpha' +_0 \beta = \alpha +_0 \beta'$. Тогда $\alpha' +_0 \beta' = (\alpha' +_0 \beta)' = (\alpha +_0 \beta')' = \alpha +_0 (\beta')'$. Следовательно, и $\beta' \in Y$.

Теперь для доказательства пункта (4) положим $X = \hat{\beta}(\beta \in \omega \,\&\, \& \forall\alpha(\alpha \in \omega \supset \alpha +_0 \beta = \beta +_0 \alpha))$. Очевидно, $0 \in X$, а с помощью леммы легко доказать, что из $\beta \in X$ следует $\beta' \in X$.

Доказательства пунктов (5)—(7) оставляются в качестве упражнений.

Читатель, вероятно, уже обратил внимание на то, что недоказанными остались некоторые основные законы арифметических операций, обычно справедливые в других, хорошо известных числовых системах; таковы, например, закон коммутативности сложения и закон коммутативности умножения. Следующие примеры показывают, что эти и некоторые другие законы обычной арифметики не переносятся на область порядковых чисел.

Примеры. 1. $\exists\alpha\exists\beta\,(\alpha +_0 \beta \neq \beta +_0 \alpha)$. В самом деле, имеем, с одной стороны, $1 +_0 \omega = \bigcup\limits_{\alpha<_0\omega} (1 +_0 \alpha) = \omega$ и вместе с тем $\omega <_0 \omega' = \omega +_0 1$

2. $\exists\alpha\exists\beta\,(\alpha \times_0 \beta \neq \beta \times_0 \alpha)$. Действительно, $2 \times_0 \omega = \bigcup\limits_{\alpha<_0\omega} (2 \times_0 \alpha) = \omega <_0 <_0 \omega +_0 \omega = (\omega \times_0 1) +_0 (\omega \times_0 1) = \omega \times_0 (1 +_0 1) = \omega \times_0 2$.

3. $\exists\gamma\exists\alpha\exists\beta\,((\alpha +_0 \beta) \times_0 \gamma \neq (\alpha \times_0 \gamma) +_0 (\beta \times_0 \gamma))$. Действительно, $(1 +_0 +_0 1) \times_0 \omega = 2 \times_0 \omega = \omega$ и $\omega <_0 \omega +_0 \omega = (1 \times_0 \omega) +_0 (1 \times_0 \omega)$.

4. $\exists\alpha\exists\beta\exists\gamma\,((\alpha \times_0 \beta)^\gamma \neq \alpha^\gamma \times_0 \beta^\gamma)$. При $\alpha = \beta = 2$ и $\gamma = \omega$ имеем $(2 \times_0 2)^\omega = 4^\omega = \bigcup\limits_{\alpha<_0\omega} 4^\alpha = \omega$, $2^\omega = \bigcup\limits_{\alpha<_0\omega} 2^\alpha = \omega$ и $\omega <_0 \omega \times_0 \omega = 2^\omega \times_0 2^\omega$.

Всякой формуле $\mathscr{A}$ формальной арифметической теории S (см. гл. 3) можно следующим образом сопоставить некоторую формулу $\mathscr{A}^*$ теории NBG: заменим сначала в $\mathscr{A}$ все знаки «$+$» и «$\cdot$» соответственно на «$+_0$» и «$\times_0$», затем, если $\mathscr{A}$ есть $\mathscr{B} \supset \mathscr{C}$ или $\neg\mathscr{B}$ и если $\mathscr{B}^*$ и $\mathscr{C}^*$ уже построены, то определим $\mathscr{A}^*$ соответственно как $\mathscr{B}^* \supset \mathscr{C}^*$ или $\neg\mathscr{B}^*$, если же $\mathscr{A}$ есть $\forall x\mathscr{B}(x)$ и $\mathscr{B}^*(x)$ построено, то определим $\mathscr{A}^*$ как $\forall x\,(x \in \omega \supset \mathscr{B}^*(x))$, чем и завершается определение $\mathscr{A}^*$. Определим теперь формулу $\mathscr{A}\#$ как $x_1 \in \omega \,\&\, \ldots \,\&\, x_n \in \omega \supset \mathscr{A}^*$, где $x_1, \ldots, x_n$ — все свободные переменные формулы $\mathscr{A}$. Таким образом, мы ограничили все переменные областью ω и проинтерпретировали сложение, умножение и функцию «непосредственно следующий» соответствующими операциями над порядковыми числами. В результате всякая аксиома $\mathscr{A}$ теории S преобразуется в некоторую теорему $\mathscr{A}\#$ теории NBG. (Для аксиом (S1) — (S3) это очевидно; (S4)$\#$ является теоремой в NBG, в силу предложения 4.9(3), а (S5)$\#$ — (S8)$\#$ выражают свойства сложения и умножения порядковых чисел (см. стр. 196—197). Для всякой формулы $\mathscr{A}$ теории S формула $\mathscr{A}\#$ есть предикативная формула теории NBG. Поэтому все частные случаи (S9)$\#$ выводимы с помощью трансфинитной индукции. Действительно, пусть $\mathscr{A}\#(0)$ & & $\forall x\,(x \in \omega \supset (\mathscr{A}\#(x) \supset \mathscr{A}\#(x')))$; положим $X = \hat{y}\,(y \in \omega \,\&\, \mathscr{A}\#(y))$; тогда, по предложению 4.10(3), $\omega \subseteq X$. Следовательно, $\forall x\,(x \in \omega \supset \supset \mathscr{A}\#(x))$.) Рассмотрим теперь правила вывода. Легко показать, что если $\vdash_{\mathrm{NBG}} \mathscr{A}\#$ и $\vdash_{\mathrm{NBG}} (\mathscr{A} \supset \mathscr{B})\#$, то $\vdash_{\mathrm{NBG}} \mathscr{B}\#$. Верно также, что если $\vdash_{\mathrm{NBG}} \mathscr{A}\#(x)$, то $\vdash_{\mathrm{NBG}} (\forall x\mathscr{A}(x))\#$. В самом деле, формула $\mathscr{A}\#(x)$ имеет вид $x \in \omega \,\&\, y_1 \in \omega \,\&\, \ldots \,\&\, y_m \in \omega \supset \mathscr{A}^*(x)$, поэтому если эта формула выводима в NBG, то выводима, очевидно, и формула $y_1 \in \omega \,\&\, \ldots \,\&\, y_m \in \omega \supset \forall x\,(x \in \omega \supset \mathscr{A}^*(x))$, но эта последняя и есть $(\forall x\,\mathscr{A}(x))\#$. Отсюда индукцией по длине вывода формулы $\mathscr{A}$ в S уже нетрудно доказать, что если формула $\mathscr{A}$ является теоремой в S, то формула $\mathscr{A}\#$ является теоремой в NBG; и мы можем перевести в NBG все теоремы теории S, выведенные в главе 3.

Рассмотрим арифметическую функцию h такую, что если x есть гёделев номер формулы $\mathscr{A}$ теории S, то h(x) есть гёделев номер формулы $\mathscr{A}\#$ теорий NBG, и h(x) = 0, если x не является гёделевым номером никакой формулы теории S. Можно доказать, что функция h

рекурсивна (и даже примитивно рекурсивна). Пусть K — произвольное непротиворечивое расширение теории NBG. Если x есть гёделев номер некоторой теоремы теории S, то, как мы теперь знаем, h(x) есть гёделев номер некоторой теоремы теории NBG, а следовательно, и гёделев номер некоторой теоремы теории K. Пусть S′ — расширение теории S, получающееся, если в качестве аксиом взять все те формулы $\mathscr{A}$ теории S, для которых соответствующие формулы $\mathscr{A}\#$ являются теоремами теории K. Поскольку теория K, согласно предположению, непротиворечива, то непротиворечива и теория S′, а так как теория S существенно рекурсивно неразрешима (следствие 3.37), то теория S′ рекурсивно неразрешима, т. е. не рекурсивно множество $T_{S'}$ гёделевых номеров теорем теории S′. Допустим теперь, что теория K рекурсивно разрешима, т. е. что рекурсивно множество T_K гёделевых номеров теорем теории K. Но характеристические функции $C_{T_{S'}}$ и C_{T_K} множеств $T_{S'}$ и T_K связаны соотношением $C_{T_{S'}}(x) = C_{T_K}(h(x))$. Следовательно, тогда и множество $T_{S'}$ оказалось бы рекурсивным, что противоречит рекурсивной неразрешимости теории S′. Таким образом, теория K рекурсивно неразрешима, и, следовательно, если теория NBG непротиворечива, то она существенно рекурсивно неразрешима. Рекурсивная неразрешимость всякой рекурсивно аксиоматизируемой теории влечет, как известно, неполноту такой теории (см. упражнение 1(b), стр. 168). Таким образом, мы имеем следующий результат: *если теория* NBG *непротиворечива, то она существенно рекурсивно неразрешима и существенно неполна.* (Этот результат может быть получен и непосредственно, т. е. тем же способом, которым в главе 3 нами был получен соответствующий результат для теории S. См. также упражнения на стр. 175.) По-видимому, теория NBG может служить базой для построения всей современной математики (мы хотим этим сказать только, что для всякого математика ясна принципиальная возможность перевода любой математической теоремы на язык теории NBG, а затем и доказательства ее в NBG или в каком-нибудь подходящем расширении NBG, получаемом добавлением различных «экстра-аксиом», вроде аксиомы выбора). Поэтому существенная неполнота теории NBG указывает, как нам кажется, на известную недостаточность «аксиоматического подхода к математике». Это заключение не зависит от специфических особенностей теории NBG. Из проведенного только что для этой теории рассуждения видно, что существенно рекурсивно неразрешимой и существенно неполной должна быть также и всякая другая непротиворечивая теория (включая сюда, наряду с теориями первого порядка, и «теории высших порядков»), если только представленная в ней арифметика натуральных чисел достаточно сильна для получения всех теорем теории S (или хотя бы теории RR). (В самом деле, достаточно лишь доказать, что в данной теории представимы все рекурсивные функции (см. следствие 3.36). Дальнейшие исследования по вопросам неразрешимости и неполноты см. у Шмульяна [1961] и Тарского, Мостовского и Робинсона [1953].)

Упражнение

Убедиться в том, что определенная выше функция h рекурсивна. (Заметим, что, поскольку $+_0$, $\times_0$ и 0 являются дополнительно введенными в NBG функциональными буквами и предметной константой, здесь следует показать, что соответствующее отображение, о котором говорится в предложении 2.29, рекурсивно.)

Имеется несколько фактов из «арифметики мощностей» порядковых чисел, которые мы хотели бы теперь рассмотреть. К «арифметике мощностей» мы относим свойства, связанные с операциями объединения $\bigcup$, декартова произведения $\times$ и X^Y, противопоставляемых операциям $+_0$, $\times_0$, и возведения в степень порядковых чисел. Напомним, что $\times$ и $\times_0$— это две различные операции и что операции X^Y (класс всех отображений Y в X) и α^β (возведение в степень для порядковых чисел), несмотря на сходство обозначений, не имеют между собой ничего общего. (Из примера 4 на стр. 212 мы знаем, что $2^\omega = \omega$ в смысле возведения в степень порядковых чисел, в то время как, в силу теоремы Кантора, $\omega \prec 2^\omega$, если под 2^ω понимать множество всех функций, отображающих ω в $2 = \{0, \{0\}\}$.) В дальнейшем, если это будет необходимо для избежания недоразумений, мы будем α^β в смысле возведения в степень порядковых чисел обозначать через $\exp(\alpha, \beta)$.

Предложение 4.32.

(a) $\vdash \omega \times \omega \simeq \omega$.

(b) *Если каждый из классов X и Y содержит не менее двух элементов, то* $X \bigcup Y \preceq X \times Y$.

(c) $Den(x) \,\&\, Den(y) \supset Den(x \bigcup y)$.

Доказательство. (a) Пусть f есть функция с областью определения ω и такая, что $f`\alpha = \langle \alpha, 0 \rangle$ для любого $\alpha \in \omega$. Такая функция является взаимно однозначной и отображает ω в некоторое подмножество множества $\omega \times \omega$. Поэтому $\omega \preceq \omega \times \omega$. Обратно, пусть g— функция с областью определения $\omega \times \omega$ и такая, что $g`\langle \alpha, \beta \rangle = 2^\alpha \times_0 3^\beta$ для любой пары $\langle \alpha, \beta \rangle \in \omega \times \omega$. Читатель может сам доказать в качестве упражнения, что эта функция взаимно однозначна. Следовательно, $\omega \times \omega \preceq \omega$. По теореме Шрёдера—Бернштейна, $\omega \times \omega \simeq \omega$.

(b) Пусть $a_1 \in X$, $a_2 \in X$, $a_1 \neq a_2$, $b_1 \in Y$, $b_2 \in Y$ и $b_1 \neq b_2$. Определим функцию f следующим образом:

$$f`x = \begin{cases} \langle x, b_1 \rangle, & \text{если } x \in X; \\ \langle a_1, x \rangle, & \text{если } x \in Y - X \text{ и } x \neq b_1; \\ \langle a_2, b_2 \rangle, & \text{если } x = b_1 \text{ и } x \in Y - X. \end{cases}$$

Функция f является взаимно однозначной, с областью определения $X \bigcup Y$ и областью значений в виде некоторого подмножества $X \times Y$. Следовательно, $X \bigcup Y \preceq X \times Y$.

(c) Пусть $Den(A)$ и $Den(B)$. Тогда множества A и B содержат каждое не менее двух элементов. Поэтому, в силу предыдущего пункта (b),

$A \cup B \preceq A \times B$. Но $A \simeq \omega$ и $B \simeq \omega$. Следовательно, $A \times B \simeq \omega \times \omega$, и потому $A \cup B \preceq \omega \times \omega \simeq \omega$. В силу предложения 4.27, либо $Den(A \cup B)$, либо $Fin(A \cup B)$. Но так как $A \subseteq A \cup B$ и $Den(A)$, то $\neg Fin(A \cup B)$.

Для дальнейшего изучения сложения и умножения порядковых чисел весьма полезно получить конкретную интерпретацию этих операций.

Предложение 4.33 (сложение). *Пусть* $\langle R, A\rangle$ *подобно* $\langle E_\alpha, \alpha\rangle$, $\langle S, B\rangle$ *подобно* $\langle E_\beta, \beta\rangle$ и $A \cap B = 0$. *Зададим отношение* T *на* $A \cup B$ *условием*: $\langle x, y\rangle \in T \equiv (x \in A \,\&\, y \in B) \vee (x \in A \,\&\, y \in A \,\&\, \langle x, y\rangle \in R) \vee (x \in B \,\&\, y \in B \,\&\, \langle x, y\rangle \in S)$. (Таким образом, T совпадает с R на A и с S на B, и всякий элемент из A T-предшествует всякому элементу из B.) *Тогда* T *вполне упорядочивает* $A \cup B$ *и* $\langle T, A \cup B\rangle$ *подобно* $\langle E_{\alpha +_0 \beta}, \alpha +_0 \beta\rangle$.

Доказательство. Прежде всего, легко убедиться в том, что T вполне упорядочивает $A \cup B$, поскольку R и S вполне упорядочивают соответственно A и B. Чтобы доказать подобие $\langle T, A \cup B\rangle$ и $\langle E_{\alpha +_0 \beta}, \alpha +_0 \beta\rangle$, применим трансфинитную индукцию по β. Если $\beta = 0$, то и $B = 0$, и тогда $T = R$, $A \cup B = A$ и $\alpha +_0 \beta = \alpha$, а потому, очевидно, $\langle T, A \cup B\rangle$ и $\langle E_{\alpha +_0 \beta}, \alpha +_0 \beta\rangle$ подобны. Предположим, что утверждение верно для γ, и положим $\beta = \gamma'$. Так как $\langle S, B\rangle$ и $\langle E_\beta, \beta\rangle$ подобны, то имеется функция f с областью определения B и областью значений β и такая, что для любых x и y из B $\langle x, y\rangle \in S$ тогда и только тогда, когда $f'x \in f'y$. Пусть $b = (\check{f})'\gamma$, и положим $B_1 = B - \{b\}$ и $S_1 = S \cap (B_1 \times B_1)$. Из того, что b является максимальным относительно отношения S элементом в B, следует, что S_1 вполне упорядочивает B_1. Кроме того, очевидно, $B_1 \mathbf{1} f$ является подобным отображением B_1 на γ. Пусть $T_1 = T \cap ((A \cup B_1) \times (A \cup B_1))$. По индуктивному предположению, $\langle T_1, A \cup B_1\rangle$ подобно $\langle E_{\alpha +_0 \gamma}, \alpha +_0 \gamma\rangle$ с некоторым подобным отображением g, имеющим областью определения $A \cup B_1$ и областью значений $\alpha +_0 \gamma$. Продолжим g до $g_1 = g \cup \{\langle b, \alpha +_0 \gamma\rangle\}$. Эта последняя функция и осуществляет подобное отображение $A \cup B$ на $(\alpha +_0 \gamma)' = \alpha +_0 \gamma' = \alpha +_0 \beta$. Пусть, наконец, имеем $Lim(\beta)$, и предположим, что утверждение справедливо при любом $\tau <_0 \beta$. Пусть снова f — подобное отображение B на β. Для каждого $\tau <_0 \beta$ положим $B_\tau = (\check{f})''\tau$, $S_\tau = S \cap (B_\tau \times B_\tau)$ и $T_\tau = T \cap ((A \cup B_\tau) \times (A \cup B_\tau))$. Согласно индуктивному предположению и в силу следствия 4.16(2), для каждого $\tau <_0 \beta$ существует единственная функция g_τ, осуществляющая подобие пар $\langle T_\tau, A \cup B_\tau\rangle$ и $\langle E_{\alpha +_0 \tau}, \alpha +_0 \tau\rangle$. Очевидно также, что если $\tau_1 <_0 \tau_2 <_0 \beta$, то $T_{\tau_1} \mathbf{1} g_{\tau_2}$ осуществляет подобие пар $\langle T_{\tau_1}, A \cup B_{\tau_1}\rangle$ и $\langle E_{\alpha +_0 \tau_1}, \alpha +_0 \tau_1\rangle$, и, следовательно, в силу единственности τ_1, $T_{\tau_1} \mathbf{1} g_{\tau_2} = g_{\tau_1}$, а потому g_{τ_2} является продолжением g_{τ_1}. Таким образом, функция $g = \bigcup\limits_{\tau <_0 \beta} g_\tau$ осуществляет подобие $\langle T, \bigcup\limits^{\tau <_0 \beta} (A \cup B_\tau)\rangle$ и $\langle E_{\bigcup\limits_{\tau <_0 \beta} (\alpha +_0 \tau)}, \bigcup\limits_{\tau <_0 \beta} (\alpha +_0 \tau)\rangle$. Но $\bigcup\limits_{\tau <_0 \beta} (A \cup B_\tau) = A \cup B$ и $\bigcup\limits^{\tau <_0 \beta} (\alpha +_0 \tau) = \alpha +_0 \beta$, чем и завершается трансфинитная индукция.

Предложение 4.34 (умножение). *Пусть* $\langle R, A\rangle$ *подобно* $\langle E_\alpha, \alpha\rangle$, $\langle S, B\rangle$ *подобно* $\langle E_\beta, \beta\rangle$ *и отношение* W *на* $A \times B$ *задано условием*

$\langle\langle x, y\rangle, \langle u, v\rangle\rangle \in W \equiv (x \in A \,\&\, u \in A \,\&\, y \in B \,\&\, v \in B) \,\&\, ((\langle y, v\rangle \in S) \vee (y = v \,\&\, \langle x, u\rangle \in R))$. *Тогда* W *вполне упорядочивает* $A \times B$ *и* $\langle W, A \times B\rangle$ *подобно* $\langle E_{\alpha \times_0 \beta}, \alpha \times_0 \beta\rangle$.

Доказательство. Аналогично доказательству предыдущего предложения 4.33. Предоставляется читателю в качестве упражнения.

Примеры. 1. $2 \times_0 \omega = \omega$. Пусть $\langle R, A\rangle = \langle E_2, 2\rangle$ и $\langle S, B\rangle = \langle E_\omega, \omega\rangle$. Тогда пары из $2 \times \omega$ могут быть вполне упорядочены следующим образом: $\langle 0, 0\rangle$, $\langle 1, 0\rangle$, $\langle 0, 1\rangle$, $\langle 1, 1\rangle$, $\langle 0, 2\rangle$, $\langle 1, 2\rangle$, ..., $\langle 0, n\rangle$, $\langle 1, n\rangle$, $\langle 0, n+1\rangle$, $\langle 1, n+1\rangle$, ...

2. В силу предложения 4.30 (5), $\omega \times_0 2 = \omega +_0 \omega$. Пусть $\langle R, A\rangle = \langle E_\omega, \omega\rangle$ и $\langle S, B\rangle = \langle E_2, 2\rangle$. Тогда $\omega \times 2$ может быть вполне упорядочено следующим образом (см. предложение 4.34): $\langle 0, 0\rangle$, $\langle 1, 0\rangle$, $\langle 2, 0\rangle$, ..., $\langle 0, 1\rangle$, $\langle 1, 1\rangle$, $\langle 2, 1\rangle$, ...

Предложение 4.35. *Для любого* α $\omega_\alpha \times \omega_\alpha \simeq \omega_\alpha$.

Доказательство. (Серпинский [1958].) Допустим, что утверждение неверно, и пусть α — наименьшее порядковое число, для которого $\neg(\omega_\alpha \times \omega_\alpha \simeq \omega_\alpha)$. Тогда для всякого $\beta < \omega_\alpha$ выполнено $\omega_\beta \times \omega_\beta \simeq \omega_\beta$. В силу предложения 4.32 (1), $0 <_0 \alpha$. Положим $P = \omega_\alpha \times \omega_\alpha$, и для любого $\beta <_0 \omega_\alpha$ $P_\beta = \hat{\gamma}\hat{\delta}(\gamma +_0 \delta = \beta)$. Покажем, что $P = \bigcup\limits_{\beta <_0 \omega_\alpha} P_\beta$. Если $\gamma +_0 \delta = \beta <_0 \omega_\alpha$, то $\gamma \leqslant_0 \beta <_0 \omega_\alpha$ и $\delta \leqslant_0 \beta <_0 \omega_\alpha$, и, следовательно, $\langle \gamma, \delta\rangle \in \omega_\alpha \times \omega_\alpha = P$. Итак, $\bigcup\limits_{\beta <_0 \omega_\alpha} P_\beta \subseteq P$. Для доказательства обратного включения $P \subseteq \bigcup\limits_{\beta <_0 \omega_\alpha} P_\beta$ достаточно показать, что если $\gamma <_0 \omega_\alpha$ и $\delta <_0 \omega_\alpha$, то $\gamma +_0 \delta <_0 \omega_\alpha$. Итак, пусть $\gamma <_0 \omega_\alpha$ и $\delta <_0 \omega_\alpha$. γ и δ равномощны соответственно некоторым начальным порядковым числам $\omega_\sigma \leqslant_0 \gamma$ и $\omega_\rho \leqslant_0 \delta$. Обозначим через ζ наибольшее из порядковых чисел σ и ρ. Так как $\gamma <_0 \omega_\alpha$ и $\delta <_0 \omega_\alpha$, то $\omega_\zeta <_0 \omega_\alpha$. Поэтому, в силу минимальности α, $\omega_\zeta \times \omega_\zeta \simeq \omega_\zeta$. Пусть $A = \gamma \times \{0\}$ и $B = \delta \times \{1\}$. В силу предложения 4.33, $A \cup B \simeq \gamma +_0 \delta$. Так как $\gamma \simeq \omega_\sigma$ и $\delta \simeq \omega_\rho$, то $A \simeq \omega_\sigma \times \{0\}$ и $B \simeq \omega_\rho \times \{1\}$. Отсюда, принимая во внимание, что $A \cap B = 0$, получаем $A \cup B \simeq (\omega_\sigma \times \{0\}) \cup (\omega_\rho \times \{1\})$. Однако, в силу предложения 4.32(2), $(\omega_\sigma \times \{0\}) \cup (\omega_\rho \times \{1\}) \preceq (\omega_\sigma \times \{0\}) \times (\omega_\rho \times \{1\}) \simeq \omega_\sigma \times \omega_\rho \preceq \omega_\zeta \times \omega_\zeta \simeq \omega_\zeta$, и потому $\gamma +_0 \delta \preceq \omega_\zeta <_0 \omega_\alpha$. Так как ω_α есть начальное порядковое число, то $\gamma +_0 \delta <_0 \omega_\alpha$. (Ибо в противном случае, т. е. если бы было $\omega_\alpha \leqslant_0 \gamma +_0 \delta$, мы имели бы $\omega_\alpha \preceq \omega_\zeta$ и $\omega_\zeta \preceq \omega_\alpha$ одновременно, что, по теореме Шрёдера — Бернштейна, влечет $\omega_\alpha = \omega_\zeta$, в противоречие с $\omega_\zeta <_0 \omega_\alpha$.) Таким образом, $P = \bigcup\limits_{\beta <_0 \omega_\alpha} P_\beta$. Рассмотрим P_β при $\beta <_0 \omega_\alpha$. На основании предложения 4.29 (6), для любого $\gamma \leqslant_0 \beta$ существует и притом единственное порядковое число δ такое, что $\gamma +_0 \delta = \beta$. Отсюда следует, что существует функция, подобно отображающая β' на множество P_β, упорядоченное по величине первых компонент γ входящих в него пар $\langle \gamma, \delta\rangle$. Определим следующее отношение R на P. Для любых $\gamma <_0 \omega_\alpha$,

$\delta <_0 \omega_\alpha$, $\mu <_0 \omega_\alpha$ и $\nu <_0 \omega_\alpha$ положим $\langle\langle \gamma, \delta\rangle, \langle \mu, \nu\rangle\rangle \in R$ тогда и только тогда, когда либо $\gamma +_0 \delta <_0 \mu +_0 \nu$, либо $\gamma +_0 \delta = \mu +_0 \nu \,\&\, \gamma <_0 \mu$. Тогда если $\beta_1 <_0 \beta_2 <_0 \omega_\alpha$, то пары из P_{β_1} предшествуют относительно R парам из P_{β_2}, а в пределах каждого P_β пары упорядочены относительно R по величине своих первых компонент. Легко видеть, что R вполне упорядочивает P. Так как $P = \omega_\alpha \times \omega_\alpha$, то теперь достаточно показать, что $\langle R, P\rangle$ подобно $\langle E_{\omega_\alpha}, \omega_\alpha\rangle$. В силу предложения 4.17, $\langle R, P\rangle$ подобно некоторой паре $\langle E_\xi, \xi\rangle$, где ξ — порядковое число. Отсюда следует, что $P \simeq \xi$. Допустим, что $\omega_\alpha <_0 \xi$. Пусть f есть функция, осуществляющая подобное отображение $\langle E_\xi, \xi\rangle$ на $\langle R, P\rangle$, и пусть $b = f\,'\,\omega_\alpha$. Тогда b есть упорядоченная пара $\langle \gamma, \delta\rangle$, где $\gamma <_0 \omega_\alpha$ и $\delta <_0 \omega_\alpha$, а $\omega_\alpha 1 f$, очевидно, является подобным отображением $\langle E_{\omega_\alpha}, \omega_\alpha\rangle$ на R-сегмент $Y = Seg_R(P, \langle \gamma, \delta\rangle)$ множества P, определенный парой $\langle \gamma, \delta\rangle$. Очевидно, $Y \simeq \omega_\alpha$. Пусть $\beta = \gamma +_0 \delta$ и $\langle \sigma, \rho\rangle \in Y$, тогда $\sigma +_0 \rho \leqslant_0 \gamma +_0 \delta = \beta$; следовательно, $\sigma \leqslant_0 \beta$ и $\rho \leqslant_0 \beta$. Поэтому $Y \subseteq \beta' \times \beta'$. Но $\beta' <_0 \omega_\alpha$. Следовательно, $\beta' \simeq \omega_\mu$, где $\mu <_0 \alpha$. На основании определения ω_α, $\omega_\mu \times \omega_\mu \simeq \omega_\mu$. Итак, мы получаем $\omega_\alpha \simeq Y \preceq \omega_\mu$, что находится в противоречии с $\omega_\mu \prec \omega_\alpha$. Следовательно, $\xi \leqslant_0 \omega_\alpha$. Поэтому $P \preceq \omega_\alpha$. Пусть теперь h есть функция, определенная на ω_α и такая, что $h\,'\,\beta = \langle \beta, 0\rangle$ для любого $\beta <_0 \omega_\alpha$. Очевидно, h является взаимно однозначным соответствием между β и подмножеством $\omega_\alpha \times \{0\}$ множества $\omega_\alpha \times \omega_\alpha$, и потому $\omega_\alpha \preceq P$. Но тогда, в силу теоремы Шрёдера — Бернштейна, $\omega_\alpha \simeq P$, что противоречит определению порядкового числа α. Следовательно, $\omega_\beta \times \omega_\beta \simeq \omega_\beta$ при любом β.

Следствие 4.36. *Если* $A \simeq \omega_\alpha$, $B \simeq \omega_\beta$, *а* γ — *наибольшее из порядковых чисел* α, β, *то* $A \times B \simeq \omega_\gamma$ и $A \cup B \simeq \omega_\gamma$. *В частности,* $\omega_\alpha \times \omega_\beta \simeq \omega_\gamma$.

Доказательство. На основании предложений 4.35 и 4.32(2), $\omega_\gamma \preceq A \cup B \preceq A \times B \simeq \omega_\alpha \times \omega_\beta \preceq \omega_\gamma \times \omega_\gamma \simeq \omega_\gamma$. Отсюда, по теореме Шрёдера — Бернштейна, следует $A \times B \simeq \omega_\gamma$ и $A \cup B \simeq \omega_\gamma$.

Мы здесь изложили лишь самые начала арифметики порядковых чисел. Дальнейшие сведения по этой теме можно найти у Серпинского [1958] и у Бахмана [1955].

§ 5. Аксиома выбора. Аксиома ограничения

Аксиома выбора является одним из самых знаменитых и наиболее оспариваемых утверждений теории множеств. Мы сформулируем эту аксиому в следующей теореме, говорящей о ее эквивалентности ряду других важных утверждений.

Предложение 4.37. *Следующие формулы эквивалентны*:

(1) Аксиома выбора (AC): *Для любого множества* x *существует функция* f *такая, что для всякого непустого подмножества* y *множества* x $f\,'\,y \in y$ (*такая функция называется* выбирающей функцией *для* x).

(2) Мультипликативная аксиома (*Mult*): *Для любого множества x непустых и попарно непересекающихся множеств, существует множество y* (называемое выбирающим множеством для x), *которое содержит в точности по одному элементу из каждого множества, являющегося элементом x.*

$$\forall u\,(u \in x \supset u \neq 0 \,\&\, \forall v\,(v \in x \,\&\, v \neq u \supset v \cap u = 0)) \supset$$
$$\supset \exists y \forall u\,(u \in x \supset \exists_1 w\,(w \in u \cap y)).$$

(3) Принцип вполне упорядочения (*W. O.*): *Всякое множество может быть вполне упорядочено.* $\forall x \exists y\,(y\ We\ x)$.

(4) Трихотомия (*Trich*): $\forall x \forall y\,(x \preceq y \vee y \preceq x)$.

(5) Лемма Цорна (*Zorn*): *Если в частично упорядоченном множестве x всякая цепь (т. е. всякое упорядоченное подмножество) имеет верхнюю грань, то в x существует максимальный элемент.*

$$\forall x \forall y\,((y\ Part\ x) \,\&\, \forall u\,(u \subseteq x \,\&\, y\ Tot\ u \supset \exists v\,(v \in x \,\&\, \forall w\,(w \in u \supset w =$$
$$= v \vee \langle w, v\rangle \in y))) \supset \exists v\,(v \in x \,\&\, \forall w\,(w \in x \supset \langle v, w\rangle \notin y))).$$

Доказательство. (1) $\vdash$ (*W. O.*) $\supset$ *Trich*. Пусть даны множества x и y. Согласно (*W. O.*), x и y могут быть вполне упорядочены. Поэтому, в силу предложения 4.17, существуют такие порядковые числа α и β, что $x \simeq \alpha$ и $y \simeq \beta$. Но так как $\alpha \preceq \beta$ или $\beta \preceq \alpha$, то либо $x \preceq y$, либо $y \preceq x$.

(2) $\vdash$ *Trich* $\supset$ (*W. O.*). Пусть дано множество x. Согласно теореме Хартогса, существует такое порядковое число α, которое не равномощно никакому подмножеству множества x. Тогда, в силу *Trich*, x равномощно некоторому подмножеству y порядкового числа α, и вполне упорядочение E_y множества y порождает некоторое вполне упорядочение множества x.

(3) $\vdash$ (*W. O.*) $\supset$ *Mult*. Пусть x есть некоторое множество непустых, попарно непересекающихся множеств. Согласно (*W. O.*), существует отношение R, вполне упорядочивающее множество $\bigcup(x)$. Следовательно, существует такая определенная на x функция f, что $f`u$ для любого $u \in x$ есть наименьший относительно R элемент u. (Заметим, что $u \subseteq \bigcup(x)$.)

(4) $\vdash$ *Mult* $\supset$ AC. Для любого множества x существует функция g такая, что если u есть непустое подмножество x, то $g`u = u \times \{u\}$. Пусть x_1 — область значений функции g. Легко видеть, что x_1 является множеством непустых попарно непересекающихся множеств. На основании *Mult*, для x_1 существует выбирающее множество y. Отсюда, если $0 \neq u$ и $u \subseteq x$, то $u \times \{u\} \in x_1$ и y содержит и притом единственный элемент $\langle v, u\rangle$ из $u \times \{u\}$. Функция $f`u = v$ является искомой выбирающей функцией для x.

(5) $\vdash$ AC $\supset$ *Zorn*. Пусть y частично упорядочивает непустое множество x таким образом, что всякая y-цепь в x имеет в x верхнюю грань. На основании AC, для x существует выбирающая функция f.

Рассмотрим произвольный элемент b множества x, и по трансфинитной индукции (предложение 4.13) определим функцию F такую, чтобы выполнялось $F`0 = b$ и $F`\alpha = f`u$ для любого α, где u есть множество всех таких верхних граней v множества $F``\alpha$ относительно упорядочения $y$, что $v \in x$ и $v \notin F``\alpha$. Пусть β есть наименьшее порядковое число, которому соответствует пустое множество верхних граней v множества $F``\beta$ относительно упорядочения $y$, принадлежащих $x$ и не принадлежащих $F``\beta$. (Порядковые числа, обладающие таким свойством, существуют; в противном случае функция F была бы взаимно однозначной с областью определения On и с некоторым подмножеством множества x в качестве области значений, откуда по аксиоме замещения R следовало бы, что On есть множество.) Пусть $g = \beta \upharpoonleft F$. Нетрудно видеть, что функция g взаимно однозначна и что если $\alpha <_0 \gamma <_0 \beta$, то $\langle g`\alpha, g`\gamma \rangle \in y$. Поэтому множество $g``\beta$ является $y$-цепью в $x$. Согласно условию, в $x$ существует верхняя грань $w$ множества $g``\beta$. Так как множество верхних граней множества $F``\beta$ $(= g``\beta)$, не содержащихся в $g``\beta$, пусто, то $w \in g``\beta$, и, следовательно, w является единственной верхней гранью множества $g``\beta$ (ибо всякое множество может содержать в себе не более одной своей верхней грани). Отсюда следует, что $w$ есть максимальный относительно упорядочения $y$ элемент множества $x$. (Действительно, если $\langle w, z \rangle \in y$ и $z \in x$, то $z$ должно быть верхней гранью $g``\beta$, что, очевидно, невозможно.)

(6) $\vdash Zorn \supset (W.\ O.)$. Пусть z есть множество, а X есть класс всех взаимно однозначных функций f таких, что $\mathscr{D}(f) \in On$ и $\mathscr{R}(f) \subseteq z$. Из теоремы Хартогса следует, что X есть множество. Очевидно также, что $0 \in X$. Отношение $\subset$ частично упорядочивает X. Каковы бы ни были две функции, принадлежащие одной и той же цепи в X, одна из них является продолжением другой. Поэтому для любой цепи в X объединение всех принадлежащих ей функций есть снова взаимно однозначная функция, принадлежащая той же цепи. Следовательно, на основании *Zorn*, в X имеется максимальный элемент g, представляющий собой взаимно однозначную функцию, определенную на некотором порядковом числе α и принимающую значения из z. Допустим, что $z - g``\alpha \neq 0$. Пусть $b \in z - g``\alpha$, и положим $f = g \cup \{\langle \alpha, b \rangle\}$. Тогда, очевидно, $f \in X$ и $g \subset f$, что противоречит максимальности g. Следовательно, $g``\alpha = z$, т. е. $\alpha \underset{g}{\simeq} z$. Посредством функции g отношение E_α, вполне упорядочивающее множество α, преобразуется в некоторое отношение, вполне упорядочивающее z.

Упражнения

1. Доказать, что следующие утверждения эквивалентны аксиоме выбора:

(a) Всякое множество равномощно некоторому порядковому числу.

(b) (Специальный случай леммы Цорна.) Если объединение всех элементов всякой непустой $\subset$-цепи в непустом множестве x является снова элементом x, то в x имеется максимальный относительно отношения $\subset$ элемент.

(c) (*Принцип максимальности* Хаусдорфа.) Если x — множество, то всякая $\subset$-цепь в x является подмножеством некоторой максимальной $\subset$-цепи в x.

(d) (Лемма Тайхмюллера — Тьюки.) Всякое множество конечного характера имеет максимальный относительно отношения $\subset$ элемент. (Непустое множество x называется множеством конечного характера, если (i) всякое конечное подмножество всякого элемента x есть также элемент x, и (ii) элементом x является всякое множество y, все конечные подмножества которого суть элементы x.)

(e) $\forall x\,(Rel\,(x) \supset \exists y\,(Fnc\,(y)\ \&\ \mathscr{D}\,(x) = \mathscr{D}\,(y)\ \&\ y \subseteq x))$.

2. Показать, что в NBG выводима следующая «конечная» аксиома выбора: для всякого конечного множества x непустых попарно непересекающихся множеств существует выбирающее множество y. (Указание. Пусть $x \simeq \alpha$, где $\alpha \in \omega$; далее — индукция по α.)

Предложение 4.38. *Следующие утверждения являются следствиями аксиомы выбора*:

(I) *Всякое бесконечное множество имеет счетное подмножество.*

(II) *Всякое бесконечное множество бесконечно по Дедекинду.*

(III) *Если x есть счетное множество, элементами которого являются счетные множества, то множество $\bigcup(x)$ счетно.*

Доказательство. (I) Примем AC. Пусть x — бесконечное множество. Согласно упражнению 1(a) на стр. 219, x равномощно некоторому порядковому числу α. Так как x бесконечно, то бесконечно и α. Следовательно, $\omega \leqslant_0 \alpha$, и потому ω равномощно некоторому подмножеству x.

(II) Следует из (I) и упражнения 13(c) на стр. 206.

(III) Пусть x — счетное множество счетных множеств. Рассмотрим функцию f, которая каждому $u \in x$ сопоставляет множество всех взаимно однозначных отображений u на ω. Пусть $z = \bigcup(\mathscr{R}(f))$. В силу аксиомы выбора (примененной к z), существует функция g такая, что $g\,'v \in v$ для каждого непустого $v \subseteq z$. В частности, если $u \in x$, то $g\,'(f\,'u)$ представляет собой некоторое взаимно однозначное соответствие между u и ω. Пусть теперь h — какое-нибудь взаимно однозначное соответствие между ω и x. Определим функцию F на $\bigcup(x)$ следующим образом. Пусть $y \in \bigcup(x)$ и n есть наименьший элемент ω, для которого $y \in h\,'n$. Очевидно, $h\,'n \in x$, и, следовательно, $g\,'(f\,'(h\,'n))$ является взаимно однозначным соответствием между $h\,'n$ и ω. Положим теперь $F\,'y = \langle n, (g\,'(f\,'(h\,'n)))\,'y\rangle$. Нетрудно видеть, что F есть взаимно однозначная функция с областью определения $\bigcup(x)$ и областью значений, являющейся подмножеством множества $\omega \times \omega$. Таким образом, $\bigcup(x) \preceq \omega \times \omega$. Но так как $\omega \times \omega \simeq \omega$, то $\bigcup(x) \preceq \omega$. Если же $v \in x$, то $v \subseteq \bigcup(x)$ и $v \simeq \omega$; следовательно, $\omega \preceq \bigcup(x)$. По теореме Шрёдера—Бернштейна, заключаем, что $\bigcup(x) \simeq \omega$.

Упражнения

1. Для каждого множества x определим декартово произведение $\prod\limits_{u \in x} u$ как множество всех функций f с областью определения x и таких, что $f\,'u \in u$ при любом $u \in x$. Доказать, что аксиома выбора эквивалентна утверждению о том,

что для каждого множества x непустых множеств декартово произведение $\prod_{u \in x} u$ непусто.

2. Опираясь на аксиому выбора, показать, что всякое частичное упорядочение произвольного множества x погружается в некоторое полное упорядочение того же множества x.

3. Доказать, что следующее предложение следует из аксиомы выбора: каковы бы ни были порядковое число α и множество x, если $x \preceq \omega_\alpha$ и $\forall u\,(u \in x \supset u \preceq \omega_\alpha)$, то $\bigcup(x) \preceq \omega_\alpha$. (Указание. Доказательство аналогично доказательству предложения 4.38 (III).)

По-видимому, более сильной формой аксиомы выбора является следующая формула (UCF): $\exists X\,(Fnc\,(X) \& \forall u\,(u \neq 0 \supset X`u \in u))$. (UCF утверждает существование *универсальной выбирающей функции*, т. е. такой функции, которая каждому множеству сопоставляет некоторый его элемент.)

UCF очевидным образом влечет AC, однако неизвестно, верно ли обратное, т. е. следует ли UCF из AC.

Если мы примем аксиому выбора AC, то теория кардинальных чисел упростится, так как AC влечет, что всякое множество x равномощно некоторому порядковому числу и, следовательно, некоторому начальному порядковому числу ω_α. Этим начальным порядковым числом ω_α мы будем обозначать *кардинальное число* (или *мощность*) множества x. Таким образом, мы отождествляем кардинальные числа с начальными порядковыми числами. В соответствии с общепринятой системой обозначений, мы будем вместо ω_α писать $\aleph_\alpha$. Предложения 4.35—4.36 устанавливают некоторые из основных свойств сложения и умножения кардинальных чисел.

Положение аксиомы выбора стало за последние годы менее спорным. Большинству математиков она представляется утверждением, совершенно правдоподобным. Кроме того, аксиома выбора имеет столь многочисленные и важные применения практически во всех отраслях математики, что отказ от нее выглядел бы как преднамеренная подножка работающему математику. Ниже в этом же параграфе мы обсудим вопрос о совместимости аксиомы выбора с остальными аксиомами теории множеств и ее независимости от них.

Другим предложением, которое было выдвинуто в качестве одного из основных принципов теории множеств, является следующая, так называемая *аксиома ограничения* (аксиома D): $\forall X\,(X \neq 0 \supset \exists y\,(y \in X \& \& y \cap X = 0))$ (т. е. всякий непустой класс X содержит элемент, не имеющий с X общих элементов).

Предложение 4.39. Аксиомой фундирования *называется формула* $\neg \exists x\,(Fnc\,(x) \& \mathscr{D}\,(x) = \omega \& \forall u\,(u \in \omega \supset x`(u') \in x`u))$ (*т. е. не существует бесконечной убывающей* $\in$*-последовательности* $x_1 \ni x_2 \ni \ldots$).

(1) *Аксиома ограничения влечет аксиому фундирования.*

(2) *Если принять аксиому выбора, то из аксиомы фундирования следует аксиома ограничения.*

(3) *Из аксиомы ограничения следует, что не существует никакого конечного* $\in$*-цикла, т. е. что невозможна функция* f,

определенная на каком-нибудь отличном от нуля конечном порядковом числе α' и такая, что $f'0 \in f'1 \in \ldots \in f'\alpha \in f'0$; в частности, отсюда следует, что не существует такого множества y, чтобы $y \in y$.

Доказательство. (1) Допустим $Fnc(x) \& \mathscr{D}(x) = \omega \& \forall u (u \in \in \omega \supset x'(u') \in x'u))$. Пусть $z = x \text{“} \omega$. По аксиоме ограничения, в z существует такой элемент y, что $y \cap z = 0$. Так как $y \in z$, то $y = f'\alpha$ для некоторого конечного порядкового числа α. Тогда $f'(\alpha') \in y \cap z$, чего, однако, не может быть из-за $y \cap z = 0$.

(2) Определим сначала для произвольного множества u *транзитивное замыкание* u. Пусть g — функция, следующим образом определенная по индукции на ω: $g'0 = \{u\}$, $g'(\alpha') = \bigcup(g'\alpha)$ для любого $\alpha \in \omega$. Таким образом, $g'1 = u$, $g'2 = \bigcup(u)$ и т. д. Назовем транзитивным замыканием множества u множество $TC(u) = \bigcup(g \text{“} \omega)$. Для любого u $TC(u)$ транзитивно, т. е. $\forall v (v \in TC(u) \supset v \subseteq TC(u))$. Примем теперь аксиому выбора и аксиому фундирования и допустим, что существует такой класс $X \neq 0$, что ни один его элемент y не удовлетворяет условию $y \cap X = 0$. Пусть b есть некоторый элемент класса X. Тогда $b \cap X \neq 0$. Пусть, далее, $c = TC(b) \cap X$ и, согласно аксиоме выбора, h — некоторая выбирающая функция для c. Зададим на ω функцию f условиями $f'0 = b$ и $f'(\alpha') = h'((f'\alpha) \cap X)$ для любого $\alpha \in \omega$. Теперь легко видеть, что $f'(\alpha') = f'\alpha$ при любом $\alpha \in \omega$, и мы пришли к противоречию с аксиомой фундирования. (Приведенное доказательство по существу сводится к следующему: выбираем сначала какой-нибудь элемент b из X, затем с помощью функции h выбираем некоторый элемент $f'1$ из $b \cap X$, затем, благодаря тому, что общая часть $f'1$ и $b \cap X$ непуста, выбираем некоторый элемент $f'2$ из $f'1 \cap X$ и т. д.)

(3) Допустим, что имеется некоторый конечный $\in$-цикл: $f'0 \in \in f'1 \in \ldots \in f'n \in f'0$. Пусть X есть область значений функции f, т. е. $X = \{f'0, f'1, \ldots, f'n\}$. Из аксиомы ограничения следует, что $f'i \cap X = 0$ при некотором i, чего не может быть, ибо всякий элемент из X содержит в себе некоторый элемент, являющийся одновременно и элементом X.

Замечание. Применение аксиомы выбора при выводе аксиомы ограничения из аксиомы фундирования является необходимым. Можно показать (см. Мендельсон [1958]), что если теория NBG непротиворечива, то, добавив к ней в качестве единственной новой аксиомы аксиому фундирования, мы получим такое расширение теории NBG, в котором аксиома ограничения невыводима.

Следующая функция Ψ, определяемая по трансфинитной индукции, была впервые рассмотрена фон Нейманом:

$$\Psi'0 = 0,$$

$$\Psi'(\alpha') = \mathscr{P}(\Psi'\alpha),$$

$$Lim(\lambda) \supset \Psi'\lambda = \bigcup_{\beta <_0 \lambda} (\Psi'\beta).$$

Пусть $H = \bigcup(\Psi``On)$, $H_\beta = \bigcup(\Psi``\beta)$ и ρ есть такая функция, определенная на H, что $\rho`x$ для любого $x \in H$ есть наименьшее порядковое число $\alpha$, для которого $x \in H`\alpha$. Назовем $\rho`x$ *рангом* $x$. Заметим, что $\rho`x$ всегда является порядковым числом первого рода.

Упражнения

1. $\vdash On \subseteq H$. (Указание. Применить трансфинитную индукцию.)
2. $\vdash \forall\alpha(\rho`\alpha = \alpha')$. (Указание. Применить трансфинитную индукцию.)
3. $\vdash Trans(H)$, т. е. $u \in H \supset u \subseteq H$.
4. $\vdash u \in H \,\&\, v \in H \,\&\, u \in v \supset \rho`u <_0 \rho`v$.
5. $\vdash u \subseteq H \supset u \in H$. (Указание. Пусть λ — наименьшее порядковое число, большее чем ранг любого элемента множества u. Тогда $u \subseteq \Psi`\lambda$ и, следовательно, $u \in \mathscr{P}(\Psi`\lambda) = \Psi(\lambda')$.)

Предложение 4.40. *Аксиома ограничения эквивалентна утверждению, что $V = H$, т. е. что всякое множество является элементом H.*

Доказательство. (1) Допустим, что $V = H$. Пусть $X \neq 0$, α — наименьший из рангов $\rho`x$, где $x \in X$, и $b$ — какой-нибудь из элементов $X$, ранг которых равен $\alpha$. Тогда $b \cap X = 0$, ибо в противном случае из $u \in b \cap X$ следовало бы, на основании предыдущего упражнения 4, что $\rho`u <_0 \rho`b = \alpha$, чего не может быть, согласно определению α.

(2) Примем аксиому ограничения и допустим, что $V - H \neq 0$. Согласно аксиоме ограничения, существует такое множество y, что $y \in V - H \,\&\, y \cap (V - H) = 0$. Легко видеть, что $y \subseteq H$. Отсюда по предыдущему упражнению 5, заключаем, что $y \in H$. Мы пришли к противоречию с $y \in V - H$.

Упражнения

1. Показать, что аксиома ограничения эквивалентна следующему своему частному случаю:

$$x \neq 0 \supset \exists y\,(y \in x \,\&\, y \cap x = 0).$$

2. Предположив аксиому ограничения, показать, что $x \in On$ эквивалентно утверждению $Trans(x) \,\&\, E\,Con\,x$, т. е. формуле $\forall u(u \in x \supset u \subseteq x) \,\&\, \forall u \forall v\,(u \in x \,\&\, v \in x \,\&\, u \neq v \supset u \in v \,\&\, v \in u)$. Таким образом, с помощью аксиомы ограничения определение понятия порядкового числа может быть значительно упрощено.

Предложение 4.40 делает весьма заманчивой идею присоединения аксиомы ограничения к NBG в качестве новой аксиомы. В самом деле, ведь равенство $V = H$ утверждает, что всякое множество может быть получено, исходя из 0, посредством применения операций образования множества всех подмножеств и объединения всех элементов данного множества некоторое трансфинитное число раз. Понятно поэтому, что, получив в свое распоряжение такое утверждение, мы смогли бы прояснить наши довольно смутные представления о множествах. Кроме того, как мы только что видели в упражнении 2, аксиома ограничения позволяет

упростить определение понятия порядкового числа. Наконец, и теорию кардинальных чисел можно строить с помощью аксиомы ограничения, определяя кардинальное число всякого множества x как множество всех тех y, которые имеют наименьший ранг в классе всевозможных u, удовлетворяющих условию $x \simeq u$. (В основу теории кардинальных чисел кладется при этом требование существования такой функции *Card*, областью определения которой был бы класс V и которая удовлетворяла бы условию $Card\,'x = Card\,'y \equiv x \simeq y$.) Математики, однако, не единодушны в вопросе о том, имеются ли достаточные основания для того, чтобы допустить аксиому ограничения в качестве новой аксиомы. Дело в том, что хотя аксиома ограничения и обладает большой упрощающей силой, однако по своему непосредственному правдоподобию она уступает даже аксиоме выбора, не говоря уже о том, что она до сих пор еще не нашла себе математических применений.

Введенный выше класс H в следующем смысле определяет *внутреннюю модель* теории NBG. Для всякой формулы $\mathscr{A}$ (записанной без сокращенных обозначений) со свободными переменными $Y_1, \ldots, Y_n$ обозначим через $Rel_H(\mathscr{A})$ формулу, полученную из формулы $\mathscr{A}$ заменой в ней всякой подформулы $\forall X \mathscr{B}(X)$ (начиная с самых внутренних) на $\forall X (X \subseteq H \subset \mathscr{B}(X))$ и добавлением к результату таких замен посылки $(Y_1 \subseteq H \& \ldots \& Y_n \subseteq H) \supset$. Иными словами, образуя $Rel_H(X)$, мы интерпретируем «класс» как «подкласс класса H». Тогда оказывается, что для любой теоремы $\mathscr{A}$ теории NBG формула $Rel_H(\mathscr{A})$ тоже является теоремой теории NBG.

Упражнение

Доказать, что для всякой аксиомы $\mathscr{A}$ теории NBG формула $Rel_H(\mathscr{A})$ есть теорема в NBG.

Отметим, что $Rel_H(\forall x \mathscr{B})$ эквивалентно $\forall x (x \in H \supset \mathscr{B}^{\#})$, где $\mathscr{B}^{\#}$ есть $Rel_H(\mathscr{B})$. В частности, $Rel_H(M(X))$ есть $\exists Y (Y \subseteq H \& X \in Y)$, что эквивалентно $X \in H$. Таким образом, «множествами» внутренней модели являются элементы H. При семантическом подходе мы должны заметить лишь, что, какова бы ни была модель N теории NBG (в обычном смысле слова «модель»), объекты X модели N, которые удовлетворяют условию $X \subseteq H$, также образуют модель теории NBG. Можно, кроме того, показать, что во внутренней модели справедлива и аксиома ограничения. Именно в этом и состоит первая часть предложения 4.40. Непосредственным следствием этого факта является совместимость аксиомы ограничения, т. е. если теория NBG непротиворечива, то непротиворечиво и расширение этой теории, получаемое за счет добавления аксиомы ограничения в качестве единственной новой аксиомы. С помощью соответствующей модели можно доказать также и независимость аксиомы ограничения от аксиом теории NBG (см. Бернайс [1954], часть VII); правда, модель эта оказывается уже более сложной, чем та, с помощью которой только что была доказана совместимость. Таким образом, по

отношению к теории NBG аксиома ограничения оказывается одновременно совместимой и независимой: как она, так и ее отрицание могут быть без противоречий присоединены к теории NBG, если, разумеется, последняя сама непротиворечива. (В сущности теми же доказательствами можно воспользоваться и для установления фактов независимости и совместимости аксиомы ограничения по отношению к теории NBG + (AC).)

Аксиома выбора также независима и совместима по отношению к теории NBG. Сначала Гёдель [1940] показал, что если теория NBG непротиворечива, то непротиворечива и теория NBG + (AC) + (аксиома ограничения) + (GCH), где (GCH) обозначает так называемую *обобщенную континуум-гипотезу*: $\forall x \forall y \neg (Inf(x) \& x \prec y \& y \prec \mathcal{P}(x))$. (На самом деле, это утверждение страдает некоторым излишеством, ибо Серпинский [1947] и Шпеккер [1954] доказали, что $\vdash (GCH) \supset \supset (AC)$.) С другой стороны, Мендельсон [1958] доказал, что если теория NBG непротиворечива, то аксиома выбора невыводима даже в расширении этой теории, получающемся в результате добавления к ней аксиомы фундирования в качестве новой аксиомы. Таким образом, если теория NBG непротиворечива, то к ней без противоречия можно присоединить как саму аксиому выбора, так и ее отрицание. (Однако вопрос о независимости аксиомы выбора от аксиом теории NBG + (аксиома ограничения) остается пока открытым *).)

Упражнения

1. Показать, что в модели H_α, «классами» которой являются подклассы H_α, все аксиомы теории NBG (кроме, быть может, аксиомы бесконечности и аксиомы замещения) выполнены тогда и только тогда, когда α есть порядковое число второго рода (т. е. когда имеет место $Lim(\alpha)$). Доказать также, что H_α удовлетворяет аксиоме бесконечности тогда и только тогда, когда $\omega <_0 \alpha$.

2. Показать, что аксиома бесконечности невыводима из остальных аксиом теории NBG, если последние образуют непротиворечивую систему аксиом. (Указание. Рассмотреть модель H_ω, «классами» которой являются подмножества H_ω, и доказать, что аксиома бесконечности в этой модели не выполнена, а остальные аксиомы NBG выполнены.)

---

*) По существу этот вопрос вместе с таким же вопросом для обобщенной континуум-гипотезы перестал быть открытым уже вскоре после того, как была написана эта книга, так как на теорию NBG + (аксиома ограничения) может быть перенесен результат П. Дж. Коэна [1963—1964] о независимости аксиомы выбора и обобщенной континуум-гипотезы для системы аксиом теории множеств Цермело - Френкеля ZF. Теория ZF получается из описываемой ниже на стр. 227 теории ZSF добавлением к ней аксиомы ограничения. Коэн доказал, что если теория ZF непротиворечива, то в ней невыводима аксиома выбора, а обобщенная континуум-гипотеза невыводима в теории ZF + (аксиома выбора). Изложение этих результатов, а заодно и прежних результатов Гёделя о совместимости аксиомы выбора и обобщенной континуум-гипотезы (применительно к ZF) можно найти также в книге Коэна [1966], переведенной недавно на русский язык. Здесь необходимо также указать на цикл статей Вопенки [1965], [1966], в которых отличными от коэновских методами доказывается, между прочим, и независимость обобщенной континуум-гипотезы (для системы Гёделя—Бернайса с аксиомой выбора). (*Прим. перев.*)

3. Показать, что аксиома замещения R невыводима из аксиом T, P, N, B1—B7, U, W, S, если эти последние совместимы. (Указание. Показать, что $H_{\omega+_0\omega}$ является моделью для аксиом T, P, N, B1—B7, U, W, S, но не для аксиомы R.)

4. Порядковое число α называется *недостижимым*, если H_α является моделью теории NBG. Поскольку NBG имеет лишь конечное множество собственных аксиом, утверждение, что α есть недостижимое порядковое число, может быть выражено как конъюнкция релятивизированных посредством H_α собственных аксиом NBG. Однако утверждение существования недостижимых порядковых чисел недоказуемо в теории NBG, если последняя непротиворечива. То же самое верно для расширения этой теории с помощью аксиомы выбора и обобщенной континуум-гипотезы. (См. Шепердсон [1951—1953], Монтегю и Воот [1959], а также, в этой связи, Бернайс [1961] и Леви [1960].) В свое время была установлена связь недостижимых порядковых чисел с некоторыми проблемами теории меры и алгебры (см. Улам [1930], Зиман [1955], Эрдёш и Тарский [1961]). Вопрос о непротиворечивости расширения теории NBG добавлением аксиомы, утверждающей существование недостижимых порядковых чисел, остается пока открытым.

5. Функция w называется *α-последовательностью*, если ее область определения совпадает с α. Если к тому же область значений функции w состоит из порядковых чисел, то назовем такую функцию *α-последовательностью порядковых чисел*. Наконец, если из $\beta <_0 \gamma <_0 \alpha$ всегда следует $w(\beta) <_0 w(\gamma)$, то будем говорить, что w есть *возрастающая α-последовательность порядковых чисел*. В силу предложения 4.11, если w есть возрастающая α-последовательность порядковых чисел, то $\mathbf{U}(w \text{ “ } \alpha)$ есть наименьшая верхняя грань области значений w. Порядковое число δ называется *регулярным*, если для любого $\alpha <_0 \delta$ всякая возрастающая α-последовательность порядковых чисел w, значения которой меньше δ, удовлетворяет неравенству $\mathbf{U}(w \text{ “ } \alpha) +_0 1 <_0 \delta$. Порядковое число, не являющееся регулярным, называется *сингулярным*.

(i) Какие конечные порядковые числа являются регулярными?

(ii) Показать, что ω_0 регулярно и ω_ω сингулярно.

(iii) Доказать, что всякое регулярное порядковое число является начальным.

(iv) С помощью аксиомы выбора доказать, что всякое порядковое число вида $\omega_{\gamma+_01}$ регулярно.

(v) Доказать, что если *Lim* (α) и порядковое число ω_α регулярно, то $\omega_\alpha = \alpha$. (Если *Lim* (α), то регулярное порядковое число ω_α называют *слабо недостижимым*.)

(vi) Показать, что если для ω_α из $\gamma <_0 \omega_\alpha$ следует $\mathcal{P}(\gamma) \prec \omega_\alpha$, то *Lim* (α). Обратное утверждение следует из обобщенной континуум-гипотезы. Если $0 <_0 \alpha$, то регулярное порядковое число ω_α, для которого $\gamma <_0 \omega_\alpha$ влечет $\mathcal{P}(\gamma) \prec \omega_\alpha$, называется *сильно недостижимым*. Всякое сильно недостижимое порядковое число является слабо недостижимым, а в предположении обобщенной континуум-гипотезы верно и обратное утверждение.

(vii) (Шепердсон [1951—1953], Монтегю и Воот [1959].)
(a) Если порядковое число γ недостижимо (т. е. если H_γ является моделью для NBG), то оно слабо недостижимо.

[D] (b) В теории NBG + (AC) всякое порядковое число недостижимо тогда и только тогда, когда оно сильно недостижимо.

(c) Если теория NBG непротиворечива, то в теории NBG + (AC) + + (GCH) невозможно доказать существование слабо недостижимых порядковых чисел.

Мы выбрали для аксиоматического построения теории множеств теорию NBG потому, что она является, возможно, самой простой и наиболее удобной для работающего математика. Конечно, имеется много других вариантов аксиоматической теории множеств.

(1) Заменим (усилив тем самым теорию NBG) аксиомы B1—B7 одной схемой аксиом: $\exists X \forall y_1 \ldots \forall y_n (\langle y_1, \ldots, y_n \rangle \in X \equiv \varphi(y_1, \ldots, y_n))$, где φ — произвольная, не обязательно предикативная, формула теории NBG. Полученная таким образом новая теория NBG^+ является расширением теории NBG. Мостовский [1951a] показал, что NBG^+ является собственным расширением теории NBG, если эта последняя непротиворечива. Теория NBG^+ проще и сильнее теории NBG; но именно сила этой теории делает более рискованными надежды на ее непротиворечивость. Кроме того, представляется правдоподобным, что на теорию NBG^+ уже не распространяется доказательство Гёделя [1940] об относительной непротиворечивости аксиомы выбора.

(2) Система ZSF Цермело — Сколема — Френкеля является по существу частью теории NBG, трактующей только о множествах. В качестве переменных в ZSF мы используем $x_1, x_2, \ldots$ Единственным предикатом в этой теории является двуместный предикат $\in$. Аксиомами ZSF служат аксиомы T (объемности), P (пары), N (пустого множества), U (объединения), W (множества всех подмножеств), I (бесконечности) и, кроме того, имеется еще схема аксиом, соответствующая аксиоме замещения R: для всякой формулы $\varphi(u, v)$ аксиомой является формула

$$(\forall v \forall w \forall u (\varphi(v, u) \& \varphi(v, w) \supset u = w)) \supset$$
$$\supset \exists y \forall u (u \in y \equiv \exists v (v \in x \& \varphi(v, u))).$$

Всякая формула теории ZSF может рассматриваться как некоторая формула теории NBG, в которой переменные теории ZSF играют роль ограниченных множествами переменных теории NBG. Доказано (Новак-Гал [1951], Россер и Ван Хао [1950], Шёнфильд [1954]), что для любой замкнутой формулы $\mathscr{A}$ теории ZSF, если $\vdash_{NBG} \mathscr{A}$, то $\vdash_{ZSF} \mathscr{A}$; а потому теория ZSF непротиворечива в том и только в том случае, когда непротиворечива теория NBG. Подробнее о построении теории ZSF см. Саппс [1960].

Обзор различных аксиоматических систем теории множеств можно найти у Френкеля и Бар-Хиллела [1958] и у Вана Хао и Мак Нотона [1953]. Мы отсылаем также читателя по вопросам, касающимся более или менее подробного изложения теории типов, к Чёрчу [1940] и Куайну [1938]; системы New Foundations (NF) Куайна — к Россеру [1953] и Шпеккеру [1953] (где доказано, что сильная аксиома выбора опровержима в NF) и системы ML Куайна — к Куайну [1951].

Глава 5

Эффективная вычислимость

§ 1. Нормальные алгорифмы Маркова

Обычно функция $f(x_1, \ldots, x_n)$ мыслится нами как *эффективно вычислимая*, если имеется какая-нибудь механическая процедура, следуя которой, можно найти значение $f(k_1, \ldots, k_n)$ этой функции всякий раз, как только даны значения $k_1, \ldots, k_n$ аргументов. Выражение «механическая процедура», разумеется, крайне неточно, но во всяком случае мы под этим понимаем некий процесс, не требующий для своего осуществления никакой изобретательности. Достаточно прозрачным тому примером может служить операция сложения двух целых чисел, записанных в десятичной системе. Можно также указать на хорошо известный алгорифм Евклида для нахождения наибольшего общего делителя двух целых чисел. В этих двух примерах представляется интуитивно ясным, что данные функции эффективно вычислимы. И так обстоит дело всякий раз, когда эффективная процедура уже найдена. Однако все чаще и чаще мы сталкиваемся в математике с задачей, состоящей в том, чтобы доказать, что не существует эффективно вычислимой функции того или иного рода или что не существует никакой эффективной процедуры для решения какого-нибудь широкого класса проблем. Поясним сказанное еще таким примером. Хорошо известен эффективный способ узнавать, имеет ли целые корни данный произвольный многочлен с целыми коэффициентами, зависящий от одной переменной. С другой стороны, до сих пор еще остается нерешенной так называемая Десятая Проблема Гильберта, т. е. не решен вопрос о существовании эффективной процедуры, следуя которой, можно было бы для любого многочлена с целыми коэффициентами, зависящего от произвольного числа переменных, ответить на вопрос, имеет ли этот многочлен целые корни *). Если мы беремся доказывать, что та или иная функция не является эффективно вычислимой, то мы прежде должны сформулировать точное математическое определение понятия эффективной вычислимости. Совершенно аналогичная ситуация сложилась в свое время в математике, когда назрела необходимость уточнения таких понятий, как непрерывность, кривая, поверхность, площадь и т. п.

---

*) Эта проблема была решена впервые Ю. В. Матиясевичем [1970] и несколько позже Г. В. Чудновским [1970]. (*Прим. ред.*)

Всякая частная проблема из какого-нибудь общего класса проблем может быть сформулирована в виде некоторого выражения подходящего языка. Всякое выражение того или иного языка в свою очередь можно рассматривать как последовательность символов этого языка при условии, что пустое место, оставляемое обычно для разделения слов, воспринимается как равноправный символ того же языка. Мы будет называть *алфавитом* всякое непустое конечное множество символов, а сами символы алфавита будем называть *буквами.* В естественных языках используется лишь конечное число букв. Равным образом и для наших целей достаточно будет ограничиться рассмотрением только таких алфавитов. (Впрочем, все, что можно записать в бесконечном алфавите $a_1, a_2, \ldots$, можно воспроизвести и в алфавите $\{b, c\}$, содержащем лишь две буквы. Для этого достаточно условиться считать, что последовательность $\underbrace{bcc \ldots ccb}_{n \text{ раз}}$ изображает букву a_n.) Для единообразия мы будем, как правило, предполагать, что буквы всех алфавитов берутся из одной и той же счетной последовательности букв $\mathcal{S}_0, \mathcal{S}_1, \ldots$, хотя иногда в целях удобства будем использовать и другие буквы.

Словом в алфавите A называется всякая конечная последовательность букв алфавита A. Пустая последовательность букв называется *пустым словом* и обозначается через Λ. Если P обозначает слово $\mathcal{S}_{j_1} \ldots \mathcal{S}_{j_k}$ и Q обозначает слово $\mathcal{S}_{r_1}, \ldots, \mathcal{S}_{r_m}$, то пусть PQ обозначает *соединение* $\mathcal{S}_{j_1} \ldots \mathcal{S}_{j_k}\mathcal{S}_{r_1} \ldots \mathcal{S}_{r_m}$ этих двух слов. В частности, $P\Lambda = \Lambda P = P$. Кроме того, $(P_1P_2)P_3 = P_1(P_2P_3)$.

Алфавит A называется *расширением* алфавита B, если $B \subseteq A$. Если алфавит A есть расширение алфавита B, то всякое слово в алфавите B есть также слово и в алфавите A. *Алгорифмом в алфавите* A называется эффективно вычислимая функция, областью определения которой служит какое-нибудь подмножество множества всех слов в алфавите A и значениями которой являются также слова в алфавите A. Пусть P есть слово в алфавите A; говорят, что *алгорифм* $\mathfrak{A}$ *применим* к слову P, если P содержится в области определения $\mathfrak{A}$. Если алфавит B является расширением алфавита A, то всякий алгорифм в алфавите B называется *алгорифмом над алфавитом* A. Разумеется, в таком виде понятие алгорифма столь же туманно, как и понятие эффективно вычислимой функции.

Большинство известных алгорифмов можно разбить на некоторые простейшие шаги. Исходя из этого наблюдения и следуя А. А. Маркову [1954], в качестве элементарной операции, на базе которой будут строиться алгорифмы, мы выделим подстановку одного слова вместо другого. Если P и Q — слова в алфавите A, то выражение $P \to Q$ и $P \to \cdot Q$ будем называть *формулами подстановки* в алфавите A. При этом предполагается, что стрелка $\to$ и точка $\cdot$ не являются буквами алфавита A. Заметим, что здесь каждое из слов P и Q может быть пустым словом. Формула подстановки $P \to Q$ называется

простой. Формула подстановки $P \to \cdot Q$ называется *заключительной*. Пусть $P \to (\cdot) Q$ обозначает одну из формул подстановки $P \to Q$ или $P \to \cdot Q$. Конечный список формул подстановки в алфавите A

$$\begin{cases} P_1 \to (\cdot)\, Q_1 \\ P_2 \to (\cdot)\, Q_2 \\ \vdots \qquad\quad \vdots \\ P_r \to (\cdot)\, Q_r \end{cases}$$

называется *схемой алгорифма* и порождает следующий алгорифм в алфавите A. Условимся предварительно говорить, что слово T *входит* в слово Q, если существуют такие (возможно пустые) слова U, V, что $Q = UTV$. Пусть теперь дано некоторое слово P в алфавите A. Представляются две возможности: (1) Ни одно из слов $P_1, \ldots, P_r$ не входит в слово P. Этот факт мы будем коротко записывать так: $\mathfrak{A} : P \sqsupset$. (2) Среди слов $P_1, \ldots, P_r$ существуют такие, которые входят в P. Пусть m — наименьшее целое число такое, что $1 \leqslant m \leqslant r$ и P_m входит в P, и R — слово, которое получается, если самое левое вхождение слова P_m в слово P заменить словом Q_m. Тот факт, что P и R находятся в описанном отношении, коротко запишем в виде

(a) $$\mathfrak{A} : P \vdash R,$$

если формула подстановки $P_m \to (\cdot)\, Q_m$ — простая (и тогда мы скажем, что алгорифм $\mathfrak{A}$ просто переводит слово P в слово R), или в виде

(b) $$\mathfrak{A} : P \vdash \cdot R,$$

если формула подстановки $P_m \to (\cdot)\, Q_m$ — заключительная (и тогда мы скажем, что алгорифм $\mathfrak{A}$ заключительно переводит слово P в слово R). Пусть, далее, $\mathfrak{A} : P \models R$ означает, что существует такая последовательность $R_0, R_1, \ldots, R_k$ слов в алфавите A, что $P = R_0$, $R = R_k$, $\mathfrak{A} : R_j \vdash R_{j+1}$ для $j = 0, 1, \ldots, k-2$ и либо $\mathfrak{A} : R_{k-1} \vdash R_k$, либо $\mathfrak{A} : R_{k-1} \vdash \cdot R_k$ (в этом последнем случае вместо $\mathfrak{A} : P \models R$ мы будем писать $\mathfrak{A}\ I \models \cdot R$). Мы полагаем теперь $\mathfrak{A}(P) = R$ тогда и только тогда, когда либо $\mathfrak{A} : P \models R$, либо $\mathfrak{A} : P \models R$ и $\mathfrak{A} : R \sqsupset$. Алгорифм, определенный таким образом, называется *нормальным алгорифмом* (или *алгорифмом Маркова*) *в алфавите* A.

Работа алгорифма $\mathfrak{A}$ может быть описана следующим образом. Пусть дано слово P в алфавите A. Находим первую в схеме алгорифма $\mathfrak{A}$ формулу подстановки $P_m \to (\cdot)\, Q_m$ такую, что P_m входит в P. Совершаем подстановку слова Q_m вместо самого левого вхождения слова P_m в слово P. Пусть R_1 — результат такой подстановки. Если $P_m \to (\cdot)\, Q_m$ — заключительная формула подстановки, то работа алгорифма заканчивается и его значением является R_1. Если формула подстановки $P_m \to (\cdot)\, Q_m$ простая, то применим к R_1 тот же поиск, который был только что применен к P, и так далее. Если мы в конце концов получим такое слово R_i, что $\mathfrak{A} : R_i \sqsupset$, т. е. ни одно из слов

$P_1, \ldots, P_r$ не входит в R_i, то работа алгорифма заканчивается и R_i будет его значением. При этом возможно, что описанный процесс никогда не закончится. В таком случае мы говорим, что алгорифм $\mathfrak{A}$ неприменим к слову P.

В нашем изложении теории нормальных алгорифмов мы следуем А. А. Маркову [1954].

Примеры. 1. Пусть А есть алфавит $\{b, c\}$. Рассмотрим схему

$$\begin{cases} b \to \cdot \Lambda \\ c \to c \end{cases}$$

Определяемый этой схемой нормальный алгорифм $\mathfrak{A}$ перерабатывает всякое слово P в алфавите А, содержащее хотя бы одно вхождение буквы b, в слово, которое получается вычеркиванием в P самого левого вхождения буквы b. Пустое слово $\mathfrak{A}$ перерабатывает в самого себя. Наконец $\mathfrak{A}$ неприменим к непустым словам, не содержащим вхождений буквы b.

2. Пусть А есть алфавит $\{a_0, a_1, \ldots, a_n\}$. Рассмотрим схему

$$\begin{cases} a_0 \to \Lambda \\ a_1 \to \Lambda \\ \vdots \\ a_n \to \Lambda \end{cases}$$

Условимся сокращенно изображать эту схему так:

$$\{\xi \to \Lambda \qquad (\xi \in \mathrm{A})$$

(При расшифровке такой сокращенной записи соответствующие формулы подстановки можно выписывать в произвольном порядке.) Эта схема определяет нормальный алгорифм $\mathfrak{A}$, перерабатывающий всякое слово (в алфавите А) в пустое слово. Например, $\mathfrak{A}: a_1a_2a_1a_3a_0 \vdash a_1a_2a_1a_3 \vdash a_2a_1a_3 \vdash a_2a_3 \vdash a_3 \vdash \Lambda$ и, наконец, $\mathfrak{A}: \Lambda \sqsupset$. Следовательно, $\mathfrak{A}(a_1a_2a_1a_3a_0) = \Lambda$.

3. Пусть А — алфавит, содержащий букву S_1, которую мы сокращенно обозначим через 1. Для всякого натурального числа n определим по индукции $\overline{0} = 1$ и $\overline{n+1} = \overline{n}1$. Таким образом, $\overline{1} = 11$, $\overline{2} = 111$ и т. д. Слова $\overline{n}$ называются *цифрами*. Определим теперь нормальный алгорифм $\mathfrak{A}$, схемой

$$\{\Lambda \to \cdot 1$$

Для любого слова P в алфавите А имеем $\mathfrak{A}(P) = 1P$ *). В частности $\mathfrak{A}(\overline{n}) = \overline{n+1}$ при любом натуральном n.

4. Пусть А — произвольный алфавит $\{a_0, a_1, \ldots, a_n\}$. Для всякого слова $P = a_{j_0}a_{j_1} \ldots a_{j_k}$ слово $\overline{P} = a_{j_k}a_{j_{k-1}} \ldots a_{j_1}a_{j_0}$ назовем *обращением*

*) Это очевидно, если заметить, что всякое слово P начинается с вхождения пустого слова Λ, ибо $P = \Lambda P$.

слова P. Построим нормальный алгорифм $\mathfrak{A}$ такой, чтобы для любого слова P в алфавите A выполнялось равенство $\mathfrak{A}(P)=\widetilde{P}$. Рассмотрим следующую (сокращенно записанную) схему алгорифма в алфавите $B=A\cup\{\alpha,\beta\}$:

$$\begin{cases} \alpha\alpha\to\beta & \text{(a)}\\ \beta\xi\to\xi\beta \quad (\xi\in A) & \text{(b)}\\ \beta\alpha\to\beta & \text{(c)}\\ \beta\to\cdot\Lambda & \text{(d)}\\ \alpha\eta\xi\to\xi\alpha\eta \quad (\eta,\ \xi\in A) & \text{(e)}\\ \Lambda\to\alpha & \text{(f)} \end{cases}$$

Эта схема определяет некоторый нормальный алгорифм $\mathfrak{A}$ в алфавите B. Рассмотрим произвольное слово $P=a_{j_0}a_{j_1}\dots a_{j_k}$ в алфавите A. В силу формулы подстановки (f), $\mathfrak{A}:P\vdash\alpha P$. Затем, применяя последовательно формулы подстановки (e), получаем $\mathfrak{A}:\alpha P\vdash a_{j_1}\alpha a_{j_0}a_{j_2}\dots a_{j_k}\vdash a_{j_1}a_{j_2}\alpha a_{j_0}a_{j_3}\dots\dots a_{j_k}\vdash\dots\vdash a_{j_1}a_{j_2}\dots a_{j_k}\alpha a_{j_0}$. Таким образом, $\mathfrak{A}:P\models a_{j_1}a_{j_2}\dots a_{j_k}\alpha a_{j_0}$. С помощью (f) получаем затем $\mathfrak{A}:P\models\alpha a_{j_1}a_{j_2}\dots a_{j_k}\alpha a_{j_0}$. Применяя, как и выше, формулы подстановки (e), получаем $\mathfrak{A}:P\models a_{j_2}a_{j_3}\dots\dots a_{j_k}\alpha a_{j_1}\alpha a_{j_0}$. Повторяя этот процесс, приходим к $\mathfrak{A}:P\models\alpha a_{j_k}\alpha a_{j_{k-1}}\dots\dots\alpha a_{j_1}\alpha a_{j_0}$. Теперь, снова на основании (f), $\mathfrak{A}:P\models\alpha\alpha a_{j_k}\alpha a_{j_{k-1}}\dots\alpha a_{j_1}\alpha a_{j_0}$, и с помощью (a) $\mathfrak{A}:P\models\beta a_{j_k}\alpha a_{j_{k-1}}\dots\alpha a_{j_1}\alpha a_{j_0}$. Теперь остается применить (b), (c) и в заключение (d), после чего и получаем $\mathfrak{A}:P\models\cdot\widetilde{P}$. Итак, мы построили некоторый нормальный алгорифм $\mathfrak{A}$ над алфавитом A, обращающий всякое слово в алфавите A *).

Упражнения

1. Пусть заданы алфавит A и произвольное слово Q в этом алфавите. Описать действие нормальных алгорифмов, задаваемых следующими схемами:

(a) $\{\Lambda\to\cdot Q.$

(b) Схема в алфавите $B=A\cup\{\alpha\}$, где α не принадлежит A:

$$\begin{cases}\alpha\xi\to\xi\alpha \quad (\xi\in A)\\ \alpha\to\cdot Q\\ \Lambda\to\alpha\end{cases}$$

*) Различие между понятием нормального алгорифма в алфавите A и понятием нормального алгорифма над алфавитом A является весьма важным. Всякий нормальный алгорифм в A использует только буквы A, тогда как нормальный алгорифм над A может использовать и некоторые дополнительные буквы, не входящие в A. Всякий нормальный алгорифм в A является также нормальным алгорифмом над A, но существуют, вообще говоря, алгорифмы в A, которые определяются нормальными алгорифмами над A, но сами не являются нормальными алгорифмами в A (см. упражнение 2 (d), стр. 251).

(c)
$$\begin{cases} \xi \to \Lambda & (\xi \in A) \\ \Lambda \to \cdot Q \end{cases}$$

(d) Схема в алфавите $B = A \cup \{1\}$:

$$\{\xi \to 1 \qquad (\xi \in A - \{1\})$$

2. Пусть алфавит A не содержит букв α, β, γ, и пусть $B = A \cup \{\alpha\}$ и $C = A \cup \{\alpha, \beta, \gamma\}$.

(a) Построить нормальный алгорифм $\mathfrak{A}$ в B такой, что $\mathfrak{A}(\Lambda) = \Lambda$ и $\mathfrak{A}(\xi P) = P$ для любой буквы ξ из A и для любого слова P в A (т. е. нормальный алгорифм, «стирающий» первую букву во всяком непустом слове в алфавите A).

(b) Построить нормальный алгорифм $\mathfrak{B}$ в алфавите C такой, чтобы для любого слова P в алфавите A было выполнено равенство $\mathfrak{B}(P) = PP$.

3. Пусть буква α не входит в алфавиты A и B, и пусть $a_1, \ldots, a_k$ — фиксированные буквы из алфавита A, а $Q_1, \ldots, Q_k$ — фиксированные слова в алфавите B. Показать, что нормальный алгорифм в алфавите $A \cup B \cup \{\alpha\}$, задаваемый схемой

$$\begin{cases} \alpha a_i \to Q_i \alpha & (i = 1, \ldots, k) \\ \alpha \xi \to \xi \alpha & (\xi \in A - \{a_1, \ldots, a_k\}) \\ \alpha \to \cdot \Lambda \\ \Lambda \to \alpha \end{cases}$$

перерабатывает всякое слово P в алфавите A в слово $\mathrm{Sub}\,{}^{a_1, \ldots, a_k}_{Q_1, \ldots, Q_k}(P)$, т. е. в результат одновременной подстановки слов $Q_1, \ldots, Q_k$ в слово P соответственно вместо букв $a_1, \ldots, a_k$.

4. Пусть $H = \{1\}$ и $M = \{1, *\}$. Всякое натуральное число n может быть представлено соответствующей цифрой $\overline{n}$, которая представляет собой слово в алфавите H. Поставим теперь в соответствие всякому вектору $(n_1, \ldots, n_k)$, где $n_1, \ldots, n_k$ — натуральные числа, слово $\overline{n_1} * \ldots * \overline{n_k}$ в алфавите M, которое обозначим через $\overline{(n_1, \ldots, n_k)}$. Так, например, $\overline{(3, 1, 2)}$ обозначает слово 1111*11*111.

(a) Показать, что схема

$$\begin{cases} * \to * \\ \alpha 1 i \to \alpha 1 \\ \alpha 1 \to \cdot 1 \\ \Lambda \to \alpha \end{cases}$$

определяет нормальный алгорифм $\mathfrak{A}_Z$ над алфавитом M, применимый только к тем словам в алфавите M, которые являются цифрами, и такой, что $\mathfrak{A}_Z(\overline{n}) = \overline{0}$ для любого n.

(b). Показать, что нормальный алгорифм $\mathfrak{A}_N$ над алфавитом M, определяемый схемой

$$\begin{cases} * \to * \\ \alpha 1 \to \cdot 11 \\ \Lambda \to \alpha \end{cases}$$

применим только к тем словам в алфавите M, которые суть цифры, причем $\mathfrak{A}_N(\overline{n}) = \overline{n+1}$ для любого n.

(c) Пусть $\alpha_1, \ldots, \alpha_{2k}$ — буквы, не входящие в алфавит M, и пусть $1 \leqslant j \leqslant k$. Обозначим через $\mathscr{S}_i$ (при $1 \leqslant i < k$) список формул подстановки

$$\begin{aligned} \alpha_{2i-1}* &\to \alpha_{2i-1}* \\ \alpha_{2i-1}1 &\to \alpha_{2i}1 \\ \alpha_{2i}1 &\to \alpha_{2i} \\ \alpha_{2i}* &\to \alpha_{2i+1} \end{aligned}$$

Рассмотрим нормальный алгорифм $\mathfrak{A}_j^k$, задаваемый одной из следующих трех схем:

если $1 < j < k$, то схемой

$\mathscr{S}_1$
$\vdots$
$\mathscr{S}_{j-1}$
$\alpha_{2j-1}* \to \alpha_{2j-1}*$
$\alpha_{2j-1}1 \to \alpha_{2j}1$
$\alpha_{2j}1 \to 1\alpha_{2j}$
$\alpha_{2j}* \to \alpha_{2j+1}$
$\mathscr{S}_{j+1}$
$\vdots$
$\mathscr{S}_{k-1}$
$\alpha_{2k-1}* \to \alpha_{2k-1}*$
$\alpha_{2k-1}1 \to \alpha_{2k}1$
$\alpha_{2k}1 \to \alpha_{2k}$
$\alpha_{2k}* \to \alpha_{2k}*$
$\alpha_{2k} \to \cdot\Lambda$
$\Lambda \to \alpha_1$

если $j = 1$, то схемой

$\alpha_1* \to \alpha_1*$
$\alpha_1 1 \to \alpha_2 1$
$\alpha_2 1 \to 1\alpha_2$
$\alpha_2* \to \alpha_3$
$\mathscr{S}_2$
$\vdots$
$\mathscr{S}_{k-1}$
$\alpha_{2k-1}* \to \alpha_{2k-1}*$
$\alpha_{2k-1}1 \to \alpha_{2k}1$
$\alpha_{2k}1 \to \alpha_{2k}$
$\alpha_{2k}* \to \alpha_{2k}*$
$\alpha_{2k} \to \cdot\Lambda$
$\Lambda \to \alpha_1$

если $j = k$, то схемой

$\mathscr{S}_1$
$\vdots$
$\mathscr{S}_{k-1}$
$\alpha_{2k-1}* \to \alpha_{2k-1}*$
$\alpha_{2k-1}1 \to \alpha_{2k}1$
$\alpha_{2k}1 \to 1\alpha_{2k}$
$\alpha_{2k}* \to \alpha_{2k}*$
$\alpha_{2k} \to \cdot\Lambda$
$\Lambda \to \alpha_1$

Показать, что $\mathfrak{A}_j^k$ применим к тем и только тем словам в алфавите M, которые имеют вид $\overline{(n_1, \ldots, n_k)}$, причем $\mathfrak{A}_j^k\left(\overline{(n_1, \ldots, n_k)}\right) = \overline{n_j}$ для любого набора $(n_1, \ldots, n_k)$.

(d) Построить схему нормального алгорифма в алфавите M, перерабатывающего $\overline{(n_1, n_2)}$ в $\overline{|n_1 - n_2|}$.

(e) Построить нормальные алгорифмы над алфавитом M для арифметических операций сложения и умножения.

Пусть $\mathfrak{A}$ и $\mathfrak{B}$ — алгорифмы, а P — слово. Мы будем применять запись $\mathfrak{A}(P) \simeq \mathfrak{B}(P)$ для выражения того факта, что либо алгорифмы $\mathfrak{A}$ и $\mathfrak{B}$ оба неприменимы к слову P, либо оба они к нему применимы и при этом $\mathfrak{A}(P) = \mathfrak{B}(P)$. Вообще, если C и D — какие-нибудь выражения, то $C \simeq D$ будет в дальнейшем означать, что либо оба эти выражения не определены, либо оба они определены и обозначают один и тот же объект. Назовем

два алгорифма $\mathfrak{A}$ и $\mathfrak{B}$ над алфавитом A *вполне эквивалентными* относительно A, если для любого слова P в алфавите A $\mathfrak{A}(P) \simeq \mathfrak{B}(P)$. Те же алгорифмы назовем *эквивалентными* относительно алфавита A, если $\mathfrak{A}(P) \simeq \mathfrak{B}(P)$ всякий раз, когда P есть слово в A, и хотя бы одно из слов $\mathfrak{A}(P)$ или $\mathfrak{B}(P)$ определено и тоже является словом в A.

Пусть, как и прежде (упражнение 4 на стр. 233), M обозначает алфавит $\{1, *\}$, пусть также ω — множество всех натуральных чисел и φ есть частичная эффективно вычислимая арифметическая функция от n аргументов, т. е. функция, отображающая некоторое подмножество множества ω^n в ω. Через $\mathfrak{B}_\varphi$ обозначим соответствующий алгорифм в M, т. е. такой алгорифм, что $\mathfrak{B}_\varphi(\overline{(k_1, \ldots, k_n)}) = \varphi(k_1, \ldots, k_n)$ всякий раз, когда хотя бы одна из частей этого равенства определена. Предполагается также, что $\mathfrak{B}_\varphi$ неприменим к словам, отличным от слов вида $\overline{(k_1, \ldots, k_n)}$. Мы назовем функцию φ *частично вычислимой по Маркову* функцией, если существует нормальный алгорифм $\mathfrak{A}$ над M, вполне эквивалентный $\mathfrak{B}_\varphi$ относительно M *). Если функция φ определена всюду, т. е. для любой n-ки натуральных чисел, и является частично вычислимой по Маркову, то мы ее назовем *вычислимой по Маркову*.

Мы теперь обобщим понятие рекурсивной функции (см. стр. 136). Частичную функцию φ от n аргументов назовем *частично рекурсивной*, если она может быть получена, исходя из начальных функций Z (нуль-функция), U_j^n (проектирующие функции) и N (прибавление единицы), с помощью подстановки, рекурсии и неограниченного μ-оператора. (Мы говорим, что функция ψ получена из функции τ с помощью неограниченного μ-оператора, если $\psi(x_1, \ldots, x_n) = \mu y\,(\tau(x_1, \ldots, x_n, y) = 0)$, где $\mu y\,(\tau(x_1, \ldots, x_n, y) = 0)$ есть наименьшее число k (если такое существует), для которого $\tau(x_1, \ldots, x_n, k) = 0$, а если $1 \leqslant i < k$, то $\tau(x_1, \ldots, x_n, i)$ определено и отлично от 0. Таким образом, $\psi(x_1, \ldots, x_n)$ может быть не определено для некоторых n-ок $(x_1, \ldots, x_n)$. В частности $\psi(x_1, \ldots, x_n)$ не определено для данных $x_1, \ldots, x_n$, если не существует такого y, что $\tau(x_1, \ldots, x_n, y) = 0$.) Очевидно, всякая рекурсивная функция является частично рекурсивной. Утверждение о том, что всякая всюду определенная частично рекурсивная функция является рекурсивной, верно, но отнюдь не очевидно, и мы его позже докажем. Мы покажем, что совпадают понятия частично вычислимой по Маркову функции и частично рекурсивной функции, а также понятия вычислимой по Маркову функции и рекурсивной функции.

Будем говорить о нормальном алгорифме, что он *замкнут*, если его схема содержит формулу подстановки вида $\Lambda \to \cdot Q$. В работе такого

*) В этом и во всех других определениях настоящей главы квантор существования понимается в обычном «классическом» смысле. Когда мы утверждаем, что существует объект того или иного рода, то мы отнюдь не хотим этим сказать, что кто-то фактически уже нашел или когда-либо найдет такой объект. Так, в нашем случае функция φ может быть частично вычислимой по Маркову и при этом не обязательно, чтобы мы когда-нибудь в этом фактически убедились.

алгорифма возможен лишь заключительный обрыв, т. е. обрыв в результате применения заключительной формулы подстановки. Пусть $\mathfrak{A}$ — произвольный алгорифм. Обозначим через $\mathfrak{A}'$ нормальный алгорифм, схема которого получается из схемы $\mathfrak{A}$ добавлением новой формулы подстановки $\Lambda \to \cdot \Lambda$ к ней в конце. Нормальный алгорифм $\mathfrak{A}'$ замкнут и вполне эквивалентен алгорифму $\mathfrak{A}$ относительно алфавита алгорифма $\mathfrak{A}$.

Покажем теперь, что композиция двух нормальных алгорифмов есть снова нормальный алгорифм. Пусть $\mathfrak{A}$ и $\mathfrak{B}$ — нормальные алгорифмы в алфавите A. Сопоставим каждой букве b этого алфавита новую букву $\bar{b}$, которую назовем *двойником* буквы b. Пусть $\bar{\mathrm{A}}$ — алфавит, состоящий из всех двойников букв алфавита A. Выберем еще какие-нибудь две буквы α и β, не принадлежащие $\mathrm{A} \cup \bar{\mathrm{A}}$. Обозначим через $\mathscr{S}_{\mathfrak{A}}$ схему, полученную из схемы нормального алгорифма $\mathfrak{A}'$ заменой в ней точки в каждой заключительной формуле подстановки буквой α, и обозначим через $\mathscr{S}_{\mathfrak{B}}$ схему, которая получается путем замены в схеме алгорифма $\mathfrak{B}'$ всех букв алфавита A их двойниками, всех точек — буквами β с последующей заменой всех формул подстановки вида $\Lambda \to Q$ и $\Lambda \to \cdot Q$ соответственно формулами подстановки $\alpha \to \alpha Q$ и $\alpha \to \alpha\beta Q$. Рассмотрим схему (в сокращенной записи):

$$\begin{cases} a\alpha \to \alpha a & (a \in \mathrm{A}) \\ \alpha a \to \alpha \bar{a} & (a \in \mathrm{A}) \\ \bar{a}\bar{b} \to \bar{a}\bar{b} & (a, b \in \mathrm{A}) \\ \bar{a}\beta \to \beta \bar{a} & (a \in \mathrm{A}) \\ \beta \bar{a} \to \beta a & (a \in \mathrm{A}) \\ a\bar{b} \to ab & (a, b \in \mathrm{A}) \\ \alpha\beta \to \cdot \Lambda & \\ \mathscr{S}_{\mathfrak{B}} & \\ \mathscr{S}_{\mathfrak{A}} & \end{cases}$$

Нормальный алгорифм $\mathfrak{C}$ над алфавитом A, определяемый этой схемой, таков, что для любого слова P в A $\mathfrak{C}(P) \simeq \mathfrak{B}(\mathfrak{A}(P))$ (доказать в качестве упражнения). Этот нормальный алгорифм называется *композицией* алгорифмов $\mathfrak{A}$ и $\mathfrak{B}$ и обозначается также символом $\mathfrak{B} \cdot \mathfrak{A}$. В общем случае под $\mathfrak{A}_n \circ \ldots \circ \mathfrak{A}_1$ мы будем понимать $\mathfrak{A}_n \cdot (\ldots \circ \mathfrak{A}_3 \circ (\mathfrak{A}_2 \circ \mathfrak{A}_1)) \ldots)$.

Пусть $\mathfrak{D}$ — некоторый нормальный алгорифм в алфавите A и B — некоторое расширение A. К схеме алгорифма $\mathfrak{D}$ добавим сверху всевозможные формулы подстановки вида $b \to b$, где b — произвольная буква из B — A. Полученная таким образом схема определяет некоторый нормальный алгорифм $\mathfrak{D}_{\mathrm{B}}$ в алфавите B, который неприменим ни к какому слову, содержащему буквы из B — A, и такой, что $\mathfrak{D}_{\mathrm{B}}(P) \simeq \mathfrak{D}(P)$ для любого слова P в A. Алгорифм $\mathfrak{D}_{\mathrm{B}}$ вполне эквивалентен алгорифму $\mathfrak{D}$

относительно алфавита A и называется *формальным распространением* алгорифма $\mathfrak{D}$ на алфавит B.

Пусть даны нормальные алгорифмы $\mathfrak{A}$ и $\mathfrak{B}$ соответственно в алфавитах A_1 и A_2. Рассмотрим алфавит $A = A_1 \cup A_2$ и формальные распространения $\mathfrak{A}_A$ и $\mathfrak{B}_A$ алгорифмов $\mathfrak{A}$ и $\mathfrak{B}$ на алфавит A. Композиция $\mathfrak{C}$ алгорифмов $\mathfrak{A}_A$ и $\mathfrak{B}_A$ называется *нормальной композицией* алгорифмов $\mathfrak{A}$ и $\mathfrak{B}$ и обозначается символом $\mathfrak{B} \cdot \mathfrak{A}$. (Недоразумений в связи с этим вторичным введением символа $\mathfrak{B} \cdot \mathfrak{A}$ не возникает, так как в случае, когда $A_1 = A_2$, нормальная композиция алгорифмов $\mathfrak{A}$ и $\mathfrak{B}$ совпадает с их композицией.) $\mathfrak{C}$ является нормальным алгорифмом над A, причем $\mathfrak{C}(P) \simeq \mathfrak{B}(\mathfrak{A}(P))$ для любого слова P в A_1, и кроме того, $\mathfrak{C}$ применим только к таким словам P в алфавите A, которые удовлетворяют условиям: (i) P есть слово в A_1, (ii) $\mathfrak{A}$ применим к P, (iii) $\mathfrak{B}$ применим к $\mathfrak{A}(P)$.

Предположим, что алфавит B является расширением алфавита A, и пусть P — произвольное слово в алфавите B. *Проекцией* P^A *слова* P *на алфавит* A называется слово, получающееся из P, если в P стереть все вхождения букв из B — A. Сокращенно записанная схема

$$\{\ \xi \to \Lambda \quad (\xi \in B - A)$$

задает нормальный алгорифм $\mathfrak{P}_{B,A}$ такой, что $\mathfrak{P}_{B,A}(P) = P^A$ для любого слова P в B. Алгорифм $\mathfrak{P}_{B,A}$ называется *проектирующим алгорифмом*.

Пусть A и C — алфавиты без общих букв. Положим $B = A \cup C$. Тогда сокращенно записанная схема

$$\{\ ca \to ac \quad (a \in A,\ c \in C)$$

задает нормальный алгорифм $\mathfrak{L}_{A,C}$ в алфавите B такой, что $\mathfrak{L}_{A,C}(P) = P^A P^C$ для любого слова P в B.

Если $\mathfrak{A}$ есть нормальный алгорифм в алфавите A и B есть расширение A, то нормальный алгорифм $\mathfrak{B}$ в алфавите B, задаваемый схемой алгорифма $\mathfrak{A}$, назовем *естественным распространением* алгорифма $\mathfrak{A}$ на алфавит B. Очевидно, что $\mathfrak{B}(P) \simeq \mathfrak{A}(P)$ для любого слова P в A и, кроме того, $\mathfrak{B}(PQ) \simeq \mathfrak{A}(P)\,Q$ для любого слова P в A и для любого слова Q в B — A. Заметим, что естественное распространение алгорифма $\mathfrak{A}$ на B, вообще говоря, отличается от формального распространения $\mathfrak{A}$ на B, так как последнее неприменимо ни к какому слову, содержащему буквы из B — A.

Предложение 5.1. *Пусть* $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$ *— нормальные алгорифмы и* A *— объединение их алфавитов. Тогда существует нормальный алгорифм* $\mathfrak{B}$ *над* A, *называемый* соединением *алгорифмов* $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$, *такой, что* $\mathfrak{B}(P) \simeq \mathfrak{A}_1^{\#}(P)\,\mathfrak{A}_2^{\#}(P) \ldots \mathfrak{A}_k^{\#}(P)$ *для любого слова* P *в алфавите* A, *где* $\mathfrak{A}_i^{\#}$ *есть естественное распространение* $\mathfrak{A}_i$ *на* A.

Доказательство. Мы докажем это предложение для $k = 2$ после чего индукцией по k легко может быть получен и общий случай

Введем алфавит $\bar{A}$ двойников букв алфавита A. Положим $B = A \cup \bar{A}$. Пусть $\bar{\mathfrak{A}}_1$ — нормальный алгорифм, схема которого получается заменой каждой буквы схемы алгорифма $\mathfrak{A}_1$ ее двойником, и пусть $\bar{\mathfrak{A}}_1^{\#}$, $\mathfrak{A}_2^{\#}$ — естественные распространения соответственно алгорифмов $\bar{\mathfrak{A}}_1$ и $\mathfrak{A}_2$ на B. Пусть $A = \{a_1, \ldots, a_n\}$. В силу упражнения 3 (стр. 233), существуют нормальные алгорифмы $\mathfrak{W}_1 = \mathrm{Sub}^{a_1 \bar{a}_1, \ldots, a_n \bar{a}_n}_{a_1, \ldots, a_n}$ и $\mathfrak{W}_2 = \mathrm{Sub}^{\bar{a}_1, \ldots, \bar{a}_n}_{a_1, \ldots, a_n}$ над B такие, что $\mathfrak{W}_1$ подставляет одновременно $a_1\bar{a}_1$ вместо a_1, $a_2\bar{a}_2$ вместо a_2 и т. д., а $\mathfrak{W}_2$ подставляет одновременно a_1 вместо $\bar{a}_1$, a_2 вместо $\bar{a}_2$ и т. д. Существуют, кроме того, нормальные алгорифмы $\mathfrak{L}_{A, \bar{A}}$ и $\mathfrak{L}_{\bar{A}, A}$ такие, что $\mathfrak{L}_{A, \bar{A}}(P) = P^A P^{\bar{A}}$ и $\mathfrak{L}_{\bar{A}, A}(P) = P^{\bar{A}} P^A$. Тогда, как легко проверить, нормальная композиция $\mathfrak{B} = \mathfrak{W}_2 \cdot \bar{\mathfrak{A}}_1^{\#} \cdot \mathfrak{L}_{\bar{A}, A} \cdot \mathfrak{A}_2^{\#} \cdot \mathfrak{L}_{A, \bar{A}} \cdot \mathfrak{W}_1$ обладает искомым свойством: $\mathfrak{B}(P) \simeq \mathfrak{A}_1^{\#}(P)\mathfrak{A}_2^{\#}(P)$ для любого слова P в алфавите A.

Следствие 5.2. *Пусть* $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$ *— нормальные алгорифмы соответственно в алфавитах* $A_1, \ldots, A_k$, *и пусть* $A = A_1 \cup \ldots \cup A_k$. *Тогда существует нормальный алгорифм* $\mathfrak{B}$ *над* $A \cup \{*\}$ *такой, что* $\mathfrak{B}(P) \simeq \mathfrak{A}_1^{\#}(P) * \mathfrak{A}_2^{\#}(P) * \ldots * \mathfrak{A}_k^{\#}(P)$ *для любого слова* P *в* A, *где* $\mathfrak{A}_i^{\#}$ *— естественное распространение* $\mathfrak{A}_i$ *на* A*). (*В частности*, $\mathfrak{B}(P) \simeq \mathfrak{A}_1(P) * \mathfrak{A}_2(P) * \ldots * \mathfrak{A}_k(P)$ *для любого слова* P *в алфавите* $A_1 \cap \ldots \cap A_k$.)

Доказательство. Существует такой нормальный алгорифм $\mathfrak{D}$ в $A \cup \{*\}$, что $\mathfrak{D}(P) = *$ для любого слова P в A.

Алгорифм $\mathfrak{D}$ зададим схемой

$$\begin{cases} a \to \Lambda & (a \in A) \\ \Lambda \to \cdot * \end{cases}$$

Пусть, на основании предложения 5.1, $\mathfrak{B}$ есть соединение алгорифмов $\mathfrak{A}_1$, $\mathfrak{D}$, $\mathfrak{A}_2$, $\mathfrak{D}$, ..., $\mathfrak{D}$, $\mathfrak{A}_k$. Тогда, как нетрудно видеть, $\mathfrak{B}(P) \simeq \mathfrak{A}_1^{\#}(P) * \mathfrak{A}_2^{\#}(P) * \ldots * \mathfrak{A}_k(P)$ для любого слова P в A и, в частности, $\mathfrak{B}(P) \simeq \mathfrak{A}_1(P) * \mathfrak{A}_2(P) * \ldots * \mathfrak{A}_k(P)$ для любого слова P в пересечении алфавитов $A_1, \ldots, A_k$.

Лемма 5.3. (1) *Пусть* $\mathfrak{C}$ *— нормальный алгорифм в алфавите* A *и* α *— произвольная буква. Тогда существует нормальный алгорифм* $\mathfrak{D}$ *над* $A \cup \{\alpha\}$ *такой, что для любого слова* P *в* A

$$\mathfrak{D}(P) = \begin{cases} \alpha P, & \text{если } \mathfrak{C}(P) = \Lambda, \\ P, & \text{если } \mathfrak{C}(P) \neq \Lambda \end{cases}$$

и алгорифм $\mathfrak{D}$ *применим только к тем словам, к которым применим* $\mathfrak{C}$.

*) Для дальнейших приложений следствия 5.2 полезно заметить, что автор здесь допускает возможность $* \in A$. (*Прим. ред.*)

(2) *Если* $\mathfrak{A}$ *и* $\mathfrak{B}$ *— нормальные алгорифмы в алфавите* A *и* α *— буква, не принадлежащая* A, *то существует нормальный алгорифм* $\mathfrak{G}$ *над* $A \cup \{\alpha\}$ *такой, что* $\mathfrak{G}(P) \simeq \mathfrak{A}(P)$ *и* $\mathfrak{G}(\alpha P) \simeq \mathfrak{B}(P)$ *для любого слова* P *в* A.

Доказательство. (1) Существует нормальный алгорифм $\mathfrak{H}_1$ над $A \cup \{\alpha\}$, перерабатывающий Λ в α и всякое непустое слово в алфавите $A \cup \{\alpha\}$ — в Λ. Такой алгорифм может быть задан, например, следующей схемой:

$$\begin{cases} a \to \beta & (a \in A \cup \{\alpha\}) \\ \beta\beta \to \beta \\ \beta \to \cdot \Lambda \\ \Lambda \to \cdot \alpha \end{cases}$$

где β — буква, не принадлежащая алфавиту $A \cup \{\alpha\}$.

Пусть $\mathfrak{H}_2 = \mathfrak{H}_1 \cdot \mathfrak{C}$. Для любого слова P в A, если $\mathfrak{C}(P) = \Lambda$, то $\mathfrak{H}_2(P) = \alpha$, и если $\mathfrak{C}(P) \neq \Lambda$, то $\mathfrak{H}_2(P) = \Lambda$. Пусть $\mathfrak{I}$ — тождественный нормальный алгорифм в A (со схемой $\{\Lambda \to \cdot \Lambda\}$), и пусть $\mathfrak{D}$ есть соединение алгорифмов $\mathfrak{H}_2$ и $\mathfrak{I}$. Тогда если $\mathfrak{C}(P) = \Lambda$, то $\mathfrak{D}(P) = \alpha P$, и если $\mathfrak{C}(P) \neq \Lambda$, то $\mathfrak{D}(P) = P$.

(2) Введем алфавит $\bar{A}$ двойников букв алфавита A. Пусть $B = A \cup \bar{A} \cup \{\alpha, \beta\}$, где $\beta \notin A \cup \bar{A} \cup \{\alpha\}$. Если мы заменим в схеме алгорифма $\mathfrak{B}$ всякую букву алфавита A ее двойником, все точки — буквой β, а в получившейся в результате этого схеме заменим всякую формулу подстановки вида $\Lambda \to Q$ и $\Lambda \to \beta Q$ соответственно на $\alpha \to \alpha Q$ и $\alpha \to \alpha\beta Q$, то получим некоторую схему, которую обозначим через $\mathscr{S}_{\bar{\mathfrak{B}}}$. Пусть $\mathscr{S}_{\mathfrak{A}\cdot}$ — схема алгорифма $\mathfrak{A}\cdot$. Построим теперь схему

$$\begin{cases} \alpha a \to \alpha \bar{a} & (a \in A) \\ \bar{a}b \to \bar{a}\bar{b} & (a, b \in A) \\ \bar{a}\beta \to \beta\bar{a} & (a \in A) \\ \beta\bar{a} \to \beta a & (a \in A) \\ a\bar{b} \to ab & (a, b \in A) \\ \alpha\beta \to \cdot \Lambda \\ \mathscr{S}_{\bar{\mathfrak{B}}} \\ \mathscr{S}_{\mathfrak{A}\cdot} \end{cases}$$

Определенный этой схемой нормальный алгорифм $\mathfrak{G}$ над $A \cup \{\alpha\}$ есть искомый алгорифм, т. е. $\mathfrak{G}(P) \simeq \mathfrak{A}(P)$ и $\mathfrak{G}(\alpha P) \simeq \mathfrak{B}(P)$ для всякого слова P в A.

Предложение 5.4. *Пусть* $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ *— нормальные алгорифмы и* A *— объединение их алфавитов. Тогда существует нормальный*

алгорифм $\mathfrak{E}$ *над* A *такой, что*

$$\mathfrak{E}(P) \simeq \begin{cases} \mathfrak{B}(P), & \text{если } P \text{ есть слово в A и } \mathfrak{C}(P) = \Lambda, \\ \mathfrak{A}(P), & \text{если } P \text{ есть слово в A и } \mathfrak{C}(P) \neq \Lambda, \end{cases}$$

и применимый к тем и только к тем словам в A, *к которым применим* $\mathfrak{C}$. *Алгорифм* $\mathfrak{E}$ *называется* разветвлением *алгорифмов* $\mathfrak{A}$ *и* $\mathfrak{B}$, *управляемым алгорифмом* $\mathfrak{C}$.

Доказательство. Пусть $\mathfrak{A}_1$, $\mathfrak{B}_1$ и $\mathfrak{C}_1$ — формальные распространения соответственно алгорифмов $\mathfrak{A}$, $\mathfrak{B}$ и $\mathfrak{C}$ на A, и пусть α — буква, не входящая в A. По лемме 5.3 (1) существует такой нормальный алгорифм $\mathfrak{D}$ над $A \cup \{\alpha\}$, что

$$\mathfrak{D}(P) = \begin{cases} \alpha P, & \text{если } P \text{ есть слово в A и } \mathfrak{C}(P) = \Lambda, \\ P, & \text{если } P \text{ есть слово в A и } \mathfrak{C}(P) \neq \Lambda. \end{cases}$$

Кроме того, по лемме 5.3(2), существует нормальный алгорифм $\mathfrak{G}$ над $A \cup \{\alpha\}$ такой, что если P есть слово в A, то $\mathfrak{G}(P) \simeq \mathfrak{A}_1(P)$ и $\mathfrak{G}(\alpha P) \simeq \mathfrak{B}_1(P)$. Теперь остается положить $\mathfrak{E} = \mathfrak{G} \cdot \mathfrak{D}$.

Пусть даны алгорифмы $\mathfrak{A}$ и $\mathfrak{C}$ в алфавите A и произвольное слово P_0 в A. Применим $\mathfrak{A}$ к P_0. Если в результате получится некоторое слово P_1, то применим $\mathfrak{C}$ к P_1. Если окажется, что $\mathfrak{C}(P_1) = \Lambda$, то процесс заканчивается. Если же окажется, что $\mathfrak{C}(P_1) \neq \Lambda$, то применим $\mathfrak{A}$ к P_1. Если в результате получится некоторое слово P_2, то применим $\mathfrak{C}$ к P_2, и снова, если окажется, что $\mathfrak{C}(P_2) = \Lambda$, то процесс останавливаем, если же окажется, что $\mathfrak{C}(P_2) \neq \Lambda$, то применяем $\mathfrak{A}$ к P_2 и т. д. Определенный таким образом алгорифм $\mathfrak{B}$ называется *повторением* алгорифма $\mathfrak{A}$, управляемым алгорифмом $\mathfrak{C}$. Очевидно, что $\mathfrak{B}(P_0) = Q$ тогда и только тогда, когда существует последовательность слов $P_0, P_1, \ldots, P_n$ $(n > 0)$ такая, что $P_n = Q$, $\mathfrak{C}(P_n) = \Lambda$, $P_i = \mathfrak{A}(P_{i-1})$ при $0 < i \leqslant n$ и $\mathfrak{C}(P_i) \neq \Lambda$ при $0 < i < n$.

Предложение 5.5. *Пусть* $\mathfrak{A}$ *и* $\mathfrak{C}$ — *нормальные алгорифмы*, A — *объединение их алфавитов и* $\mathfrak{A}_1$ *и* $\mathfrak{C}_1$ — *формальные распространения соответственно* $\mathfrak{A}$ *и* $\mathfrak{C}$ *на* A. *Тогда существует нормальный алгорифм* $\mathfrak{B}$ *над* A, *являющийся повторением алгорифма* $\mathfrak{A}_1$, *управляемым алгорифмом* $\mathfrak{C}_1$.

Доказательство. Предложение, очевидно, достаточно доказать для случая, когда алфавиты алгорифмов $\mathfrak{A}$ и $\mathfrak{C}$ совпадают и когда, следовательно, $\mathfrak{A}_1 = \mathfrak{A}$ и $\mathfrak{C}_1 = \mathfrak{C}$. Пусть буква α не входит в A. По лемме 5.3 (1) существует такой нормальный алгорифм $\mathfrak{D}$ над $B = A \cup \{\alpha\}$, что

$$\mathfrak{D}(P) = \begin{cases} \alpha P, & \text{если } P \text{ есть слово в A и } \mathfrak{C}(P) = \Lambda, \\ P, & \text{если } P \text{ есть слово в A и } \mathfrak{C}(P) \neq \Lambda. \end{cases}$$

Пусть $\mathfrak{F} = \mathfrak{D} \cdot \mathfrak{A}$. $\mathfrak{F}$ есть нормальный алгорифм в некотором расширении F алфавита B. Пусть буква β не входит в F. Рассмотрим

следующую схему:

$$\begin{cases} \xi\beta \to \beta\xi & (\xi \in F) \\ \beta\alpha \to \cdot\alpha \\ \beta \to \Lambda \\ \mathscr{S}_{\mathfrak{F}^\beta} \end{cases}$$

где $\mathscr{S}_{\mathfrak{F}^\beta}$ — схема, полученная из схемы для $\mathfrak{F}^\cdot$ путем замены в ней всех точек буквой β. Эта схема определяет некоторый нормальный алгорифм $\mathfrak{G}$, причем $\mathfrak{G}(P) = Q$ тогда и только тогда, когда существует такая последовательность слов $P_0, \ldots, P_n$, что $P = P_0$, $Q = P_n$, $P_i = \mathfrak{F}(P_{i-1})$ $(0 < i \leqslant n)$ и P_n — единственное в этой последовательности слово, начинающееся с буквы α. Пусть $\mathfrak{P}$ — алгорифм, проектирующий алфавит F на алфавит $F - \{\alpha\}$ (т. е. стирающий все вхождения буквы α; см. стр. 237). Теперь легко убедиться в том, что нормальный алгорифм $\mathfrak{B} = \mathfrak{P} \cdot \mathfrak{G}$ — искомый.

Следствие 5.6. *Пусть* $\mathfrak{A}$ *и* $\mathfrak{C}$ *— нормальные алгорифмы и* A *— объединение их алфавитов. Тогда существует нормальный алгорифм* $\mathfrak{H}$ *над* A, *который всякое слово P в алфавите* A *перерабатывает в слово Q тогда и только тогда, когда существует такая последовательность слов* $P_0, \ldots, P_n$ $(n \geqslant 0)$, *что* $P_0 = P$, $P_n = Q$, $\mathfrak{C}(P_n) = \Lambda$, $P_{i+1} = \mathfrak{A}(P_i)$ *и* $\mathfrak{C}(P_i) \neq \Lambda$ *для* $i = 0, 1, \ldots, n-1$.

Доказательство. Пусть $\mathfrak{I}$ — тождественный нормальный алгорифм и $\mathfrak{B}$ — повторение $\mathfrak{A}$, управляемое алгорифмом $\mathfrak{C}$. Искомым алгорифмом $\mathfrak{H}$ является тогда разветвление $\mathfrak{B}$ и $\mathfrak{I}$, управляемое $\mathfrak{C}$ (см. предложение 5.4). Этот алгорифм $\mathfrak{H}$ называется *полным повторением* алгорифма $\mathfrak{A}$, управляемым $\mathfrak{C}$.

Предложение 5.7. *Каков бы ни был нормальный алгорифм* $\mathfrak{A}$ *в алфавите* A, *существует такой нормальный алгорифм* $\mathfrak{A}^1$ *над алфавитом* $B = A \cup C$ (где $C = \{*, 1\}$), *что для любого слова P в* A *и для любого натурального числа n* $\mathfrak{A}^1(\overline{n} * P) = Q$ *тогда и только тогда, когда существует последовательность слов* $P_0, P_1, \ldots, P_n$ $(n \geqslant 0)$, *удовлетворяющая условиям:* $P_0 = P$, $P_n = Q$ *и* $P_i = \mathfrak{A}(P_{i-1})$ *для* $i = 1, 2, \ldots, n$.

Доказательство. Пусть α — какая-нибудь буква, не входящая в B, и положим $D = B \cup \{\alpha\}$. Рассмотрим нормальные алгорифмы в D, задаваемые следующими схемами:

$\mathfrak{H}_1$:

$$\begin{cases} \alpha 1 1 \to \cdot 1 \\ \alpha 1 * \to \alpha * \\ \alpha * \xi \to \alpha * & (\xi \in B) \\ \alpha * \to \cdot \Lambda \\ \Lambda \to \alpha \end{cases}$$

Легко видеть, что для любого слова P в алфавите B получаем $\mathfrak{H}_1(\bar{0} * P) = \Lambda$ и $\mathfrak{H}_1(\bar{n} * P) \neq \Lambda$, если $n > 0$.

$\mathfrak{H}_2$: $\begin{cases} *\xi \to * \\ * \to \Lambda \end{cases}$ $(\xi \in B)$

Если P не содержит букву $*$, то $\mathfrak{H}_2(P * Q) = P$.

$\mathfrak{H}_3$: $\begin{cases} \alpha 1 \to \alpha \\ \alpha * \to \cdot \Lambda \\ \Lambda \to \alpha \end{cases}$

Как нетрудно проверить, $\mathfrak{H}_3(\bar{n} * P) = P$ для любого P в B.

$\mathfrak{H}_4$: $\{ 1 \to \cdot \Lambda$

$\mathfrak{H}_5$: $\{ 1 * \to \cdot \Lambda$

Очевидно, $\mathfrak{H}_4(\bar{n} * P) = \overline{n-1} * P$, если $n > 0$, и $\mathfrak{H}_4(\bar{0} * P) = * P$. Кроме того, $\mathfrak{H}_5(\bar{0} * P) = P$.

Пусть теперь $\mathfrak{E}$ есть такой нормальный алгорифм, что $\mathfrak{E}(P) = (\mathfrak{H}_2 \circ \mathfrak{H}_4)(P) * (\mathfrak{A} \circ \mathfrak{H}_3)(P)$ для любого слова P в алфавите D (см. следствие 5.2). Тогда для любого слова P в алфавите A получаем

$$\mathfrak{E}(\bar{n} * P) = \begin{cases} \overline{n-1} * \mathfrak{A}(P), & \text{если } n > 0, \\ * \mathfrak{H}(P), & \text{если } n = 0. \end{cases}$$

Обозначим через E алфавит алгорифма $\mathfrak{E}$. В силу следствия 5.6, найдется такой нормальный алгорифм $\mathfrak{F}$ над E, что $\mathfrak{F}(P) = Q$ тогда и только тогда, когда существует последовательность слов $P_0, \ldots, P_k$ $(k \geqslant 0)$, удовлетворяющая условиям: $P_0 = P$, $P_k = Q$, $\mathfrak{H}_1(P_k) = \Lambda$, $P_i = \mathfrak{E}(P_{i-1})$ $(0 < i \leqslant k)$ и $\mathfrak{H}(P_i) \neq \Lambda$ $(0 \leqslant i < k)$. Читателю предоставляется в качестве упражнения доказать теперь, что алгорифм $\mathfrak{A}^! = \mathfrak{H}_5 \circ \mathfrak{F}$ есть искомый нормальный алгорифм.

Предложение 5.8. *Всякая частично рекурсивная функция является частично вычислимой по Маркову функцией, и всякая рекурсивная функция является вычислимой по Маркову функцией.*

Доказательство. (1) Начальные функции Z, N, U_j^k $(1 \leqslant j \leqslant k)$ вычислимы по Маркову (см. упражнение 4, стр. 233—234).

(2) Подстановка. Предположим, что функция ψ получается из функций $\tau, \varphi_1, \ldots, \varphi_k$ с помощью подстановки: $\psi(x_1, \ldots, x_n) = \tau(\varphi_1(x_1, \ldots, x_n), \ldots, \varphi_k(x_1, \ldots, x_n))$, где $\tau, \varphi_1, \ldots, \varphi_k$ — частично рекурсивны. Предположим также, что существуют нормальные алгорифмы $\mathfrak{A}_\tau, \mathfrak{A}_{\varphi_1}, \ldots, \mathfrak{A}_{\varphi_k}$ над $M = \{1, *\}$, которые частично вычисляют соответственно функции $\tau, \varphi_1, \ldots, \varphi_k$. Согласно следствию 5.2, существует нормальный алгорифм $\mathfrak{B}$ над M такой, что $\mathfrak{B}(P) \simeq \mathfrak{A}_{\varphi_1}(P) * \mathfrak{A}_{\varphi_2}(P) * \ldots * \mathfrak{A}_{\varphi_k}(P)$ для любого слова P в алфавите M. В частности,

$$\mathfrak{B}(\overline{(x_1, \ldots, x_n)}) \simeq \overline{\varphi_1(x_1, \ldots, x_n)} * \ldots * \overline{\varphi_k(x_1, \ldots, x_n)}$$

для любых натуральных $x_1, \ldots, x_n$. Положим $\mathfrak{C} = \mathfrak{A}_\tau \circ \mathfrak{B}$. Тогда для любых натуральных $x_1, \ldots, x_n$ имеем

$$\mathfrak{C}(\overline{(x_1, \ldots, x_n)}) \simeq \mathfrak{A}_\tau(\overline{\varphi_1(x_1, \ldots, x_n)}, \ldots, \overline{\varphi_k(x_1, \ldots, x_n)}) \simeq$$
$$\simeq \overline{\tau(\varphi_1(x_1, \ldots, x_n), \ldots, \varphi_k(x_1, \ldots, x_n))}.$$

(3) Рекурсия. Допустим, что функция ψ получена из функций τ и φ с помощью рекурсии:

$$\psi(x_1, \ldots, x_k, 0) = \tau(x_1, \ldots, x_k),$$
$$\psi(x_1, \ldots, x_k, y+1) = \varphi(x_1, \ldots, x_k, y, \psi(x_1, \ldots, x_k, y)),$$

и пусть $\mathfrak{A}_\tau$ и $\mathfrak{A}_\varphi$ — нормальные алгорифмы над M, частично вычисляющие соответственно функции τ и φ. Пусть, наконец, $\mathfrak{A}_Z$, $\mathfrak{A}_N$ и $\mathfrak{A}_j^k$ — нормальные алгорифмы, вычисляющие соответственно функции Z, N и U_j^k. С помощью алгорифмов $\mathfrak{A}_j^{k+1}$ может быть построен, в силу следствия 5.2, такой нормальный алгорифм $\mathfrak{B}_1$ над M, что $\mathfrak{B}_1(\bar{x}_1 * \ldots * \bar{x}_k * \bar{y}) \simeq \bar{x}_1 * \ldots * \bar{x}_k$. Пусть $\mathfrak{K} = \mathfrak{A}_\tau \circ \mathfrak{B}_1$. Снова на основании следствия 5.2 и исходя из алгорифмов $\mathfrak{A}_{k+1}^{k+1}$, $\mathfrak{A}_1^{k+1}$, ..., $\mathfrak{A}_k^{k+1}$, $\mathfrak{A}_Z$, $\mathfrak{K}$, строим нормальный алгорифм $\mathfrak{B}_2$ над M такой, что $\mathfrak{B}_2(\bar{x}_1 * \ldots * \bar{x}_k * \bar{y}) \simeq \bar{y} * \bar{x}_1 * \ldots * \bar{x}_k * \bar{0} * \overline{\tau(x_1, \ldots, x_k)}$. Нормальный алгорифм $\mathfrak{B}_3 = \mathfrak{A}_N \circ \mathfrak{A}_{k+1}^{k+2}$ работает таким образом, что $\mathfrak{B}_3(\bar{x}_1 * \ldots * \bar{x}_k * \bar{y} * \bar{x}) = \overline{y+1}$. Применив следствие 5.2 к алгорифмам $\mathfrak{A}_1^{k+2}, \ldots, \mathfrak{A}_k^{k+2}$, $\mathfrak{B}_3$ и $\mathfrak{A}_\varphi$, получим нормальный алгорифм $\mathfrak{B}_4$ над M такой, что

$$\mathfrak{B}_4(\bar{x}_1 * \ldots * \bar{x}_k * \bar{y} * \bar{x}) \simeq \bar{x}_1 * \ldots * \bar{x}_k * \overline{y+1} * \overline{\varphi(x_1, \ldots, x_k, y, x)}.$$

В силу предложения 5.7, существует такой нормальный алгорифм $\mathfrak{B}_4^!$, что при любом $n \geqslant 0$ равенство $\mathfrak{B}_4^!(\bar{n} * P) = Q$ выполнено тогда и только тогда, когда существует последовательность слов $P_0, \ldots, P_n$, удовлетворяющая условиям: $P_0 = P$, $P_n = Q$ и $P_i = \mathfrak{B}_4(P_{i-1})$, где $0 < i \leqslant n$. Тогда алгорифм $\mathfrak{B} = \mathfrak{A}_{k+2}^{k+2} \circ \mathfrak{B}_4^! \circ \mathfrak{B}_2$ и есть тот нормальный алгорифм над M, который вычисляет ψ. В самом деле, прежде всего,

$$\mathfrak{B}_2(\bar{x}_1 * \ldots * \bar{x}_k * \bar{y}) \simeq \bar{y} * \bar{x}_1 * \ldots * \bar{x}_k * \bar{0} * \overline{\tau(x_1, \ldots, x_k)}.$$

Применение затем к слову $\bar{y} * \bar{x}_1 * \ldots * \bar{x}_k * \bar{0} * \overline{\tau(x_1, \ldots, x_k)}$ алгорифма $\mathfrak{B}_4^!$ равносильно, очевидно, y-кратному применению алгорифма $\mathfrak{B}_4$, начиная со слова $\bar{x}_1 * \ldots * \bar{x}_k * \bar{0} * \overline{\tau(x_1, \ldots, x_k)}$. Легко видеть, что при этом в результате получится слово $\bar{x}_1 * \ldots * \bar{x}_k * \bar{y} * \overline{\psi(x_1, \ldots, x_k, y)}$. Применив затем $\mathfrak{A}_{k+2}^{k+2}$, получим окончательно $\overline{\psi(x_1, \ldots, x_k, y)}$.

(4) μ-оператор. Пусть $\psi(x_1, \ldots, x_n) = \mu y(\varphi(x_1, \ldots, x_n, y) = 0)$ и предположим, что некоторый нормальный алгорифм $\mathfrak{A}_\varphi$ над M частично вычисляет φ. Исходя из алгорифмов $\mathfrak{A}_1^{n+1}, \ldots, \mathfrak{A}_n^{n+1}$ и $\mathfrak{A}_N \circ \mathfrak{A}_{n+1}^{n+1}$ в соответствии со следствием 5.2 построим нормальный алгорифм $\mathfrak{W}$ такой,

что $\mathfrak{W}(\bar{x}_1 * \ldots * \bar{x}_n * y) = x_1 * \ldots \bar{x}_n * \overline{y+1}$. Рассмотрим нормальный алгорифм $\mathfrak{D}$ над M, задаваемый схемой

$$\begin{cases} 11 \to \cdot 11 \\ 1 \to \Lambda \end{cases}$$

Если $n=0$, то $\mathfrak{D}(\bar{n}) = \Lambda$, если же $n>0$, то $\mathfrak{D}(\bar{n}) \neq \Lambda$. Пусть $\mathfrak{C} = \mathfrak{D} \circ \mathfrak{A}_\varphi$. Тогда

$$\mathfrak{C}(\bar{x}_1 * \ldots * \bar{x}_n * \bar{y}) \begin{cases} = \Lambda, \text{ если } \varphi(x_1, \ldots, x_n) = 0, \\ \neq \Lambda, \text{ если } \varphi(x_1, \ldots, x_n) \neq 0. \end{cases}$$

Пусть, далее, $\mathfrak{K}$ — нормальный алгорифм над M такой, что

$$\mathfrak{K}(\bar{x}_1 * \ldots * \bar{x}_n) = \bar{x}_1 * \ldots * \bar{x}_n * \bar{0}.$$

Применив к алгорифмам $\mathfrak{W}$ и $\mathfrak{C}$ следствие 5.6, заключаем, что существует нормальный алгорифм $\mathfrak{H}$ над M, для которого равенство $\mathfrak{H}(P) = Q$ выполнено тогда и только тогда, когда имеется последовательность слов $P_0, \ldots, P_n$ $(n \geqslant 0)$, удовлетворяющая условиям: $P_0 = P$, $P_n = Q$, $\mathfrak{C}(P_n) = \Lambda$, $P_{i+1} = \mathfrak{W}(P_i)$ и $\mathfrak{C}(P_i) \neq \Lambda$, где $i = 0, 1, \ldots, n-1$. Определим теперь нормальный алгорифм $\mathfrak{B}$ как композицию $\mathfrak{A}_{n+1}^{n+1} \circ \mathfrak{H} \circ \mathfrak{K}$. Нетрудно видеть, что

$$\mathfrak{B}(\bar{x}_1 * \ldots * \bar{x}_n) \simeq \overline{\mu y (\varphi(x_1, \ldots, x_n, y) = 0)} \simeq \overline{\psi(x_1, \ldots, x_n)}.$$

Из пунктов (1)—(4) следует, что если ψ есть частично рекурсивная функция k аргументов, то существует такой нормальный алгорифм $\mathfrak{A}_\varphi$ над M, что

$$\mathfrak{A}_\psi(\bar{x}_1 * \ldots * \bar{x}_k) \simeq \overline{\psi(x_1, \ldots, x_k)}.$$

Читатель без труда построит схему, задающую нормальный алгорифм $\mathfrak{R}$ над M, который применим только к словам вида $\bar{x}_1 * \ldots * \bar{x}_k$, где $x_1, \ldots, x_k$ — натуральные числа, и который работает таким образом, что $\mathfrak{R}(\bar{x}_1 * \ldots * \bar{x}_k) = \bar{x}_1 * \ldots * \bar{x}_k$. Зададим нормальный алгорифм $\mathfrak{F}_\psi$ равенством $\mathfrak{F}_\psi = \mathfrak{A}_\psi \circ \mathfrak{R}$. Тогда $\mathfrak{F}_\psi(\bar{x}_1 * \ldots * \bar{x}_k) \simeq \overline{\psi(x_1, \ldots, x_k)}$, причем $\mathfrak{F}_\psi$ применим к слову P тогда и только тогда, когда P есть слово в алфавите M вида $\bar{x}_1 * \ldots * \bar{x}_k$ и $\psi(x_1, \ldots, x_k)$ определено. Следовательно, всякая частично рекурсивная функция есть также частичная вычислимая по Маркову функция. Отсюда, в частности, следует, что всякая рекурсивная функция есть функция, вычислимая по Маркову.

Мы теперь определим гёделевы номера для всех букв $S_0, S_1, \ldots$, из которых состоят наши алфавиты: $g(S_i) = 2i+3$. Далее, каждому слову $P = S_{j_0} \ldots S_{j_k}$ припишем гёделев номер

$$g(P) = 2^{g(S_{j_0})} 3^{g(S_{j_1})} \ldots p_k^{g(S_{j_k})} = 2^{2j_0+3} 3^{2j_1+3} \ldots p_k^{2j_k+3},$$

где p_k есть k-е простое число. Положим, кроме того, $g(\Lambda) = 1$. Наконец, гёделев номер последовательности слов $P_0, \ldots, P_k$ определим как $2^{g(P_0)} 3^{g(P_1)} \ldots p_k^{g(P_k)}$.

Условимся обозначать буквы S_1 и S_2 соответственно буквами 1 и $*$. Тогда, рассматривая цифры как слова в алфавите $\{S_1\}$, получаем $g(\bar{0}) = 2^3$, $g(\bar{1}) = 2^3 \cdot 3^3$ и вообще $g(\bar{n}) = \prod_{i=0}^{n} p_i^{\bar{i}}$.

Для всякого алфавита A существуют такие нормальные алгорифмы $\mathfrak{T}_1$ и $\mathfrak{T}_2$ над $A \cup \{1, *\}$, что $\mathfrak{T}_1(P) = \overline{g(P)}$ и $\mathfrak{T}_2(\overline{g(P)}) = P$ для любого слова P в A. Рассмотрим вопрос о существовании алгорифма $\mathfrak{T}_1$. Во-первых, существует такой нормальный алгорифм $\mathfrak{B}_1$ над $M \cup A$, где $M = \{1, *\}$, что для любого непустого слова $P = a_{m_0} a_{m_1} \ldots a_{m_r}$ в алфавите A

$$\mathfrak{B}_1(P) = \overline{g(a_{m_0})} * \overline{g(a_{m_1})} * \ldots * \overline{g(a_{m_r})} \text{ и } \mathfrak{B}_1(a_{m_0}) = \overline{g(a_{m_0})} *.$$

В самом деле, если $A = \{S_{j_0}, \ldots, S_{j_k}\}$, то такой алгорифм $\mathfrak{B}_1$ задается схемой *)

$$\begin{cases} \alpha S_{j_0} \to \overline{2j_0 + 3} * \alpha \\ \alpha S_{j_1} \to \overline{2j_1 + 3} * \alpha \\ \quad \vdots \\ \alpha S_{j_k} \to \overline{2j_k + 3} * \alpha \\ \alpha \to \cdot \Lambda \\ \Lambda \to \alpha \end{cases}$$

Во-вторых, существует такой нормальный алгорифм $\mathfrak{B}_2$, что $\mathfrak{B}_2(\bar{n} * Q) = 0 * \bar{2}^{\bar{n}} * Q$. (Доказательство этого факта предоставляется читателю в качестве упражнения. При этом полезно заметить, что так как функция 2^x рекурсивна, то, в силу предложения 5.8, существует вычисляющий ее нормальный алгорифм.) Положим $\mathfrak{B}_3 = \mathfrak{B}_2 \cdot \mathfrak{B}_1$. Тогда для всякого непустого слова $P = S_{m_0} \ldots S_{m_r}$

$$\mathfrak{B}_3(P) = \bar{0} * \overline{2^{g(S_{m_0})}} * \overline{g(S_{m_1})} * \ldots * \overline{g(S_{m_r})} *.$$

Пусть $\mathfrak{A}$ есть такой нормальный алгорифм, что

$$\mathfrak{A}(\bar{n} * \bar{u} * \bar{v} * Q) = \overline{n+1} * \overline{u \cdot p_{n+1}^{v}} * Q.$$

(Доказательство существования такого $\mathfrak{A}$ мы тоже оставляем на долю читателя. Заметим лишь, что функция $f(x, y, n) = x \cdot p_{n+1}^{y}$ рекурсивна и, следовательно, вычислима с помощью некоторого нормального алгорифма.) Пусть, далее, $\mathfrak{C}$ — нормальный алгорифм, удовлетворяющий условию: $\mathfrak{C}(P) = \Lambda$ тогда и только тогда, когда P содержит в точности два вхождения буквы $*$. В силу следствия 5.6, существует нормальный алгорифм $\mathfrak{H}$, являющийся полным повторением $\mathfrak{A}$, управляемым $\mathfrak{C}$. Обозначим, наконец, через $\mathfrak{E}$ нормальный алгорифм, перерабатывающий всякое слово вида $\bar{x} * \bar{y} *$ в слово $\bar{y}$, и положим $\mathfrak{F} = \mathfrak{E} \cdot \mathfrak{H} \cdot \mathfrak{B}_3$. Нетрудно

*) Здесь следует потребовать, чтобы буква α не входила в алфавит $A \cup M$. (*Прим. перев.*)

убедиться в том, что $\mathfrak{F}(P) = \overline{g(P)}$ для любого непустого слова P в А. Теперь уже существование нормального алгорифма $\mathfrak{T}_1$ над $A \cup M$ такого, что $\mathfrak{T}_1(P) = \overline{g(P)}$ для любого, в том числе и пустого, слова в А, легко следует из предыдущего с помощью предложения 5.4. (Напомним, что $g(\Lambda) = 1$.)

Упражнение

Доказать, что существует такой нормальный алгорифм $\mathfrak{T}_2$ над $A \cup M$, что $\mathfrak{T}_2(\overline{g(P)}) = P$ для любого слова P в А.

Указание. Построить нормальный алгорифм $\mathfrak{D}$, определенный только на словах вида $\overline{2i+3}$, для которых $S_i \in A$, и такой, что $\mathfrak{D}(\overline{2i+3}) = S_i$. Построить нормальный алгорифм $\mathfrak{K}$, определенный только на словах вида $\bar{u}$, где u — положительное натуральное число, и такой, что $\mathfrak{K}(\bar{u}) = \bar{0} * \bar{u} *$. Затем построить нормальный алгорифм $\mathfrak{F}$ такой, что для любых натуральных n и u и для любого слова P

$$\mathfrak{F}(\bar{n} * \bar{u} * P) = \overline{n+1} * \overline{\mathrm{qt}\left(\mathrm{p}_n^{(u)} n,\ u\right)} * P\, \mathfrak{D}(\overline{(u)_n}).$$

Пусть $\mathfrak{C}$ — нормальный алгорифм такой, что $\mathfrak{C}(\bar{n} * \bar{1} * P) = \Lambda$ для любого P и любого целого неотрицательного n, определенный также и для слов вида, отличного от $\bar{n} * \bar{1} * P$, но со значением, отличным от Λ. В силу предложения 5.5, существует нормальный алгорифм $\mathfrak{R}$, осуществляющий повторение $\mathfrak{F}$, управляемое $\mathfrak{C}$. Пусть $\mathfrak{G}$ — нормальный алгорифм, перерабатывающий всякое слово вида $\bar{n} * \bar{1} * P$ в слово P. Положить $\mathfrak{L} = \mathfrak{G} \cdot \mathfrak{R} \cdot \mathfrak{K}$. Показать, что $\mathfrak{L}(\overline{g(Q)}) = Q$ для любого непустого слова Q в А. В заключение с помощью предложения 5.4 учесть случай пустого Q.

Пусть $\mathfrak{A}$ — произвольный алгорифм (не обязательно нормальный) над алфавитом А. Поставим в соответствие алгорифму $\mathfrak{A}$ частичную функцию $\psi_{\mathfrak{A}}$, удовлетворяющую следующему условию: для любых натуральных чисел n и m равенство $\psi_{\mathfrak{A}}(n) = m$ выполнено тогда и только тогда, когда либо n не есть гёделев номер никакого слова в алфавите А и $m = 0$, либо n и m суть гёделевы номера некоторых слов P и Q в А, причем $\mathfrak{A}(P) = Q$. Предположим, что функция $\psi_{\mathfrak{A}}$ частично рекурсивна (в этом случае мы назовем $\mathfrak{A}$ *рекурсивным алгорифмом*). В силу предложения 5.8, тогда существует такой нормальный алгорифм $\mathfrak{B}$ над алфавитом $M = \{1, *\}$, что $\mathfrak{B}(\bar{n}) \simeq \overline{\psi_{\mathfrak{A}}(n)}$ для любого натурального n, причем $\mathfrak{B}$ определен только для тех $\bar{n}$, для которых определено $\psi_{\mathfrak{A}}(n)$. Пусть $\mathfrak{A}' = \mathfrak{T}_2 \cdot \mathfrak{B} \cdot \mathfrak{T}_1$. Нетрудно видеть, что $\mathfrak{A}'$ есть нормальный алгорифм над алфавитом А, вполне эквивалентный алгорифму $\mathfrak{A}$ относительно А. Таким образом, верно следующее

Предложение 5.9. *Если алгорифм* $\mathfrak{A}$ *над алфавитом* А *таков, что функция* $\psi_{\mathfrak{A}}$ *частично рекурсивна, то существует нормальный алгорифм над алфавитом* А, *вполне эквивалентный алгорифму* $\mathfrak{A}$ *относительно* А.

Предложение 5.10. *Если* $\mathfrak{A}$ *есть нормальный алгорифм над алфавитом* А, *то* $\psi_{\mathfrak{A}}$ *есть частично рекурсивная функция; если,*

кроме того, $\mathfrak{A}$ применим ко всякому слову в алфавите A, *то функция $\psi_{\mathfrak{A}}$ рекурсивна.*

Доказательство. Назовем индексом простой формулы подстановки $P \to Q$ число $2^1 \cdot 3^{g(P)} \cdot 5^{g(Q)}$ и индексом заключительной формулы подстановки — число $2^2 \cdot 3^{g(P)} \cdot 5^{g(Q)}$. Назовем, далее, индексом схемы алгорифма $P_0 \to (\cdot) Q_0, \ldots, P_r \to (\cdot) Q_r$ число $2^{k_0} 3^{k_1} \ldots p_r^{k_r}$, где k_i — индекс формулы подстановки $P_i \to (\cdot) Q_i$.

Введем следующие рекурсивные предикаты:

(1) Word (u): $u = 1 \vee \forall z\,(z < lh\,(u) \supset \exists y\,(y < u \,\&\, (u)_z = 2y + 3))$ («u есть гёделев номер некоторого слова»).

(2) SI (u): $lh\,(u) = 3 \,\&\, (u)_0 = 1 \,\&$ Word $((u)_1) \,\&$ Word $((u)_2)$ («u есть индекс простой формулы подстановки»).

(3) TI (u): $lh\,(u) = 3 \,\&\, (u)_0 = 2 \,\&$ Word $((u)_1) \,\&$ Word $((u)_2)$ («u есть индекс заключительной формулы подстановки»).

(4) Ind (u): $u > 1 \,\&\, \forall z\,(z < lh\,(u) \supset$ SI $((u)_z) \vee$ TI $((u)_z))$ («u есть индекс схемы алгорифма»).

Обозначим через $x \square y$ рекурсивную функцию, которую в главе 3 стр. 142 (4)) мы обозначали через $x * y$. Тогда если $x = \prod_{i=0}^{n} p_i^{\alpha_i}$, где $\alpha_i > 0$ ($i = 0, 1, \ldots, n$), и если $y = \prod_{i=0}^{m} p_i^{\beta_i}$, то $x \square y = \prod_{i=0}^{n} p_i^{\alpha_i} \cdot \prod_{i=0}^{m} p_{i+n+1}^{\beta_i}$. Кроме того, $x \square 1 = 1 \square x = x$. Операция $\square$ соответствует операции соединения слов.

(5) Lsub (x, y, e): «e есть индекс некоторой формулы подстановки $P \to (\cdot) Q$, а x и y суть гёделевы номера некоторых слов U и V таких, что P входит в U и V есть результат подстановки Q на место самого левого вхождения P в U», т. е. Word (x) & Word (y) & (SI (e) $\vee$ TI (e)) & $\& \exists u_{u \leqslant x} \exists v_{v \leqslant x}\,(x = u \square (e)_1 \square v \,\&\, y = u \square (e)_2 \square v \,\&\, \neg \exists w_{w \leqslant x} \exists z_{z \leqslant x}\,(x = w \square (e)_1 \square z \,\&\, w < u))$.

(6) Occ (x, y): «x и y суть гёделевы номера соответственно некоторых слов U и V и слово V входит в слово U», т. е. Word (x) & & Word (y) & $\exists v_{v \leqslant x} \exists z_{z \leqslant x}\,(x = v \square y \square z)$.

(7) End (e, z): «z есть гёделев номер некоторого слова P, e есть индекс некоторой схемы, и определяемый этой схемой алгорифм неприменим к слову P», т. е. Ind (e) & Word (z) & $\forall w_{w < lh\,(e)}\,(\neg$ Occ $(z, ((e)_w)_1))$.

(8) SCons (e, y, x): «e есть индекс некоторой схемы $\mathscr{S}$, а y и x суть гёделевы номера некоторых слов V и U таких, что V может быть получено применением к U некоторой простой формулы подстановки схемы $\mathscr{S}$», т. е. Ind (e) & Word (x) & Word (y) & $\exists v_{v < lh\,(e)}$ (SI $((e)_v)$ & & Lsub (x, y, $(e)_v$) & $\forall z_{z < v}(\neg$ Occ (x, $((e)_z)_1))))$.

(9) TCons (e, y, x): аналогично S Cons (e, y, x) с заменой SI $((e)_v)$ на TI $((e)_v)$ (т. е. слов «простой формулы подстановки» словами «заключительной формулы подстановки»).

(10) Der (e, x, y): «e есть индекс некоторой схемы $\mathscr{S}$, x есть гёделев номер некоторого слова U_0 и y есть гёделев номер последовательности слов $U_0, U_1, \ldots, U_k$ $(k \geqslant 0)$ такой, что если $0 \leqslant i < k \dot{-} 1$, то задаваемый схемой $\mathscr{S}$ алгорифм $\mathfrak{A}$ переводит U_i в U_{i+1}, и либо $\mathfrak{A}\colon U_{k \dot{-} 1} \vdash \cdot\, U_k$, либо $\mathfrak{A}\colon U_{k \dot{-} 1} \vdash U_k$ и $\mathfrak{A}\colon U_k \sqsupset$ (либо если $k = 0$, то $\mathfrak{A}\colon U_k \sqsupset$), т. е. Ind (e) & Word (x) & $\forall z_{z < \mathrm{lh}(y)}$ (Word $((y)_z)$ & $(y)_0 =$ x& & $\forall z_{z < \mathrm{lh}(y) \dot{-} 2}$ (SCons (e, $(y)_{z+1}$, $(y)_z$)) & (lh (y) = 1 & End (e, $(y)_0$)) $\vee$ (lh (y) $>$ $>$ 1 & (TCons (e, $(y)_{\mathrm{lh}(y) \dot{-} 1}$, $(y)_{\mathrm{lh}(y) \dot{-} 2}$) $\vee$ (SCons (e, $(y)_{\mathrm{lh}(y) \dot{-} 1}$, $(y)_{\mathrm{lh}(y) \dot{-} 2}$) & & End (e, $(y)_{\mathrm{lh}(y) \dot{-} 1}$))))).

(11) W_A (u): «u есть гёделев номер слова в данном алфавите A = $= \{S_{j_0}, \ldots, S_{j_m}\}$», т. е.

$$u = 1 \vee \forall z_{z < \mathrm{lh}(u)} ((u)_z = 2j_0 + 3 \vee \ldots \vee (u)_z = 2j_m + 3).$$

Пусть теперь $\mathfrak{A}$ — произвольный нормальный алгорифм над алфавитом A и e — индекс схемы, которой он задается. Рассмотрим частично рекурсивную функцию $\varphi(x) = \mu y ((W_A(x) \,\&\, \mathrm{Der}(e, x, y)) \vee \neg W_A(x))$. Как нетрудно видеть $\psi_{\mathfrak{A}}(x) = (\varphi(x))_{\mathrm{lh}(\varphi(x)) \dot{-} 1}$, откуда следует, что $\psi_{\mathfrak{A}}$ есть частично рекурсивная функция. Если же при этом алгорифм $\mathfrak{A}$ применим к каждому слову в A, то функция φ, а вместе с ней и функция $\psi_{\mathfrak{A}}$ рекурсивны.

Упражнение

Пусть задан алфавит A. Показать, что существует нормальный алгорифм $\mathfrak{B}$ над $A \cup M$ такой, что для любого нормального алгорифма $\mathfrak{A}$ в A, задаваемого схемой с индексом e, и для любого слова P в A выполнено условное равенство $\mathfrak{B}(\overline{e} * P) \simeq \mathfrak{A}(P)$. Алгорифм $\mathfrak{B}$ называется *универсальным* алгорифмом для алфавита A.

Следствие 5.11. *Если данная частичная функция φ является частично вычислимой по Маркову, то она есть функция частично рекурсивная, если же φ есть функция, вычислимая по Маркову, то функция φ рекурсивна.*

Доказательство. Пусть $\mathfrak{A}$ — нормальный алгорифм над M такой, что $\varphi(n_1, \ldots, n_k) = m$ тогда и только тогда, когда $\mathfrak{A}(\overline{(n_1, \ldots, n_k)}) = \overline{m}$. Функция $\psi_{\mathfrak{A}}$ частично рекурсивна. Положим $\tau(n) = g(\overline{n})$. Функция τ рекурсивна, так как $g(\overline{n}) = g(1^{n+1}) = \prod_{i=0}^{n} (p_i)^5$ *).

*) Здесь автором вводится обозначение 1^k для слова $\underbrace{1 \ldots 1}_{k \text{ раз}}$. *(Прим. перев.)*

Функция $\gamma(x) = \mathrm{lh}(x) \dot{-} 1$ также рекурсивна. Если $x = \prod_{i=0}^{n} (p_i)^{5}$, то $n = \gamma(x)$. Рекурсивна, очевидно, и функция

$$\xi(n_1, \ldots, n_k) = g(\overline{(n_1, \ldots, n_k)}) = g(1^{n_1+1} * 1^{n_2+1} * \ldots * 1^{n_k+1}) =$$
$$= \left[\prod_{i=0}^{n_1+1} (p_i)^{5}\right] \cdot (p_{n_1+2})^{7} \cdot \left[\prod_{i=0}^{n_2+1} (p_{i+n_1+3})^{5}\right] \cdot (p_{n_1+n_2+5})^{7} \cdot \ldots$$
$$\ldots \cdot (p_{(n_1+\ldots+n_{k-1}+2k \dot{-} 3)})^{7} \cdot \left[\prod_{i=0}^{n_k+1} (p_{i+n_1+\ldots+n_{k-1}+2k \dot{-} 2})^{5}\right].$$

Тогда функция $\varphi = \gamma \circ \psi_{\mathfrak{A}} \circ \xi$ является частично рекурсивной. Если функция φ вычислима по Маркову, то можно предполагать, что алгорифм $\mathfrak{A}$ применим к любому слову в M (схему алгорифма $\mathfrak{A}$ можно изменить таким образом, чтобы он всякое слово в M, не имеющее вида $\bar{n}_1 * \ldots * \bar{n}_k$, перерабатывал в Λ). Тогда, в силу предложения 5.10, функция $\psi_{\mathfrak{A}}$ рекурсивна, а вместе с ней рекурсивна и функция $\varphi = \gamma \circ \psi_{\mathfrak{A}} \circ \xi$.

Упражнение

Показать, что всюду определенная частично рекурсивная функция рекурсивна.

Итак, следствие 5.11 и предложение 5.8 устанавливают эквивалентность понятий частичной вычислимости по Маркову и частичной рекурсивности (а также вычислимости по Маркову и рекурсивности). Тезис Чёрча утверждает в свою очередь, что понятие вычислимости эквивалентно понятию рекурсивности (а в расширенной формулировке — что понятие частичной эффективной вычислимости эквивалентно понятию частичной рекурсивности). А. А. Марков в терминах алгорифмов сформулировал соответствующий принцип, названный им *принципом нормализации*: всякий алгорифм в A вполне эквивалентен относительно A некоторому нормальному алгорифму над A. Оказывается, что тезис Чёрча и принцип нормализации эквивалентны. В самом деле, примем сначала тезис Чёрча. Пусть $\mathfrak{A}$ есть алгорифм в алфавите A. Соответствующая функция $\psi_{\mathfrak{A}}$ является частичной эффективно вычислимой функцией. Тогда, в силу тезиса Чёрча, $\psi_{\mathfrak{A}}$ есть частично рекурсивная функция и, следовательно, алгорифм $\mathfrak{A}$, на основании предложения 5.9, вполне эквивалентен относительно A некоторому нормальному алгорифму над A. Таким образом, если верен тезис Чёрча, то верен и принцип нормализации. Обратно, пусть верен принцип нормализации, и пусть φ — произвольная частичная эффективно вычислимая функция. Пусть, далее, $\mathfrak{B}_{\varphi}$ — соответствующий алгорифм в M. Согласно принципу

нормализации, $\mathfrak{B}_\varphi$ вполне эквивалентен относительно M некоторому нормальному алгорифму над M. Следовательно, функция φ есть частичная вычислимая по Маркову функция. Но тогда, в силу следствия 5.11, φ является функцией частично рекурсивной, и мы вывели, таким образом, из принципа нормализации тезис Чёрча.

Разумеется, ввиду неточности интуитивных понятий алгорифма и эффективно вычислимой функции невозможно *доказать* верность принципа нормализации Маркова или тезиса Чёрча. Не располагаем мы и какими-либо априорными доводами в пользу этих гипотез. Нет никаких бесспорных оснований считать, что применение одних лишь формул подстановки может заменить любые эффективные операции. Здесь можно рассчитывать только на неполное подтверждение, а не на строгое доказательство. Очевидно, что всякая частично рекурсивная функция является частичной эффективно вычислимой функцией *). Обратное утверждение, а именно, что всякая частичная эффективно вычислимая функция является частично рекурсивной (или что всякий алгорифм в алфавите A вполне эквивалентен относительно A некоторому нормальному алгорифму), подтверждается для всех известных частичных эффективно вычислимых функций. Есть некоторое дополнительное обстоятельство, говорящее в пользу тезиса Чёрча, а именно, тот удивительный факт, что самые разнородные подходы к уточнению понятия частичной эффективно вычислимой функции привели к эквивалентным определениям. Мы это уже видели в отношении частично рекурсивных и частичных вычислимых по Маркову функций. Ниже будет показано, что к тому же самому результату приводят и другие подходы — Тьюринга, Эрбрана и Гёделя. Теория *λ-вычислимости* Чёрча [1941] и теория нормальных систем Поста [1943] также ведут к понятиям, эквивалентным понятиям частично рекурсивной функции или нормального алгорифма. (Доводы в пользу тезиса Чёрча подробнее рассмотрены у Клини [1952], §§ 62, 70. См. также Гермес [1961].)

Упражнения

1. Доказать, что принцип нормализации эквивалентен утверждению, что всякий алгорифм в алфавите A эквивалентен относительно A некоторому нормальному алгорифму над A.

2. Пусть B и $A=\{a_1, \ldots, a_k\}$ — алфавиты без общих букв и b, c — различные буквы, не принадлежащие $B \cup A$. Для всякой буквы a определим a^i как сокращенную запись слова $\underbrace{aa \ldots a}_{i \text{ раз}}$. *Переводом* $T(a_i)$ буквы a_i назовем

*) Читателю следует иметь в виду, что эффективная вычислимость вовсе не подразумевает фактическую вычислимость. Эффективная вычислимость функции означает лишь, что каждое ее значение может быть вычислено в некоторое конечное число шагов, согласно некоторому фиксированному предписанию. При этом вычисления, необходимые для получения значений, например частично рекурсивных функций, могут заключать в себе такое огромное число шагов, что для их выполнения не хватило бы всего времени существования человечества.

слово cb^ic, а переводом $T(u)$ всякой буквы u из B будем считать саму эту букву. Перевод $T(P)$ всякого непустого слова $P = d_1 \ldots d_n$ в $B \cup A$ определим как слово $T(d_1) \ldots T(d_n)$, а если $P = \Lambda$, то положим $T(P) = \Lambda$. Отметим, что $T(P) = P$ для любого слова P в B.

(a) Показать, что схема

$$\begin{cases} \alpha\xi \to T(\xi)\,\alpha & (\xi \in B \cup A) \\ \alpha \to \cdot\,\Lambda \\ \Lambda \to \alpha \end{cases}$$

где α не принадлежит $B \cup A \cup \{b, c\}$, определяет нормальный алгорифм $\mathfrak{T}$ такой, что $\mathfrak{T}(P) = T(P)$ для любого слова P в $B \cup A$.

(b) Построить схему для нормального алгорифма $\mathfrak{B}$ над $B \cup A \cup \{b, c\}$ такого, что $\mathfrak{B}(T(P)) = P$ для любого слова P в $B \cup A$.

(c) Пусть $\mathfrak{G}$ — нормальный алгорифм в $B \cup A$. Для всякой формулы подстановки $P \to (\cdot)\,Q$ из схемы алгорифма $\mathfrak{G}$ определим ее перевод как формулу подстановки $T(P) \to (\cdot)\,T(Q)$. Схема, получающаяся из схемы для $\mathfrak{G}$ путем замены в этой последней всякой формулы подстановки ее переводом, определяет некоторый нормальный алгорифм $T(\mathfrak{G})$ в $B \cup \{b, c\}$. Показать, что $(T(\mathfrak{G}))(\mathfrak{T}(P)) \simeq \mathfrak{T}(\mathfrak{G}(P))$, где $\mathfrak{T}$ — нормальный алгорифм из (a).

(d) Доказать, что всякий нормальный алгорифм над B вполне эквивалентен относительно B некоторому нормальному алгорифму в $B \cup \{b, c\}$. (На самом деле вместо двух можно всегда обойтись и всего лишь одной дополнительной буквой. Это доказал Н. М. Нагорный [1953]. Там же им показано, что существует нормальный алгорифм над B, а именно, *удваивающий алгорифм* (упражнение 2(b), стр. 233), который не эквивалентен относительно B никакому нормальному алгорифму в B. Доказательство этого последнего утверждения мы оставляем читателю в качестве легкого упражнения.)

§ 2. Алгорифмы Тьюринга

Стремясь найти точное определение понятия эффективной вычислимости, Тьюринг [1936] выделил некоторый класс абстрактных машин, о которых высказал предположение, что они пригодны для осуществления любой «механической» вычислительной процедуры. Эти машины называют теперь в честь их изобретателя *машинами Тьюринга*. Мы приступаем к их описанию.

Пусть имеется *лента*, потенциально бесконечная в обе стороны и разделенная на квадраты. Потенциальная бесконечность ленты понимается в том смысле, что в каждый данный момент времени она имеет

...			S_2	S_1	S_1	S_0		S_3					...

конечную длину, и вместе с тем к ней всегда как слева, так и справа могут быть добавлены новые квадраты. Имеется некоторое конечное множество *символов ленты* $S_0, \ldots, S_n$, называемое *алфавитом* машины. В каждый момент времени каждый квадрат может быть занят не более чем одним символом. Машина обладает некоторым конечным множеством *внутренних состояний* $\{q_0, q_1, \ldots, q_m\}$. В каждый данный момент времени машина находится в точности только в одном из этих состояний. Наконец, имеется *читающая головка*, которая в каждый данный

момент времени находится на одном из квадратов ленты. Машина действует не непрерывно, а лишь в дискретные моменты времени. Если в какой-то момент t читающая головка воспринимает квадрат (т. е. стоит на квадрате), содержащий символ S_i, и машина находится во внутреннем состоянии q_j, то действие машины определено, и она совершит один из следующих четырех актов: (1) головка стирает символ S_i и записывает на том же квадрате новый символ S_k, (2) головка перемещается в соседний слева квадрат, (3) головка перемещается в соседний справа квадрат, (4) машина останавливается. В случаях (1) — (3) машина переходит в новое внутреннее состояние q_r и готова снова к действию в следующий момент $t+1$. Будем предполагать, что символ S_0 представляет пустой квадрат, и что, следовательно, читающая головка всегда воспринимает какой-нибудь символ. Первые три из возможных актов действия машины могут быть описаны соответственно следующими упорядоченными четверками, которые мы в дальнейшем будем называть *командами*: (1) $q_jS_iS_kq_r$, (2) $q_jS_iLq_r$, (3) $q_jS_iRq_r$. Здесь первые два символа — это соответственно внутреннее состояние машины и воспринимаемый символ, третий символ представляет действие машины (написание головкой символа S_k или перемещение головки на один квадрат влево, или перемещение головки на один квадрат вправо), четвертый символ — новое внутреннее состояние машины, в котором она находится после данного акта действия.

Если лента вложена в машину Тьюринга, читающая головка машины помещена на один из квадратов ленты и машина приведена в одно из своих внутренних состояний, то машина начинает оперировать на ленте: ее головка пишет и стирает символы и перемещается из одного квадрата в другой — соседний. Если при этом машина когда-нибудь останавливается, то находящаяся в ней в момент остановки лента называется результатом применения машины к данной ленте.

Мы можем теперь с каждой машиной Тьюринга T связать некоторый алгорифм $\mathfrak{B}$ в алфавите A машины T. Возьмем произвольное слово P в алфавите A и запишем его слева направо в квадратах чистой ленты. Поместим эту ленту в машину таким образом, чтобы читающая головка воспринимала самый левый квадрат, и приведем машину во внутреннее состояние q_0. Машина начинает работать. Если она когда-нибудь остановится, то появившееся в результате на ленте слово в A является значением алгорифма $\mathfrak{B}$. Такой алгорифм $\mathfrak{B}$ называется *алгорифмом Тьюринга*. (Слово, объявляемое значением алгорифма $\mathfrak{B}$, определяется как последовательность символов, оказавшихся, считая в порядке слева направо, на ленте в момент прекращения работы машины. Напомним, что пустые квадраты ленты, которые могут при этом встретиться, считаются заполненными символом S_0.) Мы еще пока не уточнили того, как машина узнает, когда ей следует остановиться. Ниже это будет сделано.

Дадим теперь точное определение. *Машиной Тьюринга* называется всякое конечное множество T упорядоченных четверок символов, удов-

летворяющее условиям: (i) каждая входящая в T четверка принадлежит к одному из трех типов: (1) $q_jS_iS_kq_r$, (2) $q_jS_iLq_r$, (3) $q_jS_iRq_r$, (ii) никакие две четверки из T не имеют совпадающими первые два символа. Упорядоченные четверки указанных типов называются *командами*. Множество всех символов типа S_m, входящих в команды из T, называется *алфавитом* машины T. Входящие в эти команды символы q_s называются *внутренними состояниями* машины T. Потребуем дополнительно, чтобы q_0 было внутренним состоянием каждой машины Тьюринга.

Назовем *конфигурацией* машины T всякое слово вида Pq_sQ, где P — слово (возможно пустое) в алфавите машины T, q_s — какое-нибудь внутреннее состояние T и Q — непустое слово в алфавите машины T *). Скажем, что *машина* T *переводит конфигурацию* α *в конфигурацию* β (сокращенно: $\alpha \xrightarrow{T} \beta$), если либо a) α имеет вид Pq_jS_iQ, β имеет вид Pq_rS_kQ и $q_jS_iS_kq_r$ есть одна из команд T; либо b) α имеет вид $PS_sq_jS_iQ$, β имеет вид $Pq_rS_sS_iQ$ и $q_jS_iLq_r$ есть одна из команд T; либо c) α имеет вид q_jS_iQ, β имеет вид $q_rS_0S_iQ$ и команда $q_jS_iLq_r$ принадлежит T; либо d) α имеет вид $Pq_jS_iS_kQ$, β имеет вид $PS_iq_rS_kQ$ и команда $q_jS_iRq_r$ принадлежит T; либо e) α имеет вид Pq_jS_i, β имеет вид $PS_iq_rS_0$ и $q_jS_iRq_r$ входит в число команд T **). Мы будем говорить, что машина *останавливается при конфигурации* α, если не существует такой конфигурации β, что $\alpha \xrightarrow{T} \beta$. (Это происходит в том случае, когда q_jS_i входит в α, а среди команд, определяющих T, нет такой, которая начиналась бы с q_jS_i.)

Вычисление машины T есть всякая конечная последовательность конфигураций $\alpha_0, \ldots, \alpha_m$ $(m \geqslant 0)$ такая, что входящее в α_0 внутреннее состояние есть q_0; $\alpha_i \xrightarrow{T} \alpha_{i+1}$ для $i = 0, 1, \ldots, m-1$ и T останавливается при α_m. Будем говорить, что данное вычисление $\alpha_0, \ldots, \alpha_m$ начинается с α_0 и заканчивается α_m. Пусть C — алфавит, содержащий в себе алфавит A машины T. Определим алгорифм $\mathfrak{B}_{T,C}$ в C следующим образом: для любых слов P и Q в C равенство $\mathfrak{B}_{T,C}(P) = Q$ имеет место тогда и только тогда, когда существует вычисление машины T, начинающееся с конфигурации q_0P и заканчивающееся конфигурацией вида $R_1q_jR_2$, где $R_1R_2 = Q$. Алгорифм $\mathfrak{A}$ в алфавите D называется вычислимым по

---

*) С помощью конфигурации описывается состояние машины и ленты в данный момент времени: буквы конфигурации, отличные от q_s, суть символы, заполняющие в данный момент в том же порядке, что и в конфигурации, квадраты ленты; q_s — внутреннее состояние машины в данный момент; первая, следующая в конфигурации за q_s буква есть символ, стоящий в том квадрате, который в тот же момент воспринимает читающая головка машины.

**) В соответствии с содержательной картиной дела, «T переводит α в β» означает, что если α описывает состояние ленты и машины T в момент времени t, то β делает то же для момента $t+1$. Заметим также, что в соответствии с содержательным смыслом случая c), если головка подходит к левому краю ленты и получает приказ двигаться дальше влево, то машина присоединяет к ленте слева новый «пустой» квадрат. (Аналогично в случае e) пустой квадрат присоединяется к ленте справа.)

Тьюрингу, если существуют машина Тьюринга T с алфавитом A и алфавит C, содержащий A ∪ D, такие, что алгорифмы $\mathfrak{B}_{T,C}$ и $\mathfrak{A}$ вполне эквивалентны относительно D.

Будем, как и прежде, писать 1 вместо S_1. Вспомним также, что $\bar{m}$ для любого натурального m обозначает у нас слово 1^{m+1}. Пусть, кроме того, $*$ обозначает S_2. Мы будем говорить, что машина Тьюринга T (с алфавитом A, включающим 1 и $*$) *вычисляет* частичную арифметическую функцию $f(x_1, \ldots, x_n)$, если для любых натуральных $k_1, \ldots, k_n$ и для любого слова Q равенство $\mathfrak{B}_{T,C}(\bar{k}_1 * \ldots * \bar{k}_n) = Q$ справедливо тогда и только тогда, когда существуют такие слова R_1 и R_2 в алфавите $\{S_0\}$, что $Q = R_1\overline{f(k_1, \ldots, k_n)}R_2$. (Форма $R_1\overline{f(k_1, \ldots, k_n)}R_2$ для Q допускается в связи с тем, что S_0 интерпретируется как изображение пустого квадрата ленты.) Функция называется *вычислимой по Тьюрингу*, если существует машина Тьюринга, вычисляющая эту функцию.

Примеры. 1. Рассмотрим машину Тьюринга T, определяемую следующими командами:

$$q_0 \quad 1 \quad L \quad q_1$$
$$q_1 \quad S_0 \quad 1 \quad q_2$$

Алфавит машины T состоит из 1 и S_0. T вычисляет функцию N (прибавление единицы). В самом деле, нетрудно видеть, что $q_0\bar{k} \underset{T}{\rightarrow} q_1S_0\bar{k} \underset{T}{\rightarrow} q_2\overline{k+1}$. Вообще, машина T переводит любую конфигурацию вида $q_0 1P$ в конфигурацию $q_0 11P$, а всякое слово P, не начинающееся с буквы 1, она переводит в P.

2. Машина, определенная командами

$$q_0 \quad 1 \quad L \quad q_1$$
$$q_1 \quad S_0 \quad 1 \quad q_0,$$

начав работу со слова вида $1P$, приписывает к нему слева по одной букве 1 на каждом шаге, никогда при этом не останавливаясь

3. Читающая головка машины Тьюринга, задаваемой командами

$$q_0 \quad S_0 \quad R \quad q_0$$
$$q_0 \quad S_2 \quad R \quad q_0$$
$$\vdots$$
$$q_0 \quad S_k \quad R \quad q_0$$
$$q_0 \quad 1 \quad 1 \quad q_1$$

двигается по ленте вправо, пока не встретит вхождение (если такое вообще имеется) символа 1, после чего машина останавливается.

4. Построим машину Тьюринга, вычисляющую функцию $x + y$. Пусть T есть машина Тьюринга, заданная системой команд

$$\begin{array}{cccc} q_0 & 1 & S_0 & q_0 \\ q_0 & S_0 & R & q_1 \\ q_1 & 1 & R & q_1 \\ q_1 & * & 1 & q_2 \\ q_2 & 1 & R & q_2 \\ q_2 & S_0 & L & q_3 \\ q_3 & 1 & S_0 & q_3 \end{array}$$

Тогда

$$q_0\bar{m} * \bar{n} = q_0 1^{m+1} * 1^{n+1} \underset{T}{\rightarrow} q_0 S_0 1^m * 1^{n+1} \underset{T}{\rightarrow} S_0 q_1 1^m * 1^{n+1} \underset{T}{\rightarrow}$$
$$\underset{T}{\rightarrow} S_0 1 q_1 1^{m-1} * 1^{n+1} \underset{T}{\rightarrow} \ldots \underset{T}{\rightarrow} S_0 1^m q_1 * 1^{n+1} \underset{T}{\rightarrow} S_0 1^m q_2 1 1^{n+1} \underset{T}{\rightarrow}$$
$$\underset{T}{\rightarrow} S_0 1^{m+1} q_2 1^{n+1} \underset{T}{\rightarrow} S_0 1^{m+1} 1 q_2 1^n \underset{T}{\rightarrow} \ldots \underset{T}{\rightarrow} S_0 1^{m+1} 1^{n+1} q_2 S_0 \underset{T}{\rightarrow} S_0 1^{m+1} 1^n q_3 1 S_0 \underset{T}{\rightarrow}$$
$$\underset{T}{\rightarrow} S_0 1^{m+1} 1^n q_3 S_0 S_0 = S_0 1^{m+n+1} q_3 S_0 S_0 = S_0 \overline{m+n} q_3 S_0 S_0.$$

Упражнения

1. Показать, что функция $m \dot{-} n$ вычислима по Тьюрингу.

2. Показать, что исходные примитивно рекурсивные функции $U_i^n(x_1, \ldots, x_n)$ вычислимы по Тьюрингу. (Дальнейшие примеры см. Девис [1958], гл. I.)

Предложение 5.12. *Пусть* T — *машина Тьюринга с алфавитом* A *и* C — *расширение* A. *Тогда существует нормальный алгорифм* $\mathfrak{A}$ *над* C, *вполне эквивалентный относительно* C *алгорифму Тьюринга* $\mathfrak{B}_{T,C}$.

Доказательство. Пусть $D = C \cup \{q_{k_0}, \ldots, q_{k_m}\}$, где $q_{k_0}, \ldots, q_{k_m}$ — внутренние состояния T и $q_{k_0} = q_0$. Построим схему для искомого алгорифма $\mathfrak{A}$ следующим образом. Выпишем сначала для всех команд $q_j S_i S_k q_r$ машины Тьюринга T формулы подстановки $q_j S_i \to q_r S_k$. Затем для каждой команды $q_j S_i L q_r$ выпишем всевозможные формулы подстановки вида $S_l q_j S_i \to q_r S_l S_i$, где $S_l \in C$, и формулу подстановки $q_j S_i \to q_r S_0 S_i$. Далее для каждой команды $q_j S_i R q_r$ выпишем всевозможные формулы подстановки $q_j S_i S_l \to S_i q_r S_l$, где $S_l \in C$, и формулу подстановки $q_j S_i \to S_i q_r S_0$. Наконец, выпишем всевозможные формулы подстановки $q_{k_i} \to \Lambda$, где $q_{k_i} \in D$, и формулу подстановки $\Lambda \to q_0$. Полученная таким образом схема определяет некоторый алгорифм $\mathfrak{A}$ над C, и легко показать, что $\mathfrak{B}_{T,C}(P) \simeq \mathfrak{A}(P)$ для любого слова P в C, т. е. $\mathfrak{A}$ есть искомый алгорифм.

Следствие 5.13. *Всякая вычислимая по Тьюрингу функция* f *является частичной вычислимой по Маркову функцией; следовательно, в силу следствия* 5.11, f *есть частично рекурсивная функция, и если при этом* f *определена всюду, то она рекурсивна.*

Доказательство. Пусть функция $f(x_1, \ldots, x_n)$ вычислима по Тьюрингу и ее вычисляет машина Тьюринга T с алфавитом $A \supseteq \{1, *\}$. Это означает, что для любых натуральных чисел $k_1, \ldots, k_n$ найдутся такие слова R_1 и R_2 (возможно, пустые) в алфавите $\{S_0\}$, что $\mathfrak{B}_{T, A}(\bar{k}_1 * \ldots * \bar{k}_n) \simeq R_1 \overline{f(k_1, \ldots, k_n)} R_2$. В силу предложения 5.12, существует нормальный алгорифм $\mathfrak{A}$ над A, вполне эквивалентный относительно A алгорифму $\mathfrak{A}_{T, A}$. Пусть $\mathfrak{C}_1$ — нормальный алгорифм над $\{1, *, S_0\}$, стирающий все вхождения S_0 перед первым вхождением 1 или $*$ во всяком слове в алфавите $\{1, *, S_0\}$. Такой алгорифм можно задать схемой

$$\begin{cases} \alpha S_0 \to \alpha \\ \alpha 1 \to \cdot 1 \\ \alpha * \to \cdot * \\ \alpha \to \cdot \Lambda \\ \Lambda \to \alpha \end{cases}$$

Пусть также $\mathfrak{C}_2$ — нормальный алгорифм над $\{1, *, S_0\}$, который стирает все вхождения S_0 после последнего вхождения 1 или $*$ во всяком слове в алфавите $\{1, *, S_0\}$. $\mathfrak{C}_2$ можно задать схемой

$$\begin{cases} \alpha * \to * \alpha \\ \alpha 1 \to 1 \alpha \\ \alpha S_0 \to \alpha \\ \alpha \to \cdot \Lambda \\ \Lambda \to \alpha \end{cases}$$

Положим теперь $\mathfrak{C} = \mathfrak{C}_2 \cdot \mathfrak{C}_1 \cdot \mathfrak{A}$. Для любых натуральных $k_1, \ldots, k_n$ имеем

$$\mathfrak{A}(k_1 * \ldots * k_n) \simeq \mathfrak{B}_{T, A}(\bar{k}_1 * \ldots * k_n) \simeq R_1 \overline{f(k_1, \ldots, k_n)} R_2,$$

где R_1 и R_2 — некоторые слова в $\{S_0\}$ Поэтому

$$\mathfrak{C}_1(R_1 \overline{f(k_1, \ldots, k_n)} R_2) \simeq \overline{f(k_1, \ldots, k_n)} R_2$$

и

$$\mathfrak{C}_2(\overline{f(k_1, \ldots, k_n)} R_2) \simeq \overline{f(k_1, \ldots, k_n)}.$$

Отсюда видно, что f есть частичная вычислимая по Маркову функция; ее вычисляет нормальный алгорифм $\mathfrak{C}$

Предложение 5.14. *Пусть* $\mathfrak{A}$ — *нормальный алгорифм в алфавите* A, *не содержащем* S_0 *и* δ *Тогда существует такая машина Тьюринга* T, *что алгорифм Тьюринга* $\mathfrak{B} = \mathfrak{B}_{T, (A \cup \{S_0, \delta\})}$ *в алфавите* $A \cup \{S_0, \delta\}$ *обладает следующим свойством: для всякого слова* W *в* A *алгорифм* $\mathfrak{B}$ *применим к* W *тогда и только тогда, когда к* W *применим алгорифм* $\mathfrak{A}$, *и при этом* $\mathfrak{B}(W)$ *имеет вид* $S_0^n \mathfrak{A}(W) S_0^n$,

где m и n — целые неотрицательные числа. (Значения алгорифмов $\mathfrak{B}$ и $\mathfrak{A}$ формально различны, так как на ленте машины Тьюринга S_0 есть по существу символ пустого квадрата, а в нормальном алгорифме S_0 есть буква, равноправная с любой другой буквой.)

Доказательство. Ограничимся рассмотрением случая, когда $A = \{S_1, S_2, \ldots, S_k\}$. (Всякий другой случай сводится к этому подходящим изменением индексов.) Пусть $P \to (\cdot) Q$ — произвольная формула подстановки. Построим систему команд машины Тьюринга, действие которой состоит в замещении самого левого вхождения слова P в произвольное слово W (если такие вхождения вообще имеются) словом Q. Если $P \neq \Lambda$, то пусть $P = b_0 \ldots b_r$. Рассмотрим тогда следующую систему команд:

$$
\begin{array}{llll}
q_0 & S_i & R & q_0 \quad (S_i \in A,\ S_i \neq b_0) \\
q_0 & b_0 & \delta & q_0 \\
q_0 & \delta & R & q_2 \\
q_2 & b_1 & R & q_3 \\
q_2 & S_i & S_i & q_{r+2} \quad (S_i \in A \cup \{S_0\},\ S_i \neq b_1) \\
q_3 & b_2 & R & q_4 \\
q_3 & S_i & S_i & q_{r+2} \quad (S_i \in A \cup \{S_0\},\ S_i \neq b_2) \\
 & \vdots & & \\
q_r & b_{r-1} & R & q_{r+1} \\
q_r & S_i & S_i & q_{r+2} \quad (S_i \in A \cup \{S_0\},\ S_i \neq b_{r-1}) \\
q_{r+1} & b_r & R & q_{r+4} \\
q_{r+1} & S_i & S_i & q_{r+2} \quad (S_i \in A \cup \{S_0\},\ S_i \neq b_r) \\
q_{r+2} & S_i & L & q_{r+2} \quad (S_i \in A \cup \{S_0\}) \\
q_{r+2} & \delta & b_0 & q_{r+3} \\
q_{r+3} & b_0 & R & q_0 \\
q_0 & S_0 & L & q_{r+5} \\
q_{r+5} & S_i & L & q_{r+5} \quad (S_i \in A) \\
q_{r+5} & \delta & b_0 & q_{r+5} \\
q_{r+5} & S_0 & R & q_Y
\end{array}
$$

где индекс Y — некоторое целое число, большее любого из индексов, которые в дальнейшем будут еще употреблены. Эта система команд следующим образом действует на слово W. (Заметим, что мы до сих пор не употребили символ внутреннего состояния q_1, он будет еще применен в дальнейшем со специальной целью.) Если W не содержит вхождений слова P, то действие этой системы команд заканчивается конфигурацией $q_Y W$. Если же W содержит вхождения слова P и $W = W_1 P W_2$, где W_1 и W_2 определяются самым левым вхождением слова P в W, то работа системы команд закончится конфигурацией $W_1 P q_{r+4} W_2$. Учитывая эту возможность, нашу систему команд следует

расширить дополнительными командами, с помощью которых выделенное вхождение слова P было бы заменено на Q. Пусть $Q = c_0 \ldots c_s$. Возможны три случая.

(1) $s = r$, т. е. P и Q — слова одной длины. В этом случае добавим команды:

$$
\begin{array}{llll}
q_{r+4} & S_i & L & q_{r+7} \qquad (S_i \in \mathrm{A} \cup \{S_0\}) \\
q_{r+7} & b_r & c_r & q_{r+8} \\
q_{r+8} & c_r & L & q_{r+9} \\
q_{r+9} & b_{r-1} & c_{r-1} & q_{r+10} \\
q_{r+10} & c_{r-1} & L & q_{r+11} \\
 & & \vdots & \\
q_{3r+7} & b_0 & c_0 & q_{3r+8} \\
q_{3r+8} & S_i & L & q_{3r+8} \qquad (S_i \in \mathrm{A}) \\
q_{3r+9} & S_0 & R & q_u
\end{array}
$$

где

$$
u = \begin{cases} 0, & \text{если формула подстановки } P \to (\cdot)\, Q \text{ простая,} \\ 1, & \text{если формула подстановки } P \to (\cdot)\, Q \text{ заключительная.} \end{cases}
$$

Применяя эти команды к $W_1 P q_{r+4} W_2$, мы получим $q_u W_1 Q W_2$.

(2) $s < r$. Q короче P.

Добавим команды:

$$
\begin{array}{llll}
q_{r+4} & S_i & L & q_{r+7} \qquad (S_i \in \mathrm{A} \cup \{S_0\}) \\
q_{r+7} & b_r & c_s & q_{r+8} \\
q_{r+8} & c_s & L & q_{r+8} \\
 & & \vdots & \\
q_{r+7+2s} & b_{r-s} & c_0 & q_{r+7+2s+1} \\
q_{r+7+2s+1} & c_0 & L & q_{r+7+2s+2} \\
q_{r+7+2s+2} & b_{r-s-1} & S_0 & q_{r+7+2s+2} \\
q_{r+7+2s+2} & S_0 & L & q_{r+7+2s+3} \\
q_{r+7+2s+3} & b_{r-s-2} & S_0 & q_{r+7+2s+3} \\
q_{r+7+2s+3} & S_0 & L & q_{r+7+2s+4} \\
 & & \vdots & \\
q_{2r+s+8} & b_0 & S_0 & q_{2r+s+8}
\end{array}
$$

Применение этих команд к $W_1 P q_{r+4} W_2$ приводит к конфигурации

$$W_1 q_{2r+s+8} S_0^{r-s} Q W_2.$$

Теперь следует предусмотреть команды, с помощью которых можно было бы слово W_1 подвинуть на ленте на $r - s$ квадратов вправо, чтобы получить слово $W_1 Q W_2$ (которому предшествует некоторое слово в алфавите $\{S_0\}$). Пусть M — целое число, большее всех встречающихся

выше индексов при q_i и S_i, например, пусть $M = 3r + 9$. Добавляем команды

$$
\begin{array}{lllll}
 & q_{2r+s+8} & S_0 & L & q_M \\
 & q_M & S_j & \delta & q_{M+j} \qquad (S_j \in \mathrm{A}) \\
 & q_{M+j} & \delta & R & q_{M+j} \\
 & q_{M+j} & S_0 & R & q_{M+j} \\
 & q_{M+j} & S_l & L & q_{2M+j} \qquad (S_l \in \mathrm{A}) \\
 & q_{2M+j} & S_0 & S_j & q_{2M+j} \\
 & q_{2M+j} & S_j & L & q_{3M+j} \\
 & q_{3M+j} & S_0 & L & q_{3M+j} \\
 & q_{3M+j} & \delta & S_0 & q_{4M+j} \\
(j = 1, 2, \ldots k) & q_{4M+j} & S_0 & L & q_{5M+j} \\
 & q_{5M+j} & S_0 & R & q_{6M+j} \\
 & q_{6M+j} & S_0 & R & q_{6M+j} \\
 & q_{6M+j} & S_l & S_l & q_u \qquad (S_l \in \mathrm{A})
\end{array}
$$

где

$$u = \begin{cases} 0, \text{ если формула подстановки } P \to (\cdot) Q \text{ простая,} \\ 1, \text{ если формула подстановки } P \to (\cdot) Q \text{ заключительная,} \end{cases}$$

$$q_{5M+j} \quad S_l \quad S_l \quad q_M \qquad (S_l \in \mathrm{A})$$

Начиная с конфигурации $W_1 q_{2r+s+8} S_0^{r-s} Q W_2$, мы с помощью этих последних команд придем при некотором положительном p к конфигурации $(S_0)^p q_u W_1 Q W_2$.

(3) $s > r$, т. е. слово Q длиннее слова P. Этот случай рассматривается аналогично предыдущему, и мы его оставляем на долю читателя в качестве упражнения, равно как и те модификации конструкции, которые необходимы, когда какое-нибудь из слов P или Q — пустое.

Пусть теперь задан произвольный нормальный алгорифм $\mathfrak{A}$ в алфавите $\mathrm{A} = \{S_1, \ldots, S_k\}$, не содержащем S_0 и δ, и пусть схемой алгорифма $\mathfrak{A}$ будет $P_1 \to (\cdot) Q_1, \ldots, P_h \to (\cdot) Q_h$. Определим машину Тьюринга T следующим образом. Воспроизведем всю предыдущую конструкцию для первой формулы подстановки $P_1 \to (\cdot) Q_1$ (с учетом дальнейшего хода рассуждений в качестве значения индекса Y достаточно взять, например, число, в 100 раз превышающее сумму k и числа всех вхождений букв в схему $\mathfrak{A}$). Мы получим систему команд, применение которой к $q_0 W$ приводит к прекращению ее действия на конфигурации $q_Y W$, если W не содержит вхождений слова P_1, а если $W = W_1 P_1 W_2$, где выделено первое слева вхождение P_1 в W, то на конфигурации вида $(S_0)^v q_u W_1 Q_1 W_2$ (где $v \geqslant 0$ и $u = 0$ или $u = 1$, смотря по тому, простой или заключи-

тельной является формула подстановки $P_1 \to (\cdot)\, Q_1$). Обратимся теперь к следующей формуле подстановки $P_2 \to (\cdot)\, Q_2$ и для нее построим сначала систему команд, следуя изложенному выше образцу для общего случая $P \to (\cdot)\, Q$, а затем индексы всех встречающихся в этой системе внутренних состояний q_i, кроме q_u, увеличим на Y. Полученная таким образом система команд и будет той системой команд, которая в конструируемой машине соответствует формула подстановки $P_2 \to (\cdot)\, Q_2$. Очевидно, что действие команд двух уже построенных систем команд не накладывается. Новые, т. е. соответствующие формуле подстановки $P_2 \to (\cdot)\, Q_2$, команды могут начать действие только после того, как слово, последовательно получающееся от применения команд, соответствующих $P_1 \to (\cdot)\, Q_1$, окажется лишенным вхождений слова P_1. Тогда с помощью этих новых команд находящееся на ленте слово будет испытываться на наличие в нем вхождений слова P_2. При этом имеются две возможности. 1) Такие вхождения имеются. Самое левое из них будет замещено на Q_2, и машина перейдет в состояние q_1, если $P_2 \to (\cdot)\, Q_2$ — заключительная формула подстановки, либо в состояние q_0, если $P_2 \to (\cdot)\, Q_2$ — простая формула подстановки. В этом последнем случае вновь начинают действовать команды, соответствующие $P_1 \to (\cdot)\, Q_1$. 2) Вхождений P_2 нет. Машина, работая по командам, соответствующим $P_2 \to (\cdot)\, Q_2$, в конечном итоге оставляет без изменения находившееся на ленте слово и переходит в состояние q_{2Y}. Теперь должны начать действовать команды, соответствующие $P_3 \to (\cdot)\, Q_3$, которые мы построим так же, как и для $P_2 \to (\cdot)\, Q_2$, с той разницей, что индексы внутренних состояний увеличим не на Y, а на $2Y$. Рассуждая аналогичным образом, мы достроим всю систему команд машины Т, которая имитирует работу алгорифма $\mathfrak{A}$ в том смысле, что для любого слова W в А алгорифм $\mathfrak{B} = \mathfrak{B}_{\mathrm{T},\ \mathrm{A} \cup \{S_0, \delta\}}$ применим к W тогда и только тогда, когда к W применим $\mathfrak{A}$ и $\mathfrak{B}(W)$ имеет вид $(S_0)^m \mathfrak{A}(W)(S_0)^n$, где m и n — целые неотрицательные числа. (Сходное доказательство можно найти у Ассера [1959]. Косвенное доказательство можно было бы получить с помощью следствия 5.11, доказав, что всякая частично рекурсивная функция вычислима по Тьюрингу. Читателю станет яснее намеченная здесь процедура, если он познакомится с изложенным у Гермеса [1961] (II, § 7) методом соединения машин Тьюринга и их программ.)

Следствие 5.15. *Всякая частичная вычислимая по Маркову функция вычислима по Тьюрингу.* (И следовательно, всякая частично рекурсивная функция вычислима по Тьюрингу. Другое доказательство см. у Клини [1952], § 68.)

Доказательство. Следует из предложения 5.14 и определения вычислимой по Тьюрингу функции.

Итак, мы видим, что три способа уточнения понятия эффективной вычислимости — в терминах машин Тьюринга, нормальных алгорифмов и рекурсивных функций — по существу эквивалентны. Машины Тьюринга можно рассматривать как некую абстрактную форму цифровых вычислительных машин (если не принимать во внимание вопросы скорости

и удобства вычислений). Совпадение классов функций, частично рекурсивных и вычислимых по Тьюрингу, интуитивно воспринимается как еще один факт, говорящий в пользу тезиса Черча. К этому можно также добавить, что класс вычислимых по Тьюрингу функций не изменится, если мы усложним определение машины Тьюринга, допуская, например, не одну, а несколько лент и читающих головок или используя двумерную ленту. (Подробнее об этом см. у Клини [1952], гл. XIII, § 70.)

§ 3. Вычислимость по Эрбрану — Гёделю. Рекурсивно перечислимые множества

Идея определения понятия вычислимой функции в терминах довольно простых систем уравнений была выдвинута Эрбраном и затем развита Гёделем [1934].

Мы построим теорию вычислимости по Эрбрану — Гёделю, следуя в основном изложению Клини [1952], гл. XI.

Сначала определим *термы*.

(a) Переменные суть термы.

(b) 0 есть терм.

(c) Если t есть терм, то $(t)'$ есть терм.

(d) Если $t_1, \ldots, t_n$ — термы и f_j^n — функциональная буква, то $f_j^n(t_1, \ldots, t_n)$ есть терм.

Каждому натуральному числу n мы ставим в соответствие *цифру* $\overline{n}$ по следующему правилу: (1) $\overline{0}$ есть 0, (2) $\overline{n+1}$ есть $(\overline{n})'$. Таким образом, всякая цифра есть терм.

Равенством называется всякая формула $r = s$, где r и s — термы. *Системой равенств* называется всякая конечная последовательность E равенств $r_1 = s_1, \ldots, r_k = s_k$ таких, что r_k имеет вид $f_j^n(t_1, \ldots, t_n)$. Эта функциональная буква f_j^n называется *главной функциональной буквой* системы E. Те функциональные буквы системы E, которые встречаются только в правых частях равенств, называются *начальными функциональными буквами* E. Функциональная буква, отличная от главной, называется *вспомогательной функциональной буквой* E, если она встречается как в левых, так и в правых частях равенств из E.

Имеются два правила вывода:

R_1: равенство e_2 является следствием равенства e_1 по правилу R_1 тогда и только тогда, когда e_2 получается из e_1 подстановкой в e_1 какой-нибудь цифры вместо всех вхождений некоторой переменной.

R_2: равенство e есть следствие по правилу R_2 равенств $f_h^m(\overline{n}_1, \ldots, \overline{n}_m) = \overline{p}$ и $r = s$ тогда и только тогда, когда $r = s$ не содержит переменных и e получается из $r = s$ заменой одного или одновременно нескольких вхождений в s терма $f_h^m(\overline{n}_1, \ldots, \overline{n}_m)$ термом $\overline{p}$.

Выводом равенства e из данного множества B равенств называется всякая последовательность $e_0, \ldots, e_q$ равенств такая, что e_q есть e,

и если $0 \leqslant i \leqslant q$, то либо (1) e_i принадлежит B, либо (2) e_i есть следствие по правилу R_1 какого-нибудь предыдущего равенства e_j $(j < i)$, либо (3) e_i есть следствие по правилу R_2 каких-нибудь двух предшествующих равенств e_j и e_m $(j < i,\ m < i)$. Утверждение «существует вывод e из B» будет в дальнейшем изображаться символически записью $B \vdash e$, которую мы будем читать как «e выводимо из B».

Пример. Пусть E есть система равенств

$$f_1^1(x_1) = (x_1)',$$
$$f_1^2(x_1, x_2) = f_1^3(\overline{2}, x_2, f_1^1(x_1)).$$

Главной функциональной буквой E является f_1^2. Функциональные буквы f_1^3 и f_1^1 являются в E соответственно начальной и вспомогательной. Последовательность равенств

$$f_1^2(x_1, x_2) = f_1^3(\overline{2}, x_2, f_1^1(x_1)),$$
$$f_1^2(\overline{2}, x_2) = f_1^3(\overline{2}, x_2, f_1^1(\overline{2})),$$
$$f_1^2(\overline{2}, \overline{1}) = f_1^3(\overline{2}, \overline{1}, f_1^1(\overline{2})),$$
$$f_1^1(x_1) = (x_1)',$$
$$f_1^1(\overline{2}) = (\overline{2})' \qquad (\text{т. е. } f_1^1(\overline{2}) = \overline{3}),$$
$$f_1^2(\overline{2}, \overline{1}) = f_1^3(\overline{2}, \overline{1}, \overline{3})$$

является выводом $f_1^2(\overline{2}, \overline{1}) = f_1^3(\overline{2}, \overline{1}, \overline{3})$ из E.

Частичная арифметическая функция $\varphi(x_1, \ldots, x_n)$ называется *вычислимой с помощью системы равенств* E, если главной функциональной буквой E является n-местная функциональная буква, например, f_i^n, и для любых натуральных чисел $k_1, \ldots, k_n$ и p имеет место $E \vdash f_i^n(\overline{k_1}, \ldots, \overline{k_n}) = \overline{p}$ тогда и только тогда, когда $\varphi(k_1, \ldots, k_n) = p$. Функция φ называется *вычислимой по Эрбрану — Гёделю* (коротко — ЭГ-вычислимой), если существует система равенств E, с помощью которой она вычислима.

Примеры. 1. Пусть система E состоит из единственного равенства $f_1^1(x_1) = 0$. Тогда с помощью E вычислима нуль-функция Z. Таким образом, функция Z ЭГ-вычислима.

2. Пусть система равенств E состоит из одного равенства $f_1^1(x_1) = (x_1)'$. С помощью E вычислима тогда функция N «следующий за». Таким образом, функция N ЭГ-вычислима.

3. Проектирующая функция U_i^n вычислима, очевидно, с помощью системы E, состоящей из единственного равенства $f_i^n(x_1, \ldots, x_n) = x_i$, и, следовательно, ЭГ-вычислима.

4. Пусть E есть система равенств

$$f_1^2(x_1, 0) = x_1,$$
$$f_1^2(x_1, (x_2)') = (f_1^2(x_1, x_2))'.$$

С помощью E вычислима операция сложения.

Предложение 5.16. *Всякая частично рекурсивная функция* ЭГ-*вычислима.*

Доказательство. (1) Как показывают предыдущие примеры 1 — 3, начальные функции Z, N и U_i^n ЭГ-вычислимы.

(2) Пусть функция φ получается из функций η, $\psi_1, \ldots, \psi_m$ с помощью подстановки: $\varphi(x_1, \ldots, x_n) = \eta(\psi_1(x_1, \ldots, x_n), \ldots, \psi_m(x_1, \ldots, x_n))$ (правило IV определения частично рекурсивной функции). Предположим, что η, $\psi_1, \ldots, \psi_m$ ЭГ-вычислимы. Пусть тогда E_i — система равенств, с помощью которой вычислима функция ψ_i, и f_i^n — главная функциональная буква в E_i ($i = 1, \ldots, m$), и пусть E_{m+1} — система равенств, с помощью которой вычислима функция η, и f_{m+1}^m — главная функциональная буква в E_{m+1}. Изменив (если это потребуется) индексы, мы можем добиться того, чтобы никакие две из систем $E_1, \ldots, E_m$, E_{m+1} не содержали одинаковых функциональных букв. Покажем, что системой равенств, с помощью которой вычислима функция φ, может служить система E, получающаяся, если выписать в одну последовательность равенства систем $E_1, \ldots, E_m$, E_{m+1} и в конце приписать еще равенство $f_{m+2}^n(x_1, \ldots, x_n) = f_{m+1}^m(f_1^n(x_1, \ldots, x_n), \ldots, f_m^n(x_1, \ldots, x_n))$, где функциональная буква f_{m+2}^n отлична от всех функциональных букв, входящих в $E_1, \ldots, E_{m+1}$. В самом деле, с одной стороны, ясно, что если $\varphi(k_1, \ldots, k_n) = p$, то $E \vdash f_{m+2}^n(\bar{k}_1, \ldots, \bar{k}_n) = \bar{p}$. Обратно, если $E \vdash f_{m+2}^n(\bar{k}_1, \ldots, \bar{k}_n) = \bar{p}$, то $E \vdash f_1^n(\bar{k}_1, \ldots, \bar{k}_n) = \bar{p}_1, \ldots,$ $E \vdash f_m^n(\bar{k}_1, \ldots, \bar{k}_n) = \bar{p}_m$ и $E \vdash f_{m+1}^m(\bar{p}_1, \ldots, \bar{p}_m) = \bar{p}$. Но это значит на самом деле, что $E_1 \vdash f_1^n(\bar{k}_1, \ldots, \bar{k}_n) = \bar{p}_1, \ldots, E_m \vdash f_m^n(\bar{k}_1, \ldots, \bar{k}_n) = \bar{p}_m$ и $E_{m+1} \vdash f_{m+1}^m(\bar{p}_1, \ldots, \bar{p}_m) = \bar{p}$. Следовательно, в силу ЭГ-вычислимости функций $\psi_1, \ldots, \psi_m$ и η с помощью систем $E_1, \ldots, E_m$ и E_{m+1}, имеем $\psi_1(k_1, \ldots, k_n) = p_1, \ldots, \psi_m(k_1, \ldots, k_n) = p_m$ и $\eta(p_1, \ldots, p_m) = p$. Поэтому и $\varphi(k_1, \ldots, k_n) = p$. (Проведение этого доказательства во всех деталях мы оставляем читателю в качестве упражнения. За указаниями можно обратиться к Клини [1952], гл. XI, § 54.) Итак, функция φ ЭГ-вычислима.

(3) Пусть функция φ получается из функций ψ и θ с помощью рекурсии (правило V из определения частично рекурсивных функций), т. е.

$$\varphi(x_1, \ldots, x_n, 0) = \psi(x_1, \ldots, x_n),$$

$$\varphi(x_1, \ldots, x_n, x_{n+1} + 1) = \theta(x_1, \ldots, x_{n+1}, \varphi(x_1, \ldots, x_{n+1})),$$

где ψ и θ ЭГ-вычислимы. Допустим, что функция ψ вычислима с помощью системы равенств E_1 с главной функциональной буквой f_1^n, а функция θ вычислима с помощью системы равенств E_2 с главной функциональной буквой f_1^{n+2}. Тогда систему равенств E, с помощью которой вычислима функция φ, построим как объединение систем E_1 и E_2 с добавлением равенств

$$f_1^{n+1}(x_1, \ldots, x_n, 0) = f_1^n(x_1, \ldots, x_n),$$

$$f_1^{n+1}(x_1, \ldots, x_n, (x_{n+1})') = f_1^{n+2}(x_1, \ldots, x_{n+1}, f_1^{n+1}(x_1, \ldots, x_{n+1})).$$

(Мы здесь предполагаем снова, что E_1 и E_2 не имеют общих функциональных букв.) Очевидно, что если $\varphi(k_1, \ldots, k_n, k) = p$, то $E \vdash f_1^{n+1}(\bar{k}_1, \ldots, \bar{k}_n, \bar{k}) = \bar{p}$. Индукцией по k легко доказать и обратное, т. е. что если $E \vdash f_1^{n+1}(\bar{k}_1, \ldots, \bar{k}_n, \bar{k}) = \bar{p}$, то $\varphi(k_1, \ldots, k_n, k) = p$. Отсюда получаем ЭГ-вычислимость φ. (Рассмотреть самостоятельно случай $n = 0$.)

(4) Пусть функция φ получается из функции ψ с помощью μ-оператора, т. е. $\varphi(x_1, \ldots, x_n) = \mu y(\psi(x_1, \ldots, x_n, y) = 0)$ (правило VI определения частично рекурсивной функции). Предположим, что функция ψ ЭГ-вычислима с помощью системы равенств E_1 с главной функциональной буквой f_1^{n+1}. На основании предыдущих пунктов (1) — (3) можно утверждать, что всякая примитивно рекурсивная функция ЭГ-вычислима. В частности, ЭГ-вычислима операция умножения. Следовательно, существует такая система равенств E_2 с главной функциональной буквой f_2^3, не содержащая общих с E_1 букв, что $E_2 \vdash f_2^3(\bar{k}_1, \bar{k}_2) = \bar{p}$ тогда и только тогда, когда $k_1 \cdot k_2 = p$. Образуем систему равенств E_3, объединив системы E_1 и E_2 и добавив к ним равенства

$$f_2^{n+1}(x_1, \ldots, x_n, 0) = 1,$$

$$f_2^{n+1}(x_1, \ldots, x_n, (x_{n+1})') = f_2^3(f_2^{n+1}(x_1, \ldots, x_n, x_{n+1}), f_1^{n+1}(x_1, \ldots, x_n, x_{n+1})).$$

По индукции легко доказать, что с помощью E_3 вычислима функция $\prod_{x<z} \psi(x_1, \ldots, x_n, y)$, т. е. $E_3 \vdash f_2^{n+1}(\bar{k}_1, \ldots, \bar{k}_n, \bar{k}) = \bar{p}$ тогда и только тогда, когда $\prod_{y<k} \psi(k_1, \ldots, k_n, y) = p$. Пусть теперь E есть система равенств, получающаяся путем добавления к E_3 равенств

$$f_2^3((x_1)', 0, x_3) = x_3,$$

$$f_3^n(x_1, \ldots, x_n) = f_2^3(f_2^{n+1}(x_1, \ldots, x_n, x_{n+1}), f_2^{n+1}(x_1, \ldots, x_n, (x_{n+1})'), x_{n+1}).$$

Тогда функция $\varphi(x_1, \ldots, x_n) = \mu y(\psi(x_1, \ldots, x_n, y) = 0)$ вычислима с помощью E. В самом деле, если $\mu y(\psi(k_1, \ldots, k_n, y) = 0) = q$, то $E_3 \vdash f_2^{n+2}(\bar{k}_1, \ldots, \bar{k}_n, \bar{q}) = \bar{p}'$, где $p + 1 = \prod_{y<q} \psi(k_1, \ldots, k_n, y)$, и $E_3 \vdash f_2^{n+1}(\bar{k}_1, \ldots, \bar{k}_n, \bar{q}') = 0$. Следовательно, $E \vdash f_3^n(\bar{k}_1, \ldots, \bar{k}_n) = f_2^3(\bar{p}', 0, \bar{q})$. Но $E \vdash f_2^3(\bar{p}', 0, \bar{q}) = \bar{q}$, и, таким образом, окончательно имеем $E \vdash f_3^n(\bar{k}_1, \ldots, \bar{k}_n) = \bar{q}$. Обратно, пусть $E \vdash f_3^n(\bar{k}_1, \ldots, \bar{k}_n) = \bar{q}$; тогда $E \vdash f_2^3(\bar{m}', 0, \bar{q}) = \bar{q}$ при некотором m, где $E_3 \vdash f_2^{n+1}(\bar{k}_1, \ldots, \bar{k}_n, \bar{q}) = (\bar{m})'$ и $E_3 \vdash f_2^{n+1}(\bar{k}_1, \ldots, \bar{k}_n, \bar{q}') = 0$. Следовательно, $\prod_{y<q} \psi(k_1, \ldots, k_n, y) = m + 1 \neq 0$ и $\prod_{y<q+1} \psi(k_1, \ldots, k_n, y) = 0$. Иначе говоря, $\psi(k_1, \ldots, k_n, y) \neq 0$, если $y \leq q$, и $\psi(k_1, \ldots, k_n, q) = 0$. Поэтому $\mu y(\psi(k_1, \ldots, k_n, y) =$

$= 0) = q$. Функция φ, таким образом, тоже ЭГ-вычислима. Этим и завершается доказательство предложения 5.16.

Мы теперь поставим себе целью доказать, что всякая вычислимая по Эрбрану — Гёделю функция частично рекурсивна. Для этого мы применим арифметизацию аппарата ЭГ-вычислимости. Воспользуемся готовой уже арифметизацией из § 4 гл. 3. (Символ $'$ служит сокращением для $f1$. Напомним также, что $r = s$ есть сокращенная запись элементарной формулы $A_2^2(r, s)$ и единственной предметной константой является 0.) В частности (см. § 4 гл. 3), следующие отношения и функции являются примитивно рекурсивными.

FL (x): «x есть гёделев номер функциональной буквы» или формально

$$\exists y_{y<x} \exists z_{z<x} (x = 9 + 8(2^y \cdot 3^z) \,\&\, y > 0 \,\&\, z > 0),$$

EVbl (x): «x есть гёделев номер выражения, состоящего из переменной»,

EFL (x): «x есть гёделев номер выражения, состоящего из функциональной буквы»,

Nu (x): «x есть гёделев номер цифры»,

Trm (x): «x есть гёделев номер терма»,

Atfml (x): «x есть гёделев номер элементарной формулы»,

Num (x) = гёделеву номеру цифры $\bar{x}$,

Arg_T (x) = числу аргументов функциональной буквы f, если x есть гёделев номер f,

x * y = гёделеву номеру выражения AB, если x есть гёделев номер выражения A, а y — гёделев номер выражения B,

Subst (a, b, u, v): «v есть гёделев номер некоторой переменной x_i, u есть гёделев номер некоторого терма t, b есть гёделев номер некоторого выражения $\mathscr{A}$ и a есть гёделев номер результата подстановки терма t вместо всех вхождений x_i в $\mathscr{A}$».

Примитивно рекурсивными являются, кроме того, следующие предикаты.

Eqt (x): «x есть гёделев номер равенства», что можно выразить формально как Atfml (x) & $(x)_0 = 107$. (Напомним, что A_1^2 есть предикат равенства и его гёделев номер равен 107.)

Syst (x): «x есть гёделев номер системы равенств» или формально

$$\forall y_{y < \mathrm{lh}(x)} \mathrm{Eqt}((x)_y) \,\&\, \mathrm{FL}(((x)_{\mathrm{lh}(x) \dot{-} 1})_2).$$

Occ (u, v): «u есть гёделев номер некоторого терма t или некоторого равенства $\mathfrak{B}$, а v есть гёделев номер терма, входящего в t или в $\mathfrak{B}$»:

$$(\mathrm{Trm}(u) \vee \mathrm{Eqt}(u)) \,\&\, \mathrm{Trm}(v) \,\&\, \exists x_{x<u} \exists y_{y<u} (u = x * v * y \vee u = x * v \vee u = v * y \vee u = v)$$

Cons_1 (u, v): «существуют такие равенства e_1 и e_2, что u есть гёделев номер e_1, v есть гёделев номер e_2 и e_2 есть следствие e_1 по

правилу R_1», что выражается формулой

$$\mathrm{Eqt}(u) \,\&\, \mathrm{Eqt}(v) \,\&\, \exists x_{x<u} \exists y_{y<v} (\mathrm{Nu}(y) \,\&\, \mathrm{Subst}(v, u, y, x) \,\&\, \mathrm{Occ}(u, x)).$$

$\mathrm{Cons}_2(u, z, v)$: «существуют равенства e_1, e_2, e_3 такие, что u, z, v являются соответственно их гёделевыми номерами и e_3 есть следствие e_1 и e_2 по правилу R_2» или формально (в случае, когда заменяется цифрой лишь одно вхождение терма):

$$\mathrm{Eqt}(u) \,\&\, \mathrm{Eqt}(z) \,\&\, \mathrm{Eqt}(v) \,\&\, \neg \exists x_{x \leqslant z} (\mathrm{EVbl}(x) \,\&\, \mathrm{Occ}(z, x)) \,\&\, \mathrm{FL}((z)_2) \,\&$$
$$\&\, \forall x_{2<x<\mathrm{lh}(z)} \neg \mathrm{FL}((z)_x) \,\&\, \exists s_{s \leqslant z} \exists w_{w \leqslant z} \exists x_{x \leqslant u} \exists y_{y \leqslant u} \exists t_{t \leqslant u} \exists r_{r \leqslant u} (z =$$
$$= p_0^{107} \cdot p_1^s * s * 2^7 * w * 2^5 \,\&\, \mathrm{Trm}(s) \,\&\, \mathrm{Nu}(w) \,\&\, \mathrm{Trm}(x) \,\&$$
$$\&\, u = y * x * 2^5 \,\&\, x = t * s * r \,\&\, v = y * t * w * r * 2^5).$$

(Напомним, что $g((= 3$, $g()) = 5$, $g(,) = 7$.)

$\mathrm{Ded}(u, z)$: «u есть гёделев номер некоторой системы равенств E и z есть гёделев номер некоторого вывода из E» или формально

$$\mathrm{Syst}(u) \,\&\, \forall x_{x<\mathrm{lh}(z)} (\exists w_{w<\mathrm{lh}(u)} ((u)_w = (z)_x) \vee$$
$$\vee \exists y_{y<x} \mathrm{Cons}_1((z)_y, (z)_x) \vee \exists y_{y<x} \exists v_{v<x} \mathrm{Cons}_2((z)_y, (z)_v, (z)_x)).$$

$S_n(u, x_1, \ldots, x_n, z)$: «u есть гёделев номер некоторой системы равенств E с главной буквой f_j^n и z есть гёделев номер некоторого вывода из E равенства $f_j^n(\bar{x}_1, \ldots, \bar{x}_n) = \bar{p}$». Этот предикат может быть выражен формулой

$$\mathrm{Ded}(u, z) \,\&\, \mathrm{Arg}_T(((u)_{\mathrm{lh}(u) \dot{-} 1})_2) = n \,\&\, \exists x_{x \leqslant z} \exists y_{y \leqslant z} (x = ((u)_{\mathrm{lh}(u) \dot{-} 1})_2 \,\&\, z =$$
$$= p_0^{107} \cdot p_1^3 \cdot p_2^x \cdot p_3^3 \cdot p_4^{\mathrm{Num}(x_1)} \cdot p_5^7 \cdot \ldots \cdot p_{2n+1}^7 \cdot p_{2n+2}^{\mathrm{Num}(x_n)} \times$$
$$\times p_{2n+3}^5 \cdot p_{2n+4}^7 * y * 2^5 \,\&\, \mathrm{Nu}(y)).$$

Примитивно рекурсивной является и функция

$U(x) = \mu y_{y<x} (\mathrm{Num}(y) = ((x)_{\mathrm{lh}(x) \dot{-} 1})_{\mathrm{lh}(x) \dot{-} 2})$. (Если x есть гёделев номер вывода равенства $r = \bar{p}$, то $U(x) = p$.)

Предложение 5.17 (Клини [1936a]). *Если функция* $\varphi(x_1, \ldots, x_n)$ ЭГ-*вычислима и e — гёделев номер системы равенств* E, *с помощью которой она вычислима, то*

$$\varphi(x_1, \ldots, x_n) = U(\mu y S_n(e, x_1, \ldots, x_n, y)),$$

и, следовательно, всякая ЭГ-*вычислимая функция* φ *является частично рекурсивной функцией, если же, кроме того,* φ *определена всюду, то* φ *рекурсивна.*

Доказательство. Пусть функция φ вычислима с помощью системы равенств E, имеющей f_j^n своей главной функциональной буквой и e своим гёделевым номером. Для любых $k_1, \ldots, k_n$ и p имеет место $\varphi(k_1, \ldots, k_n) = p$ тогда и только тогда, когда $E \vdash f_j^n(\bar{k}_1, \ldots, \bar{k}_n) = \bar{p}$. Кроме того, $\varphi(k_1, \ldots, k_n)$ определено тогда и только тогда, когда $\exists y S_n(e, k_1, \ldots, k_n, y)$. Если $\varphi(k_1, \ldots, k_n)$ определено, то $\mu y S_n(e, k_1, \ldots$

$\ldots, k_n, y)$ является гёделевым номером вывода из E равенства $f_j^n(\bar{k}_1, \ldots, \bar{k}_n) = \bar{p}$. Следовательно, $U(\mu y S_n(e, k_1, \ldots, k_n, y)) = p = \varphi(k_1, \ldots, k_n)$. Так как предикат S_n примитивно рекурсивен, то функция $U(\mu y S_n(e, x_1, \ldots, x_n, y))$ — частично рекурсивная. Если же функция $\varphi(x_1, \ldots, x_n)$ определена всюду, то $\forall x_1 \ldots \forall x_n \exists y S_n(e, x_1, \ldots, x_n, y)$. Это означает, что функция $\mu y S_n(e, x_1, \ldots, x_n)$ рекурсивна. Тогда рекурсивна и функция $U(\mu y S_n(e, x_1, \ldots, x_n, y))$.

Итак, класс функций, вычислимых по Эрбрану — Гёделю, совпадает с классом частично рекурсивных функций. Этот факт служит еще одним доводом в пользу тезиса Чёрча.

Иногда вместо S_n удобнее бывает пользоваться предикатом $T_n(z, x_1, \ldots, x_n, y)$, определяемым формулой $S_n(z, x_1, \ldots, x_n, y)$ & & $\forall u_{u<y} \neg S_n(z, x_1, \ldots, x_n, u)$. Очевидно, если $T_n(z, x_1, \ldots, x_n, y)$, то $S_n(z, x_1, \ldots, x_n, y)$. Зато в отличие от S_n предикат T_n обладает тем свойством, что если $T_n(z, x_1, \ldots, x_n, u)$ и $T_n(z, x_1, \ldots, x_n, y)$, то $u = y$. Очевидно также, что

$$\exists y S_n(z, x_1, \ldots, x_n, y) \equiv \exists y T_n(z, x_1, \ldots, x_n, y)$$

и

$$U(\mu y S_n(z, x_1, \ldots, x_n, y)) = U(\mu y T_n(z, x_1, \ldots, x_n, y)),$$

если только хотя бы одна из частей этого равенства определена. Из предложений 5.16 и 5.17 следует, что всякая частично рекурсивная функция представима в форме $U(\mu y T_n(e, x_1, \ldots, x_n, y))$, где e — гёделев номер системы равенств, с помощью которой эта функция вычислима. И обратно, для любого натурального числа e функция $U(\mu y T_n(e, x_1, \ldots, x_n, y))$ является частично рекурсивной. Таким образом, поскольку z пробегает весь натуральный ряд, $U(\mu y T_n(z, x_1, \ldots, x_n, y))$ дает нам некоторую *нумерацию* (с повторениями) *всех частично рекурсивных функций от n аргументов*. Число e такое, что $\varphi(x_1, \ldots, x_n) = U(\mu y T_n(e, x_1, \ldots, x_n, y))$, называется *индексом функции* φ. Гёделев номер любой системы равенств, с помощью которой вычислима функция φ, является индексом φ. Каждая частично рекурсивная функция имеет бесконечно много индексов. (Пусть читатель докажет это сам в качестве упражнения.)

Индексом рекурсивного предиката R мы будем называть индекс его характеристической функции. Тогда, очевидно,

$$R(x_1, \ldots, x_n) \equiv \exists y (T_n(e, x_1, \ldots, x_n, y) \& U(y) = 0),$$

где e есть индекс предиката R.

Лемма 5.18. (1) *Пусть* $n > 0$ *и* $R(x_1, \ldots, x_n, y)$ — *рекурсивный предикат. Тогда существуют такие натуральные числа* e_1 *и* e_2, *что*

$$\exists y R(x_1, \ldots, x_n, y) \equiv \exists y T_n(e_1, x_1, \ldots, x_n, y)$$

и

$$\forall y R(x_1, \ldots, x_n, y) \equiv \forall y \neg T_n(e_2, x_1, \ldots, x_n, y).$$

(2) *Если* $n > 0$, *то для любого рекурсивного предиката* $R(x_1, \ldots, x_n, z, y)$ *существуют такие натуральные числа* e_3, e_4, *что*

$$\forall z \exists y R(x_1, \ldots, x_n, z, y) \equiv \forall z \exists y T_{n+1}(e_3, x_1, \ldots, x_n, z, y)$$

и

$$\exists z \forall y R(x_1, \ldots, x_n, z, y) \equiv \exists z \forall y \neg T_{n+1}(e_4, x_1, \ldots, x_n, z, y),$$

и так далее, для трех и большего числа кванторов.

Доказательство. (1) Пусть $\varphi(x_1, \ldots, x_n, y)$ — характеристическая функция предиката R. Функция φ рекурсивна, и, следовательно, $\mu y(\varphi(x_1, \ldots, x_n, y) = 0)$ есть функция частично рекурсивная. Пусть e_1 — гёделев номер какой-нибудь системы равенств, с помощью которой вычислима функция $\mu y(\varphi(x_1, \ldots, x_n, y) = 0)$. Тогда $\exists y R(x_1, \ldots, x_n, y)$ в том и только в том случае, когда определено $\mu y(\varphi(x_1, \ldots, x_n, y) = 0)$. Следовательно, $\exists y R(x_1, \ldots, x_n, y) \equiv \exists y T_n(e_1, x_1, \ldots, x_n, y)$. Применяя этот результат к $\neg R$, заключаем, что существует число e_2 такое, что $\exists y \neg R(x_1, \ldots, x_n, y) \equiv \exists y T_n(e_2, x_1, \ldots, x_n, y)$, откуда следует, очевидно, $\forall y R(x_1, \ldots, x_n, y) \equiv \forall y \neg T_n(e_2, x_1, \ldots, x_n, y)$.

(2) Эта часть леммы следует из (1), если в (1) n заменить на $n + 1$.

Придавая u всевозможные натуральные значения, мы, в силу леммы 5.18, получаем с помощью предикатов $\exists y T_n(u, x_1, \ldots, x_n, y)$, $\forall y \neg T_n(u, x_1, \ldots, x_n, y)$ и т. д. нумерацию всех предикатов, имеющих соответственно форму $\exists y R(x_1, \ldots, x_n, y)$, $\forall y R(x_1, \ldots, x_n, y)$ и т. д. при рекурсивных R.

Предложение 5.19 (Клини [1943]; [1952], § 57; Мостовский [1947a].) (1) *Для любого рекурсивного предиката* $R(x, y)$ *существуют натуральные числа* e_1 *и* e_2 *такие, что*

$$\neg(\exists y R(e_1, y) \equiv \forall y \neg T_1(e_1, e_1, y))$$

и

$$\neg(\forall y R(e_2, y) \equiv \exists y T_1(e_2, e_2, y)).$$

(2) *Если* $R(x)$ — *рекурсивный предикат, то существуют натуральные числа* e_1 *и* e_2 *такие, что*

$$\neg(R(e_1) \equiv \forall y \neg T_1(e_1, e_1, y))$$

и

$$\neg(R(e_2) \equiv \exists y T_1(e_2, e_2, y)).$$

(3) *Предикаты* $\forall y \neg T_1(x, x, y)$ *и* $\exists y T_1(x, x, y)$ *не являются рекурсивными.*

(4) *Рассмотрим следующие формы предикатов*:

$R(x_1, \ldots, x_n)$

$\exists y_1 R(x_1, \ldots, x_n, y_1)$ $\quad \exists y_1 \forall y_2 R(x_1, \ldots, x_n, y_1, y_2)$

$\forall y_1 R(x_1, \ldots, x_n, y_1)$ $\quad \forall y_1 \exists y_2 R(x_1, \ldots, x_n, y_1, y_2)$

$\exists y_1 \forall y_2 \exists y_3 R(x_1, \ldots, x_n, y_1, y_2, y_3) \ldots$

$\forall y_1 \exists y_2 \forall y_3 R(x_1, \ldots, x_n, y_1, y_2, y_3) \ldots$

где R — *произвольный рекурсивный предикат. Обозначим через* Π_0^n *и одновременно через* Σ_0^n *класс всех n-местных рекурсивных предикатов. Для любого* $k > 0$ *обозначим через* Σ_k^n *класс всех n-местных предикатов, выразимых в «предваренной форме»* $\exists y_1 \forall y_2 \ldots Qy_k R(x_1, \ldots, x_n, y_1, y_2, \ldots, y_k)$, *где произвольному рекурсивному предикату предшествует кванторная приставка из k кванторов, в которой кванторы существования и общности чередуются, первым является квантор существования, а* Qy_k *есть квантор существования или всеобщности. Класс* Π_k^n *определим так же, как и* Σ_k^n, *с той лишь разницей, что потребуем, чтобы в кванторной приставке первым стоял квантор всеобщности. Итак, имеем последовательность классов*:

$$\Sigma_0^n = \Pi_0^n \quad \begin{matrix} \Sigma_1^n & \Sigma_2^n & \Sigma_3^n & \ldots \\ \Pi_1^n & \Pi_2^n & \Pi_3^n & \ldots \end{matrix}$$

(a) *Если предикат выразим в какой-либо из вышеприведенных форм, то он выразим и во всякой форме из любого столбца, расположенного вправо от нее, т. е.* $\Sigma_k^n \subseteq \Sigma_j^n \cap \Pi_j^n$ *и* $\Pi_k^n \subseteq \Sigma_j^n \cap \Pi_j^n$ *для любого* $j > k$.

(b) *Для любого* $k > 0$ *имеем* $\Sigma_k^n - \Pi_k^n \neq 0$ *и* $\Pi_k^n - \Sigma_k^n \neq 0$, *т. е. существуют предикаты, выразимые в форме* $\exists y_1 \forall y_2 \ldots Qy_k R$, *но невыразимые в форме* $\forall y_1 \exists y_2 \ldots Qy_k R$ *и наоборот; следовательно, и те и другие невыразимы ни в какой форме с более короткой кванторной приставкой.*

(c) *Всякий арифметический предикат* (см. стр. 151, упражнение 2) *выразим по крайней мере в одной из этих форм.*

(d) (Э. Пост.) *Отношение* $Q(x_1, \ldots, x_n)$ *рекурсивно тогда и только тогда, когда* Q *и* $\neg Q$ *выразимы в форме* $\exists y_1 R(x_1, \ldots, x_n, y_1)$ *с рекурсивным* R; *иными словами,* $\Sigma_1^n \cap \Pi_1^n = \Sigma_0^n$.

(e) *Если* $Q_1 \in \Sigma_k^n$ *и* $Q_2 \in \Sigma_k^n$, *то* $Q_1 \vee Q_2 \in \Sigma_k^n$ *и* $Q_1 \& Q_2 \in \Sigma_k^n$; *если* $Q_1 \in \Pi_k^n$ *и* $Q_2 \in \Pi_k^n$, *то* $Q_1 \vee Q_2 \in \Pi_k^n$ *и* $Q_1 \& Q_2 \in \Pi_k^n$.

(f) *В отличие от* (d), *если* $k > 0$, *то*

$$(\Sigma_{k+1}^n \cap \Pi_{k+1}^n) - (\Sigma_k^n \cup \Pi_k^n) \neq 0.$$

Доказательство. (1) Пусть $R(x, y)$ — рекурсивный предикат. По лемме 5.18 существуют числа e_1 и e_2 такие, что $\exists y R(x, y) \equiv \exists y T_1(e_1, x, y)$ и $\forall y R(x, y) \equiv \forall y \neg T_1(e_2, x, y)$.

(2) Пусть $R(x)$ — рекурсивный предикат. Тогда предикат $R(x) \& y = y$ — тоже рекурсивный. Очевидно, $\exists y (R(x) \& y = y) \equiv R(x)$ и $\forall y (R(x) \& y = y) \equiv R(x)$. Теперь остается применить (1).

(3) Допустим, что предикат $\forall y \neg T_1(x, x, y)$ рекурсивен. Тогда, в силу (2), существует число e_1 такое, что $\neg(\forall y \neg T_1(e_1, e_1, y) \equiv \forall y \neg T_1(e_1, e_1, y))$, что является противоречием. Аналогично, если бы предикат $\exists y T_1(x, x, y)$ был рекурсивным, то, в силу (2), должно было

бы существовать число e_2 такое, что $\neg(\exists y T_1(e_2, e_2, y) \equiv \exists y T_1(e_2, e_2, y))$, и мы опять имели бы противоречие.

(4) (a) $\exists z_1 \forall y_1 \exists z_2 \forall y_2 \ldots \exists z_k \forall y_k R(x_1, \ldots, x_n, z_1, y_1, \ldots, z_k, y_k) \equiv$
$\equiv \forall u \exists z_1 \forall y_1 \ldots \exists z_k \forall y_k (R(x_1, \ldots, x_n, z_1, y_1, \ldots, z_k, y_k) \& u = u) \equiv$
$\equiv \exists z_1 \forall y_1 \ldots \exists z_k \forall y_k \exists u (R(x_1, \ldots, x_n, z_1, y_1, \ldots, z_k, y_k) \& u = u)$.

Отсюда следует, что всякое отношение, выразимое в одной из рассматриваемых в доказываемом предложении форм, выразимо и в любой другой форме с более длинной кванторной приставкой.

(b) Здесь мы просто рассмотрим некоторый типичный случай. Предположим, что предикат $\exists v \forall z \exists y T_{n+2}(x_1, x_1, x_2, \ldots, x_n, v, z, y)$ выразим в форме $\forall v \exists z \forall y R(x_1, \ldots, x_n, v, z, y)$, где предикат R рекурсивен. По лемме 5.18, это отношение эквивалентно при некотором e отношению $\forall v \exists z \forall y \neg T_{n+2}(e, x_1, \ldots, x_n, v, z, y)$. Теперь при $x_1 = e$ получаем противоречие.

(c) Всякая формула теории первого порядка S может быть приведена к предваренной нормальной форме. После этого достаточно заметить, что $\exists u \exists v R(u, v)$ эквивалентно $\exists z R(\sigma_1^2(z), \sigma_2^2(z))$, где σ_1^2 и σ_2^2 — рекурсивные функции, обратные взаимно однозначному отображению σ^2 множества всех пар натуральных чисел на натуральный ряд (см. стр. 144). Точно так же $\forall u \forall v R(u, v)$ эквивалентно $\forall z R(\sigma_1^2(z), \sigma_2^2(z))$. Следовательно, рядом стоящие кванторы одного типа (т. е. существования или всеобщности) могут быть свернуты в один квантор того же типа.

(d) Если предикат Q рекурсивен, то рекурсивен и предикат $\neg Q$. Далее, если предикат $P(x_1, \ldots, x_n)$ рекурсивен, то рекурсивен и предикат $P(x_1, \ldots, x_n) \& y = y$; при этом, очевидно, $P(x_1, \ldots, x_n) \equiv$
$\equiv \exists y (P(x_1, \ldots, x_n) \& y = y)$. Обратно, предположим, что предикат Q выразим в форме $\exists y R_1(x_1, \ldots, x_n, y)$ и предикат $\neg Q$ — в форме $\exists y R_2(x_1, \ldots, x_n, y)$, где предикаты R_1 и R_2 рекурсивны. Так как $\forall x_1 \ldots \forall x_n \exists y (R_1(x_1, \ldots, x_n, y) \vee R_2(x_1, \ldots, x_n, y))$, то функция $\varphi(x_1, \ldots, x_n) = \mu y (R_1(x_1, \ldots, x_n, y) \vee R_2(x_1, \ldots, x_n, y))$ рекурсивна. Тогда $Q(x_1, \ldots, x_n) \equiv R_1(x_1, \ldots, x_n, \varphi(x_1, \ldots, x_n))$, и, следовательно, предикат Q рекурсивный.

(e) Читатель легко докажет этот пункт, используя следующие факты: если x не входит свободно в $\mathfrak{A}$, то $\vdash \exists x (\mathfrak{A} \vee \mathfrak{B}) \equiv (\mathfrak{A} \vee \exists x \mathfrak{B})$, $\vdash \exists x (\mathfrak{A} \& \mathfrak{B}) \equiv \mathfrak{A} \& \exists x \mathfrak{B}$, $\vdash \forall x (\mathfrak{A} \vee \mathfrak{B}) \equiv (\mathfrak{A} \vee \forall x \mathfrak{B})$ и $\vdash \forall x (\mathfrak{A} \& \mathfrak{B}) \equiv$
$\equiv (\mathfrak{A} \& \forall x \mathfrak{B})$.

(f) Мы рассмотрим для простоты случай $n = 1$; остальные случаи из него легко следуют. Пусть $Q(x) \in \Sigma_k^1 - \Pi_k^1$. Определим $P(x)$ как $\exists z ((x = 2z \& Q(z)) \vee (x = 2z + 1 \& \neg Q(z)))$. Легко показать, что $P \notin$
$\notin \Sigma_k^1 \cup \Pi_k^1$ и $P \in \Sigma_{k+1}^1$. Нетрудно также видеть, что $P \in \Pi_{k+1}^1$, если заметить, что $P(x)$ истинно тогда и только тогда, когда

$$\exists z (x = 2z \& Q(z)) \vee (\exists z_{z<x} (x = 2z + 1) \& \forall z (x = 2z + 1 \supset \neg Q(z)))$$

(Роджерс [1959]).

Упражнение

В этом упражнении ставится цель доказать, что существуют рекурсивные, но не примитивно рекурсивные функции.

1. Пусть $[\sqrt{n}]$ означает наибольшее целое число, не превосходящее $\sqrt{n}$. Показать, что функция $[\sqrt{n}]$ определяется рекурсией

$$\varkappa(0) = 0,$$
$$\varkappa(n+1) = \varkappa(n) + \overline{\operatorname{sg}}\,|(n+1) - (\varkappa(n)+1)^2|$$

и, следовательно, является примитивно рекурсивной.

2. Функция $\operatorname{Quadrem}(n) = n \dot{-} [\sqrt{n}]^2$, дающая при каждом n разность между n и наибольшим квадратом, не превосходящим n, является примитивно рекурсивной.

3. Пусть $\rho(x, y) = (((x+y)^2 + y)^2 + x)$, $\rho_1(n) = \operatorname{Quadrem}(n)$ и $\rho_2(n) = \operatorname{Quadrem}([\sqrt{n}])$. Эти функции также примитивно рекурсивные. Доказать, что

(a) $\rho_1(\rho(x, y)) = x$ и $\rho_2(\rho(x, y)) = y$;

(b) $\rho(\rho_1(n), \rho_2(n)) = n$;

(c) ρ взаимно однозначно отображает ω^2 на ω;

(d) $\rho_1(0) = \rho_2(0) = 0$,

и если $\rho_1(n+1) \neq 0$, то

$$\rho_1(n+1) = \rho_1(n) + 1,$$
$$\rho_2(n+1) = \rho_2(n).$$

(e) Для каждого $n \geqslant 3$ положим $\rho^n(x_1, \ldots, x_n) = \rho(\rho^{n-1}(x_1, \ldots, x_{n-1}), x_n)$, где $\rho^2 = \rho$. Каждая из функций ρ^n примитивно рекурсивная. Положим далее $\rho_i^n(k) = \rho_i^{n-1}(\rho_1(k))$ для $1 \leqslant i \leqslant n-1$ и $\rho_n^n(k) = \rho_2(k)$. Функции ρ_i^n $(1 \leqslant i \leqslant n)$ — примитивно рекурсивные, причем $\rho_i^n(\rho^n(x_1, \ldots, x_n)) = x_i$ и $\rho^n(\rho_1^n(k), \rho_2^n(k), \ldots, \rho_n^n(k)) = k$. Функция ρ^n, таким образом, взаимно однозначно отображает ω^n на ω и функции ρ_i^n являются соответствующими «обратными» отображениями. Функции ρ^n и ρ_i^n построены из ρ, ρ_1, ρ_2 с помощью подстановки.

4. Схема рекурсии (стр. 135, (V)) может быть ограничена следующей формой:

$$\psi(x_1, \ldots, x_{n+1}, 0) = x_{n+1} \qquad (n \geqslant 0),$$
$$\psi(x_1, \ldots, x_{n+1}, y+1) = \varphi(x_1, \ldots, x_{n+1}, y, \psi(x_1, \ldots, x_{n+1}, y)).$$

В самом деле, пусть дана рекурсия:

$$\theta(x_1, \ldots, x_n, 0) = \gamma(x_1, \ldots, x_n),$$
$$\theta(x_1, \ldots, x_n, y+1) = \delta(x_1, \ldots, x_n, y, \theta(x_1, \ldots, x_n, y)).$$

Полагая $\varphi(x_1, \ldots, x_{n+1}, y, z) = \delta(x_1, \ldots, x_n, y, z)$, определим ψ требуемым образом. Тогда $\theta(x_1, \ldots, x_n, y) = \psi(x_1, \ldots, x_n, \gamma(x_1, \ldots, x_n), y)$.

5. Допустив ρ, ρ_1, ρ_2 в качестве дополнительных исходных функций, мы можем ограничиться применением лишь правила рекурсии (V) в однопараметрической форме:

$$\psi(x, 0) = \alpha(x),$$
$$\psi(x, y+1) = \beta(x, y, \psi(x, y)).$$

[Указание. Пусть $n \geqslant 2$. Если дано

$$\theta(x_1, \ldots, x_n, 0) = \gamma(x_1, \ldots, x_n),$$
$$\theta(x_1, \ldots, x_n, y+1) = \delta(x_1, \ldots, x_n, y, \theta(x_1, \ldots, x_n, y)),$$

то положить $\eta(u, y) = \theta\left(\rho_1^n(u), \ldots, \rho_n^n(u), y\right)$ и определить η с помощью однопараметрической рекурсии.]

6. Допустив ρ, ρ_1, ρ_2 в качестве дополнительных исходных функций, можно в (5) вместо $\beta(x, y, \psi(x, y))$ использовать функцию вида $\delta(y, \psi(x, y))$. [Указание. Пусть

$$\psi(x, 0) = \alpha(x),$$
$$\psi(x, y+1) = \beta(x, y, \psi(x, y)).$$

Положим $\psi_1(x, y) = \rho(x, \psi(x, y))$. Тогда $x = \rho_1(\psi_1(x, y))$ и $\psi(x, y) = \rho_2(\psi_1(x, y))$. Функцию ψ_1 определить с помощью рекурсии типа (5), где вместо $\beta(x, y, \psi(x, y))$ применена функция вида $\delta(y, \psi(x, y))$.]

7. Допустив ρ, ρ_1, ρ_2 в качестве дополнительных исходных функций, можно ограничить применение правила рекурсии (V) схемами вида

$$(*)\quad \begin{cases} \psi(x, 0) = x \\ \psi(x, y+1) = \beta(y, \psi(x, y)) \end{cases}$$

[Указание. Применить пункт (6). Пусть тогда

$$(**)\quad \begin{cases} \varphi(x, 0) = \alpha(x) \\ \varphi(x, y+1) = \beta(y, \varphi(x, y)). \end{cases}$$

Если теперь ψ задать схемой (*) с β из схемы (**), то можно доказать, что $\varphi(x, y) = \psi(\alpha(x), y)$.]

8. Если в качестве дополнительных исходных функций принять функции $\rho, \rho_1, \rho_2, +, \cdot, \overline{sg}$, то применение правила рекурсии (V) можно ограничить схемами вида

$$f(0) = 0$$
$$f(y+1) = h(y, f(y)).$$

Указание. Пусть, согласно (7),

$$\psi(x, 0) = x,$$
$$\psi(x, y+1) = \beta(y, \psi(x, y)).$$

Положим $f(n) = \psi(\rho_1(n), \rho_2(n))$. Тогда

$$f(0) = \psi(\rho_1(0), \rho_2(0)) = \psi(0, 0) = 0,$$
$$f(n+1) = \psi(\rho_1(n+1), \rho_2(n+1)) =$$
$$= \begin{cases} \rho_2(n+1), \text{ если } \rho_1(n+1) = 0 \\ \beta(\rho_1(n+1) \dot{-} 1, \psi(\rho_1(n+1) \dot{-} 1, \rho_2(n+1))), \text{ если } \rho_1(n+1) \neq 0 \end{cases}$$
$$= \begin{cases} \rho_2(n+1), \text{ если } \rho_1(n+1) = 0 \\ \beta(\rho_1(n), \psi(\rho_1(n), \rho_2(n))), \text{ если } \rho_1(n+1) \neq 0 \end{cases}$$
$$= \begin{cases} \rho_2(n+1), \text{ если } \rho_1(n+1) = 0 \\ \beta(\rho_1(n), f(n)), \text{ если } \rho_1(n+1) \neq 0 \end{cases}$$
$$= \rho_2(n+1) \cdot \overline{sg}(\rho_1(n+1)) + \beta(\rho_1(n), f(n)) \cdot sg(\rho_1(n+1)) =$$
$$= h(n, f(n)).$$

(Заметим, что функция sg может быть построена с помощью рекурсии рассматриваемого типа). Теперь легко доказать, что $\psi(x, y) = f(\rho(x, y))$.

9. Все примитивно рекурсивные функции можно получить, исходя из функций Z, N, U_i^n, ρ, ρ_1, ρ_2, $+$, $\cdot$, $\overline{sg}$, с помощью подстановки и рекурсии

(правило (V)) вида

$$f(0) = 0,$$
$$f(y+1) = h(y, f(y)).$$

(Следует из (8).)

10. В пункте (9) функция $h(y, f(y))$ может быть заменена функцией вида $h(f(y))$. Указание. Пусть

$$f(0) = 0,$$
$$f(y+1) = h(y, f(y)).$$

Положим $g(u) = \rho(u, f(u))$ и $\varphi(w) = \rho(\rho_1(w) + 1, h(\rho_1(w), \rho_2(w)))$. Тогда

$$g(0) = 0,$$
$$g(y+1) = \varphi(g(u))$$

и

$$f(u) = \rho_2(g(u)).$$

11. Доказать, что равенства

$$\psi(n, 0) = n + 1,$$
$$\psi(0, m+1) = \psi(1, m),$$
$$\psi(n+1, m+1) = \psi(\psi(n, m+1), m)$$

определяют рекурсивную функцию. (Указание. Показать, что ψ вычислима по Эрбрану—Гёделю с помощью этих равенств, и затем применить предложение 5.17.) Доказать, кроме того:

(I) $\psi(n, m) > n$.

(II) ψ монотонна по каждой из переменных, т. е. если $x < z$, то $\psi(x, y) < \psi(z, y)$ и $\psi(y, x) < \psi(y, z)$.

(III) $\psi(n, m+1) \geqslant \psi(n+1, m)$.

(IV) Для всякой примитивно рекурсивной функции $f(x_1, \ldots, x_n)$ существует такое число m, что $f(x_1, \ldots, x_n) < \psi(\max(x_1, \ldots, x_n), m)$ для любых $x_1, \ldots, x_n$. (Указание. Доказать сначала это утверждение для исходных функций Z, N, U_i^n, ρ, ρ_1, ρ_2, $+$, $\cdot$, $\overline{sg}$, а затем показать, что истинность его сохраняется при применении подстановки и схемы рекурсии вида, который рассмотрен в (10).) В частности, для всякой примитивно рекурсивной функции $f(x)$ от одного аргумента существует число m такое, что $f(x) < \psi(x, m)$ для любого x.

(V) Показать, используя (IV), что функция $\psi(x, x) + 1$ рекурсивна, но не является примитивно рекурсивной.

Другие доказательства существования рекурсивных, но не примитивно рекурсивных функций см. у Аккермана [1928], Петер [1935], [1951], Р. Робинсона [1948].

Очень важным метаматематическим понятием является понятие рекурсивно перечислимого множества. Множество натуральных чисел называется *рекурсивно перечислимым* (р. п.), если оно либо есть пустое множество, либо есть область значений какой-нибудь рекурсивной функции. Если мы принимаем тезис Чёрча, то, говоря неформально, можно считать, что рекурсивно перечислимым является всякое множество натуральных чисел, порождаемое каким-либо механическим процессом.

Предложение 5.20. (1) *Множество* B *рекурсивно перечислимо тогда и только тогда, когда отношение* $x \in B$ *выразимо в форме* $\exists y R(x, y)$, *где* R *рекурсивно.* (*Утверждение остается в силе, если слова «*R *рекурсивно» заменить на «*R *примитивно рекурсивно».*)

(2) *Множество* B *рекурсивно перечислимо тогда и только тогда, когда оно либо пусто, либо совпадает с областью значений какой-нибудь частично рекурсивной функции.* (*Слова «частично рекурсивной» можно заменить на «примитивно рекурсивной».*)

(3) *Множество* B *рекурсивно перечислимо тогда и только тогда, когда оно совпадает с областью определения какой-либо частично рекурсивной функции.*

(4) *Множество* B *рекурсивно тогда и только тогда, когда оно само и его дополнение* $\bar{B}$ *) рекурсивно перечислимы.*

(5) *Множество* $\{x \mid \exists y T_1(x, x, y)\}$ **) *рекурсивно перечислимо, но нерекурсивно.*

Доказательство. (1) Пусть множество B рекурсивно перечислимо. Если B пусто, то $x \in B \equiv \exists y (x \neq x \,\&\, y \neq y)$. Если B непусто, то оно есть область значений некоторой рекурсивной функции φ. Тогда $x \in B \equiv \exists y (\varphi(y) = x)$. Обратно, пусть $x \in B \equiv \exists y R(x, y)$, где R рекурсивно. Если множество B пусто, то оно и рекурсивно перечислимо. Предположим теперь, что B непусто, и пусть k — какой-нибудь фиксированный элемент B. Определим функцию $\theta(z)$ условиями:

$$\theta(z) = \begin{cases} k, & \text{если } \neg R((z)_0, (z)_1), \\ (z)_0, & \text{если } R((z)_0, (z)_1). \end{cases}$$

Очевидно, что функция $\theta(z)$ — рекурсивная, и B является ее областью значений. (Кроме того, в силу леммы 5.8, если R рекурсивно, то $\exists y R(x, y) \equiv \exists y T_1(e, x, y)$ при некотором e, где T_1 — примитивно рекурсивный предикат.)

(2) Предположим, что B есть область значений частично рекурсивной функции φ. Если B пусто, то оно и рекурсивно перечислимо. Если же B непусто, то пусть k — какой-либо фиксированный его элемент. Существует такое число e, что $\varphi(x) = U(\mu y T_1(e, x, y))$. Положим

$$\theta(z) = \begin{cases} U((z)_1), & \text{если } T_1(e, (z)_0, (z)_1), \\ k, & \text{если } \neg T(e, (z)_0, (z)_1). \end{cases}$$

Очевидно, θ есть примитивно рекурсивная функция и B — ее область значений. Поэтому множество B рекурсивно перечислимо. Это же рассуждение одновременно показывает, что всякое рекурсивно перечислимое множество является областью значений примитивно рекурсивной функции.

---

*) То есть $\omega - B$, где ω — множество всех неотрицательных целых чисел.

**) Напомним, что $\{x \mid P(x)\}$ означает множество всех тех x, для которых $P(x)$ истинно.

(3) Пусть B рекурсивно перечислимо. Если $B = 0$, то B является областью определения частично рекурсивной функции $\mu y\,(x + y + 1 = 0)$. Пусть B непусто. Существует частично рекурсивная функция f, областью значений которой служит B. Тогда нетрудно видеть, что B является областью определения для частично рекурсивной функции $g(y) = \mu x\,(f(x) = y)$. Обратно, пусть B есть область определения частично рекурсивной функции φ. Существует число e такое, что $\varphi(x) = U(\mu y T_1(e, x, y))$. Отсюда $\varphi(x) = z \equiv \exists y\,(T_1(e, x, y) \,\&\, U(y) = z)$. Но, с другой стороны, $x \in B \equiv \exists z\,(\varphi(x) = z)$. Поэтому $x \in B \equiv \exists z \exists y\,(T_1(e, x, y) \,\&\, U(y) = z)$, откуда, наконец, $x \in B \equiv \exists u\,(T_1(e, x, (u)_1) \,\&\, U((u)_1) = (u)_0)$. Предикат, стоящий в этой последней формуле под знаком квантора $\exists u$, рекурсивен. Поэтому, в силу (1), множество B рекурсивно перечислимо.

(4) Следует из (1) и предположения 5.19(4)(d). (Содержательный смысл (4) состоит в том, что если имеются механические процедуры для порождения B и $\overline{B}$, то для того, чтобы узнать, принадлежит ли данное число n множеству B, нужно лишь дождаться того момента, когда это число n будет порождено одной из этих машин, и при этом заметить, какой именно.)

(5) Следует из (1) и предложения 5.19 (3).

Упражнения

1. Прообраз рекурсивно перечислимого множества при отображении посредством рекурсивной функции рекурсивно перечислим (т. е. если функция f рекурсивна и множество B рекурсивно перечислимо, то множество $\{x \mid f(x) \in B\}$ рекурсивно перечислимо). Прообраз рекурсивного множества при отображении посредством рекурсивной функции рекурсивен. При отображении посредством рекурсивной функции образ рекурсивно перечислимого множества рекурсивно перечислим, однако образ рекурсивного множества не обязательно рекурсивен.

2. Бесконечное множество рекурсивно тогда и только тогда, когда оно есть область значений строго возрастающей рекурсивной функции.

3. Бесконечное множество рекурсивно перечислимо тогда и только тогда, когда оно есть область значений взаимно однозначной рекурсивной функции.

4. Всякое бесконечное рекурсивно перечислимое множество содержит бесконечное рекурсивное подмножество.

5. Если множества A и B рекурсивно перечислимы, то рекурсивно перечислимы и множества $A \cup B$ и $A \cap B$. Существует, однако, такое рекурсивно перечислимое множество A, что $\omega - A$ не является рекурсивно перечислимым.

В силу предложения 5.20(3), всякое множество натуральных чисел рекурсивно перечислимо тогда и только тогда, когда при некотором n оно является областью определения ζ_n частично рекурсивной функции $U(\mu y T_1(n, x, y))$. Согласно определению ζ_n, $x \in \zeta_n$ тогда и только тогда, когда $\exists y\, T_1(n, x, y)$. Назовем число n *индексом множества* ζ_n. Таким образом, мы получаем *нумерацию* (с повторениями) $\zeta_1, \zeta_2, \ldots$ *всех рекурсивно перечислимых множеств.*

Как мы уже видели (предложение 5.20(5)), примером рекурсивно перечислимого, но нерекурсивного множества может служить множество всех тех x, для которых $\exists y\, T_1(x, x, y)$. В силу предложения 5.20(4), дополнение к этому множеству, т. е. множество $\{x \mid \forall y \neg T_1(x, x, y)\}$, не является рекурсивно перечислимым.

Упражнения

1. Множество B называется *креативным*, если оно рекурсивно перечислимо и если существует такая частично рекурсивная функция φ, что для любого n, если $\zeta_n \subseteq B$, то $\varphi(n)$ определено и $\varphi(n) \in \bar{B} - \zeta_n$. Доказать, что множество $\{x \mid \exists y\, T_1(x, x, y)\}$ креативно. (Указание. Пусть $\varphi(n) = n$ при любом n.) Показать также, что всякое креативное множество нерекурсивно.

2. Частично рекурсивная функция φ называется *потенциально рекурсивной*, если существует такая рекурсивная функция ψ, что $\varphi(x_1, \ldots, x_n) = \psi(x_1, \ldots, x_n)$ всякий раз, когда $\varphi(x_1, \ldots, x_n)$ определено. Показать, что функция $\mu y T_1(x, x, y)$ не является потенциально рекурсивной. (Указание. Если бы существовало рекурсивное продолжение $\psi(x)$ функции $\mu y\, T_1(x, x, y)$, то оказалось бы, что предикат $\exists y\, T_1(x, x, y)$ эквивалентен рекурсивному предикату $T_1(x, x, \psi(x))$.)

[D]**3.** Множество B называется *простым*, если оно рекурсивно перечислимо, а его дополнение $\bar{B}$ бесконечно и не содержит никакого бесконечного рекурсивно перечислимого подмножества. Всякое простое множество нерекурсивно. Доказать, что простые множества существуют. (Указание. Рассмотреть множество B, являющееся областью значений функции $\varphi(z) = \sigma_1^2(\mu y\, (T_1(z, \sigma_1^2(y), \sigma_2^2(y)) \,\&\, \sigma_1^2(y) > 2z))$.)

4. Взаимно однозначную рекурсивную функцию, отображающую ω на ω, назовем *рекурсивной перестановкой*. Множества натуральных чисел X и Y называются *изоморфными*, если существует рекурсивная перестановка, отображающая X на Y. Утверждение «множества X и Y изоморфны» будет сокращенно обозначаться через $X \cong Y$.

(a) Показать, что рекурсивные перестановки образуют группу относительно операции композиции перестановок.

(b) Отношение $\cong$ является отношением эквивалентности.

(c) Если множество X рекурсивно (рекурсивно перечислимо, креативно или просто) и $X \cong Y$, то и множество Y рекурсивно (рекурсивно перечислимо, креативно или просто).

Майхилл [1955] доказал, что любые два креативные множества изоморфны. (См. также Бернайс [1957].)

5. Будем говорить, что

(i) множество X *однозначно сводимо* к множеству Y (сокращенно: XR_mY), если существует такая рекурсивная функция f, что $x \in X$ тогда и только тогда, когда $f(x) \in Y$;

(ii) множества X и Y *однозначно эквивалентны* (сокращенно: $X \equiv_m Y$), если XR_mY и YR_mX;

(iii) множество X *взаимно однозначно сводимо* к множеству Y (сокращенно: XR_1Y), если существует взаимно однозначная рекурсивная функция f такая, что $x \in X$ тогда и только тогда, когда $f(x) \in Y$;

(iv) множества X и Y *взаимно однозначно эквивалентны* (сокращенно: $X \equiv_1 Y$), если XR_1Y и YR_1X.

(a) Отношения $\equiv_m$ и $\equiv_1$ суть отношения эквивалентности.

(b) Если X креативно, Y рекурсивно перечислимо и $X \equiv_m Y$, то Y креативно. Можно показать также (Майхилл [1955]), что если X креативно, а Y рекурсивно перечислимо, то YR_mX.

(c) (Майхилл [1955].) Если XR_1Y, то XR_mY, и если $X \equiv_1 Y$, то $X \equiv_m Y$. Однако однозначная сводимость не влечет взаимно однозначную сводимость, рав-

но как и однозначная эквивалентность не влечет взаимно однозначную эквивалентность. (У к а з а н и е. Пусть X — простое множество, Z — бесконечное рекурсивное подмножество X и Y = X — Z. Тогда XR_1Y, YR_mX, но не YR_1X.) Можно также доказать, что $X \equiv_1 Y$ тогда и только тогда, когда $X \simeq Y$.

6. (Д е к к е р [1955].) Множество X называется *продуктивным*, если существует частично рекурсивная функция f такая, что для всякого множества ζ_n, являющегося подмножеством X, $f(n) \in X - \zeta_n$.

(a) Если множество X — продуктивное, то оно не может быть рекурсивно перечислимым; следовательно, оно и его дополнение $\overline{X}$ бесконечны.

[D](b) Всякое продуктивное множество X содержит бесконечное рекурсивно перечислимое подмножество, и, следовательно, его дополнение $\overline{X}$ не является простым.

(c) Рекурсивно перечислимое множество X креативно тогда и только тогда, когда его дополнение $\overline{X}$ является продуктивным.

(d) Существует $2^{\aleph_0}$ продуктивных множеств.

7. (Д е к к е р и М а й х и л л [1960].) Говорят, что множество X *рекурсивно эквивалентно* множеству Y (сокращенно $X \sim Y$), если существует взаимно однозначная частично рекурсивная функция, отображающая X на Y.

(a) Отношение $\sim$ есть отношение эквивалентности.

[D](b) Множество называется *иммунным*, если оно бесконечно и не содержит никакого бесконечного рекурсивно перечислимого подмножества. Множество X называется *изолированным*, если оно не является рекурсивно эквивалентным никакому собственному подмножеству X. (Изолированные множества можно рассматривать как некий рекурсивный аналог конечных по Дедекинду множеств.) Показать, что бесконечное множество является изолированным тогда и только тогда, когда оно иммунное.

[D](c) Существует $2^{\aleph_0}$ иммунных множеств.

Для того, кто принимает тезис Чёрча, рекурсивно перечислимые множества важны еще и потому, что для всякой эффективно аксиоматизированной теории первого порядка K рекурсивно перечислимым оказывается множество T_K гёделевых номеров теорем теории K (что, впрочем, справедливо и вообще для всякой формальной эффективно аксиоматизированной теории). В самом деле, если множество гёделевых номеров аксиом теории K рекурсивно (а это так, если наша теория K эффективно аксиоматизирована и если мы принимаем тезис Чёрча), то рекурсивно, очевидно, и отношение Pf(y, x) («y есть гёделев номер вывода в K формулы с гёделевым номером x»). А так как $x \in T_K \equiv \equiv \exists y\, Pf(y, x)$, то T_K рекурсивно перечислимо. Приняв тезис Чёрча, мы можем также утверждать, что теория K эффективно разрешима тогда и только тогда, когда множество T_K рекурсивно. В предложении 3.41 мы показали, что всякое непротиворечивое расширение K теории RR рекурсивно неразрешимо, т. е. что соответствующие множества нерекурсивны.

В этом направлении могут быть доказаны и некоторые гораздо более общие результаты (см. Ш м у л ь я н [1961], Ф е ф е р м а н [1957], П у т н а м [1957], Э р е н ф о й х т и Ф е ф е р м а н [1960], М а й х и л л [1955]). Так, например, (1) если всякое рекурсивное множество выразимо в теории K, то эта теория существенно рекурсивно неразрешима, т. е. для

всякого непротиворечивого расширения K′ теории K множество $T_{K'}$ нерекурсивно (см. упражнение 3, ниже); (2) если K есть непротиворечивая теория первого порядка с равенством, в которой представимы все рекурсивные функции и которая удовлетворяет условиям (i) и (ii) на стр. 163, то соответствующее этой теории множество T_K креативно. (Здесь предполагается также, что K имеет среди своих термов все цифры $\bar{0}$, $\bar{1}$, $\bar{2}$, ...) Читателя, интересующегося более обстоятельным изучением рекурсивно перечислимых множеств, мы отсылаем к Посту [1944] и к Роджерсу [1956].

Упражнения

1. Всякому множеству A натуральных чисел поставим в соответствие множество A*, которое определим следующим образом: $u \in A^*$ тогда и только тогда, когда u есть гёделев номер некоторой формулы $\mathfrak{A}(x_1)$ и гёделев номер формулы $\mathfrak{A}(\bar{n})$ принадлежит A. Если A рекурсивно, то рекурсивно и A*.

2. Пусть T_K — множество гёделевых номеров всех теорем непротиворечивой теории первого порядка K. Тогда $(\overline{T}_K)^*$ невыразимо в K. [Указание. Допустим, что $(\overline{T}_K)^*$ выразимо в K с помощью некоторой формулы $\mathfrak{B}(x_1)$. Тогда $\vdash_K \mathfrak{B}(\bar{n})$ для любого n в том и только в том случае, когда $n \in (\overline{T}_K)^*$. (Это последнее утверждение слабее факта выразимости $(\overline{T}_K)^*$ в K посредством $\mathfrak{B}(x_1)$.) Пусть гёделев номер формулы $\mathfrak{B}(x_1)$ равен p. Тогда $\vdash_K \mathfrak{B}(\bar{p})$ эквивалентно $p \in (\overline{T}_K)^*$. Следовательно, $\vdash_K \mathfrak{B}(\bar{p})$ тогда и только тогда, когда гёделев номер формулы $\mathfrak{B}(\bar{p})$ принадлежит $\overline{T}_K$, т. е. $\vdash_K \mathfrak{B}(\bar{p})$ тогда и только тогда, когда не $\vdash_K \mathfrak{B}(\bar{p})$.]

3. Если всякое рекурсивное множество выразимо в теории K, то эта теория существенно рекурсивно неразрешима. (Достаточно показать, что нерекурсивно множество T_K, так как всякое рекурсивное множество выразимо, очевидно, и во всяком расширении теории K. Допустим, что T_K рекурсивно. Тогда рекурсивно $\overline{T}_K$, а в силу предыдущего упражнения 1, рекурсивно и $(\overline{T}_K)^*$. Следовательно, $(\overline{T}_K)^*$ выразимо в K, что противоречит предыдущему упражнению 2.)

§ 4. Неразрешимые проблемы

Массовая проблема (т. е. бесконечный класс однотипных проблем) называется неразрешимой, если не существует единой эффективной (или механической) процедуры, с помощью которой мог бы быть решен любой частный случай этой проблемы (т. е. любая проблема данного класса). Так, например, имеет смысл ставить вопрос о неразрешимости массовой проблемы, состоящей в том, чтобы по заданному многочлену с целыми коэффициентами узнавать, существуют ли целые значения переменных, которые обращают этот многочлен в нуль. Хотя мы умеем решать этот вопрос для некоторых многочленов специального вида, однако до сих пор неизвестно, существует ли для решения этой проблемы общая эффективная процедура, дающая ответ в любом ее частном случае (см. примечание редактора на стр. 228).

Если мы умеем арифметизировать формулировку массовой проблемы, т. е. если мы можем отнести каждому частному случаю массовой проблемы свое натуральное число в качестве ее номера, то эта массовая проблема неразрешима тогда и только тогда, когда не существует эффективно вычислимой функции h такой, что если n есть номер какого-нибудь частного случая массовой проблемы, то $h(n)$ есть решение этого частного случая. В силу тезиса Чёрча (который мы принимаем на протяжении настоящего параграфа), эта функция должна быть частично рекурсивной, и тогда мы приходим к некоторой точной математической задаче. Примерами важных математических проблем разрешения, которые были решены (отрицательно), являются проблема тождества для полугрупп (Пост [1947] *), Клини [1952], § 71) и весьма трудная проблема тождества для групп (Новиков [1955], Бун [1959], Бриттон [1958], Хигмен [1961]). Кроме того, для целого ряда теорий первого порядка получено отрицательное решение проблемы разрешения для выводимости, т. е. доказано, что ни для какой из этих теорий не существует единой эффективной процедуры, позволяющей, коль скоро задана формула $\mathscr{A}$ такой теории, ответить на вопрос, выводима или нет в этой теории формула $\mathscr{A}$ (см. следствие 3.36, следствие 3.37, предложение 3.41, следствие 3.45, лемму 3.46). Мы приведем здесь еще несколько примеров неразрешимых массовых проблем.

Последовательность функций $\psi_n(x) = U(\mu y\, T_1(n, x, y))$ дает, как мы знаем, нумерацию всех одноместных частично рекурсивных функций. Существует ли эффективная процедура, позволяющая для любого n узнавать, является функция рекурсивной (т. е. всюду определенной) или нет? Положительный ответ на этот вопрос был бы равносилен утверждению, что рекурсивно множество A тех значений n, для которых функция ψ_n рекурсивна. Мы сейчас покажем, что множество A не является даже рекурсивно перечислимым. Допустим, что A рекурсивно перечислимо. Пусть тогда h — рекурсивная функция, область значений которой совпадает с A. Рассмотрим функцию $f(x) = \psi_{h(x)}(x) + 1 = [U(\mu y T_1(h(x), x, y))] + 1$. Эта функция, очевидно, рекурсивна, и потому существует такое натуральное число m, что $f = \psi_m$ и $m \in A$. Тогда, следовательно, $\psi_m(x) = \psi_{h(x)}(x) + 1$. Так как $m \in A$, то $m = h(k)$ при некотором k. Отсюда при $x = k$ получаем $\psi_m(k) = \psi_m(k) + 1$, что невозможно. Таким образом, не существует эффективной процедуры, следуя которой, можно было бы для любой системы равенств узнавать, определяет ли она рекурсивную функцию.

Можно доказать также и некоторую «локальную» форму этого результата. Поставим такой вопрос: существует ли единый эффективный метод, позволяющий для любых m и n узнавать, определено ли значение $\psi_n(m)$? Ответ и здесь оказывается отрицательным. В самом деле,

*) Независимо от Поста и одновременно с ним неразрешимость проблемы тождества слов для полугрупп доказал А. А. Марков [1947]. (*Прим. перев.*)

допустим, что рекурсивной является функция $\theta(x, y)$, определенная следующим образом:

$$\theta(x, y) = \begin{cases} 0, & \text{если } \psi_x(y) \text{ определено,} \\ 1, & \text{если } \psi_x(y) \text{ не определено.} \end{cases}$$

Положим $\alpha(z) = \mu y(\theta(z, z) = 1 \ \& \ y = y)$. Как легко видеть,

$$\alpha(z) = \begin{cases} 0, & \text{если } \psi_z(z) \text{ не определено,} \\ \text{не определено,} & \text{если } \psi_z(z) \text{ определено.} \end{cases}$$

Так как α есть частично рекурсивная функция, то $\alpha = \psi_k$ при некотором k. Тогда

$$\psi_k(k) = \alpha(k) = \begin{cases} 0, & \text{если } \psi_k(k) \text{ не определено,} \\ \text{не определено,} & \text{если } \psi_k(k) \text{ определено,} \end{cases}$$

что является противоречием. (Другие примеры неразрешимых массовых проблем можно найти у Роджерса [1956].)

Упражнения

1. Пусть дана машина Тьюринга T. Существует ли эффективная процедура, позволяющая для любой конфигурации α решать вопрос о существовании вычисления машины T, начинающегося с α? (*Проблема остановки* для T.) Показать, что существуют машины Тьюринга с неразрешимой проблемой остановки. (Указание. Пусть T — машина Тьюринга, вычисляющая функцию $\mu y T_1(x, x, y)$; применить предложение 5.19(3).) Эта и некоторые сходные проблемы рассматриваются у Девиса ([1958], гл. 5).

2. Не существует нормального алгорифма над алфавитом $M = \{1, *\}$, который был бы применим к слову $\bar{n}$ в M тогда и только тогда, когда n есть гёделев номер нормального алгорифма над M, неприменимого к $\bar{n}$.

Ряд других примеров неразрешимых массовых проблем в теории алгорифмов можно найти у Маркова [1954], гл. V. В силу эквивалентности различных способов уточнения понятия эффективной вычислимости, которые мы находим соответственно в теориях нормальных алгорифмов, машин Тьюринга и систем равенств Эрбрана—Гёделя, всякая теорема о неразрешимости в терминах одной из этих теорий может быть переформулирована в некоторую теорему о неразрешимости в терминах любой из двух остальных теорий.

3. Функция f, определенная условиями

$$f(x) = \begin{cases} 0, & \text{если } \psi_x(x) \text{ определено,} \\ 1, & \text{если } \psi_x(x) \text{ не определено,} \end{cases}$$

нерекурсивна. (Здесь и ниже $\psi_n(x) = U(\mu y(T_1(n, x, y)))$.)

[D] **4.** Доказать существование такой рекурсивной функции $\eta(x)$, что для любого x $\eta(x)$ есть индекс частично рекурсивной функции $v(y)$, где

$$v(y) = \begin{cases} 0, & \text{если } \psi_x(x) \text{ определено,} \\ \text{не определено,} & \text{если } \psi_x(x) \text{ не определено.} \end{cases}$$

[D] **5.** (Роджерс.) Показать, что следующие отношения нерекурсивны (и потому, в силу тезиса Чёрча, неразрешимы).

(a) y принадлежит области значений ψ_x.

(b) $\psi_x(y) = z$.

(c) $\psi_x = \psi_y$. (Указание. Применить предыдущие упражнения 4 и 3.)

У читателя не должно создаться впечатления, что все проблемы разрешения решаются отрицательно. В самом деле, вспомним, например, что в главе 1 мы видели, как с помощью таблиц истинности можно для любой пропозициональной формы установить, является ли она тавтологией. Далее, на стр. 174 было показано, что разрешимо чистое исчисление одноместных предикатов (У Аккермана [1954] и Шураньи [1959] можно найти много других положительных результатов такого рода.) Пресбургер [1929] показал, что разрешима теория первого порядка, которая получается из теории S, если из числа ее элементарных символов удалить знак умножения, а в списке аксиом опустить относящиеся к умножению аксиомы (см. стр. 131, упражнение 4). Шмелева [1955] доказала разрешимость теории первого порядка для абелевых групп. Наконец, укажем еще на принадлежащее Тарскому [1951] доказательство разрешимости теории первого порядка для вещественно замкнутых полей, которая представляет собой элементарный фрагмент теории вещественных чисел.

Дополнение

Доказательство непротиворечивости формальной арифметики

Первое доказательство непротиворечивости теории первого порядка S арифметики было дано Генценом [1936], [1938b]. Сходные доказательства были впоследствии предложены Аккерманом [1940], Лоренценом [1951], Шютте [1951], [1960] и Хлодовским [1959] *). Во всех этих доказательствах используются методы, которые, очевидно, в силу второй теоремы Гёделя, не могут быть выражены в рамках самой теории S. Мы здесь изложим доказательство непротиворечивости формальной арифметики, следуя Шютте [1951].

Будем доказывать непротиворечивость некоторой системы S_∞, которая значительно сильнее теории S. Система S_∞ имеет ту же, что и теория S, предметную константу 0, те же функциональные буквы $+$, $\cdot$, $'$ и ту же предикатную букву $=$. Таким образом, теория S и система S_∞ имеют одни и те же термы и элементарные формулы (т. е. формулы вида $t = s$, где t и s — термы). Однако элементарными пропозициональными связками в S_∞ будут в отличие от S не $\supset$ и $\neg$, а $\bigvee$ и $\neg$. Формулу в S_∞ мы определим как всякое выражение, построенное из элементарных формул с помощью конечного числа применений связок $\bigvee$, $\neg$ и кванторов $\forall x_i$ ($i = 1, 2, \ldots$). Вместо $(\neg \mathfrak{A}) \vee \mathfrak{B}$ мы будем писать $\mathfrak{A} \supset \mathfrak{B}$; таким образом, всякая формула теории S будет служить обозначением некоторой формулы системы S_∞. Замкнутую элементарную формулу $s = t$ (т. е. элементарную формулу без переменных) назовем *корректной*, если, вычисляя с помощью обычных рекуррентных равенств для $+$ и $\cdot$ значения s и t, мы обнаруживаем, что эти значения равны; в противном случае эту формулу назовем *некорректной*. Очевидно, по любой данной замкнутой элементарной формуле можно эффективно определять, является ли она корректной или нет.

В качестве аксиом S_∞ мы берем: (a) все корректные замкнутые элементарные формулы, (b) отрицания всех некорректных замкнутых элементарных формул. Так, например, формулы $(0'') \cdot (0'') + 0'' = (0''') \cdot (0'')$ и $0' + 0'' \neq 0' \cdot 0''$ являются аксиомами S_∞.

S_∞ имеет следующие правила вывода:

I. Слабые правила

(a) *Перестановка:* $\dfrac{\mathfrak{C} \vee \mathfrak{A} \vee \mathfrak{B} \vee \mathfrak{D}}{\mathfrak{C} \vee \mathfrak{B} \vee \mathfrak{A} \vee \mathfrak{D}}$.

(b) *Сокращение:* $\dfrac{\mathfrak{A} \vee \mathfrak{A} \vee \mathfrak{D}}{\mathfrak{A} \vee \mathfrak{D}}$.

*) См. также П. С. Новиков [1943]. (*Прим. ред.*)

II. Сильные правила

(a) *Ослабление:* $\dfrac{\mathscr{D}}{\mathscr{A} \vee \mathscr{D}}$ (где $\mathscr{A}$ — произвольная замкнутая формула).

(b) *Правило де Моргана:* $\dfrac{\neg \mathscr{A} \vee \mathscr{D} \quad \neg \mathscr{B} \vee \mathscr{D}}{\neg (\mathscr{A} \vee \mathscr{B}) \vee \mathscr{D}}$.

(c) *Отрицание:* $\dfrac{\mathscr{A} \vee \mathscr{D}}{\neg\neg \mathscr{A} \vee \mathscr{D}}$.

(d) *Квантификация:* $\dfrac{\neg \mathscr{A}(t) \vee \mathscr{D}}{(\neg \forall x \mathscr{A}(x)) \vee \mathscr{D}}$ (где t — постоянный терм).

(e) *Бесконечная индукция:* $\dfrac{\mathscr{A}(n) \vee \mathscr{D} \text{ для любого натурального } n}{(\forall x \mathscr{A}(x)) \vee \mathscr{D}}$.

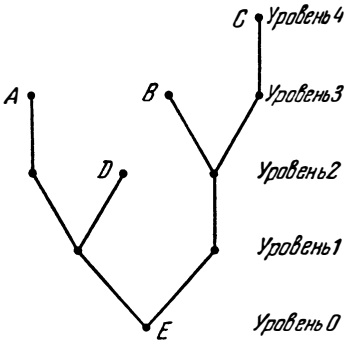
III. Сечение: $\dfrac{\mathscr{C} \vee \mathscr{A} \quad \neg \mathscr{A} \vee \mathscr{D}}{\mathscr{C} \vee \mathscr{D}}$.

Во всех этих правилах формулы, стоящие над чертой, называются *посылками*, а формулы, стоящие под чертой, — *заключениями*. Формулы, обозначенные буквами $\mathscr{C}$ и $\mathscr{D}$, называются *боковыми* формулами правила. Впрочем, одна или обе боковые формулы могут отсутствовать во всяком правиле, за исключением правила ослабления (II (a)), где обязательно присутствие формулы $\mathscr{D}$, и правила сечения (III), где должна присутствовать по крайней мере одна из формул $\mathscr{C}$, $\mathscr{D}$. Так, например, $\dfrac{\mathscr{A} \quad \neg \mathscr{A} \vee \mathscr{D}}{\mathscr{D}}$ есть сечение, а $\dfrac{\neg \mathscr{A} \quad \neg \mathscr{B}}{\neg (\mathscr{A} \vee \mathscr{B})}$ представляет собой частный случай правила де Моргана II(b). В каждом из правил формулы, не являющиеся боковыми, называются *главными* формулами данного правила; они обозначены буквами $\mathscr{A}$ и $\mathscr{B}$. Главная формула $\mathscr{A}$ сечения называется *секущей* формулой, а число пропозициональных связок и кванторов в $\neg \mathscr{A}$ называется *степенью сечения*.

Остается определить понятие вывода в S_∞. Из-за правила бесконечной индукции это понятие гораздо сложнее, чем понятие вывода для S. Определим сначала понятие Г-дерева. *Г-деревом* называется граф, вершины которого следующим образом распределяются по непересекающимся «уровням»: нулевой уровень состоит из единственной вершины, называемой *заключительной вершиной*; каждая вершина $i+1$-го уровня соединена отрезком в точности с одной вершиной i-го уровня; каждая вершина P i-го уровня либо не соединена ни с какой вершиной $i+1$-го уровня, либо соединена отрезками с одной, двумя или счетным множеством вершин $i+1$-го уровня (эти вершины $i+1$-го уровня называются *предшественниками* вершины P); всякая вершина i-го уровня может быть соединена только с вершинами $i-1$-го и $i+1$-го уровней; вершина i-го уровня, не соединенная ни с какой вершиной $i+1$-го уровня, называется *начальной вершиной*.

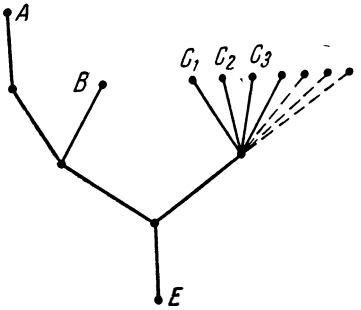
Примеры Г-деревьев

(1)



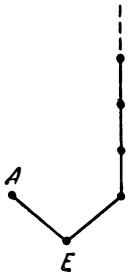
A, B, C, D — начальные вершины, E — заключительная вершина.

(2)



A, B, C_1, C_2, C_3 ... — начальные вершины, E — заключительная вершина.

(3)



A — единственная начальная вершина, E — заключительная вершина.

Под *деревом вывода* мы понимаем такое распределение формул системы S_∞ по вершинам Г-дерева, при котором

(1) формулы, отнесенные к начальным вершинам Г-дерева, суть аксиомы;

(2) формулы, отнесенные к не начальной вершине P и ее предшественникам, являются соответственно заключением и посылками какого-нибудь правила вывода;

(3) существует максимальная степень среди степеней сечений, встречающихся в дереве вывода; эта степень называется *степенью дерева вывода* (если в дереве вывода нет сечений, то степень его равна 0);

(4) каждой формуле, встречающейся в дереве вывода, отнесено некоторое порядковое число таким образом, что (a) посылке и заключению слабого правила вывода отнесено одно и то же порядковое число, (b) порядковое число, отнесенное заключению любого сильного правила или правила сечения, больше порядковых чисел, отнесенных соответствующим посылкам.

Формула, помещенная в заключительной вершине дерева вывода, называется *заключительной формулой* дерева вывода. Порядковое число, отнесенное заключительной формуле, называется *порядком дерева вывода*. Дерево вывода называется *выводом* своей заключительной формулы. Формула $\mathfrak{A}$ называется *теоремой системы* S_∞, если существует вывод $\mathfrak{A}$, т. е. если существует дерево вывода, в котором $\mathfrak{A}$ есть заключительная формула. Так как все аксиомы S_∞ суть замкнутые формулы и так как применение правил вывода к замкнутым формулам приводит снова к замкнутым формулам, то всякая теорема системы S_∞ есть замкнутая формула.

Конечная или счетная последовательность формул $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ называется *нитью* данного дерева вывода, если $\mathfrak{A}_1$ есть заключительная формула этого дерева вывода и всякая формула $\mathfrak{A}_{i+1}$ есть предшественник $\mathfrak{A}_i$. Следовательно, последовательность ординальных чисел $\alpha_1, \alpha_2, \ldots$, соответствующих формулам некоторой нити, не возрастает, и эти числа убывают с каждым применением строгого правила или сечения. Так как невозможна бесконечная строго убывающая последовательность порядковых чисел, то всякая нить всякого дерева вывода содержит лишь конечное число случаев применения сильного правила вывода или сечений. Кроме того, для любой данной формулы всегда возможно обойтись лишь конечным числом последовательных применений к ней одних только слабых правил. Ввиду этого мы добавим в качестве дополнительного условия в определении дерева вывода требование, чтобы в каждой нити всякого дерева вывода участки последовательных применений слабых правил вывода были конечны. Тогда во всяком дереве вывода любая нить будет конечна.

Если мы ограничим каким-либо условием класс порядковых чисел, которые в соответствии с условием (4) должны приписываться вершинам дерева вывода, то тем самым будет ограничено и понятие дерева вывода, и, быть может, мы даже получим более узкое множество теорем. Полученные при этом системы и используемые ниже методы доказательства непротиворечивости будут в большей или меньшей степени «конструктивными» в зависимости от того, какие «конструктивные» отрезки порядковых чисел будут использованы.

Упражнение

Показать, что правила сочетания $\dfrac{(\mathscr{C} \vee \mathscr{A}) \vee \mathscr{B}}{\mathscr{C} \vee (\mathscr{A} \vee \mathscr{B})}$ и $\dfrac{\mathscr{C} \vee (\mathscr{A} \vee \mathscr{B})}{(\mathscr{C} \vee \mathscr{A}) \vee \mathscr{B}}$ являются производными от правила перестановки, предполагая, что в последнем опущены скобки, сочетающие влево. Следовательно, в дизъюнкции скобки можно опускать.

Лемма А.1. *Пусть общее число входящих в замкнутую формулу $\mathscr{A}$ пропозициональных связок и кванторов равно n. Тогда существует (не содержащий сечений) вывод порядка $\leqslant 2n+1$ формулы $\neg \mathscr{A} \vee \mathscr{A}$.*

Доказательство. Индукция по n. (1) $n=0$, т. е. $\mathscr{A}$ есть элементарная замкнутая формула. Одна из формул $\neg \mathscr{A}$ или $\mathscr{A}$ является аксиомой, так как $\mathscr{A}$ есть либо корректная, либо некорректная формула. Тогда, в силу правила ослабления (II (а)), одно из следующих построений является деревом вывода:

$$\text{ослабление}\ \dfrac{\mathscr{A}}{\neg \mathscr{A} \vee \mathscr{A}} \qquad \text{ослабление}\ \dfrac{\text{ослабление}\ \dfrac{\neg \mathscr{A}}{\mathscr{A} \vee \neg \mathscr{A}}}{\neg \mathscr{A} \vee \mathscr{A}}\ \text{перестановка}$$

При этом, очевидно, вершинам дерева вывода можно приписать порядковые числа таким образом, чтобы порядок вывода был равен 1.

(2) Предположим, что лемма верна для любого $k<n$.

(i) Пусть $\mathscr{A}$ есть $\mathscr{A}_1 \vee \mathscr{A}_2$. Согласно индуктивному предположению, существуют выводы формул $\neg \mathscr{A}_1 \vee \mathscr{A}_1$ и $\neg \mathscr{A}_2 \vee \mathscr{A}_2$ порядков $\leqslant 2(n-1)+1 = 2n-1$. Тогда с помощью правил ослабления и перестановки мы можем построить выводы порядка $2n$ для формул $\neg \mathscr{A}_1 \vee \vee \mathscr{A}_1 \vee \mathscr{A}_2$ и $\neg \mathscr{A}_2 \vee \mathscr{A}_1 \vee \mathscr{A}_2$, а с помощью правила де Моргана и вывод порядка $2n+1$ для формулы $\neg(\mathscr{A}_1 \vee \mathscr{A}_2) \vee \mathscr{A}_1 \vee \mathscr{A}_2$.

(ii) Пусть $\mathscr{A}$ есть $\neg \mathscr{B}$. По индуктивному предположению, существует вывод порядка $2n-1$ формулы $\neg \mathscr{B} \vee \mathscr{B}$. С помощью этого вывода и правила перестановки построим вывод порядка $2n-1$ формулы $\mathscr{B} \vee \neg \mathscr{B}$. Теперь с помощью правила отрицания достраиваем этот вывод до вывода формулы $\neg \neg \mathscr{B} \vee \neg \mathscr{B}$, т. е. формулы $\neg \mathscr{A} \vee \mathscr{A}$. Порядок этого последнего вывода равен $2n \leqslant 2n+1$.

(iii) Пусть $\mathscr{A}$ есть $\forall x \mathscr{B}(x)$. В силу индуктивного предположения, для любого натурального k существует вывод формулы $\neg \mathscr{B}(\bar{k}) \vee \mathscr{B}(\bar{k})$, имеющий порядок $\leqslant 2n-1$. Тогда с помощью правила квантификации получим вывод порядка $\leqslant 2n$ формулы $\neg \forall x \mathscr{B}(x) \vee \mathscr{B}(\bar{k})$. Применяя затем последовательно правила перестановки, бесконечной индукции и снова перестановки, построим выводы порядков соответственно $\leqslant 2n$, $\leqslant 2n+1$ и снова $\leqslant 2n+1$ для формул $\mathscr{B}(\bar{k}) \vee \neg \forall x \mathscr{B}(x)$, $\forall x \mathscr{B}(x) \vee \vee \neg \forall x \mathscr{B}(x)$ и $\neg \forall x \mathscr{B}(x) \vee \forall x \mathscr{B}(x)$.

Лемма А.2. *Для любых постоянных термов s и t и для любой формулы $\mathscr{A}(x)$ с единственной свободной переменной x формула*

$s \neq t \vee \neg \mathscr{A}(s) \vee \mathscr{A}(t)$ является теоремой и выводима без употребления правила сечения.

Доказательство. Заметим сначала, что если замкнутая формула $\mathscr{B}(t)$ выводима в S_∞ и s имеет значение, равное значению t, то формула $\mathscr{B}(s)$ тоже выводима в S_∞. (Чтобы убедиться в этом, достаточно в выводе $\mathscr{B}(t)$ все вхождения t, «дедуктивно связанные» с вхождением t в заключительную формулу $\mathscr{B}(t)$, заменить на s.) Если термы s и t имеют одно и то же значение $\bar{n}$, то, в силу предыдущего замечания и выводимости формулы $\neg \mathscr{A}(\bar{n}) \vee \mathscr{A}(\bar{n})$, выводима формула $\neg \mathscr{A}(s) \vee \vee \mathscr{A}(t)$. Следовательно, в этом случае выводима и формула $s \neq t \vee \vee \neg \mathscr{A}(s) \vee \mathscr{A}(t)$ (правило ослабления). Если же значения термов s и t не равны между собой, то $s = t$ есть некорректная формула, и тогда $s \neq t$ является аксиомой. Отсюда с помощью правил ослабления и перестановки получаем, что формула $s \neq t \vee \neg \mathscr{A}(s) \vee \mathscr{A}(t)$ выводима.

Лемма А.3. *Всякая выводимая в* S *замкнутая формула есть теорема системы* S_∞.

Доказательство. Пусть замкнутая формула $\mathscr{A}$ является теоремой теории S. Очевидно, всякий вывод в S может быть представлен в форме конечного дерева вывода, где начальными формулами служат аксиомы S, а правилами вывода являются modus ponens и Gen. Пусть n — порядок такого дерева вывода для $\mathscr{A}$.

Если $n = 0$, то $\mathscr{A}$ есть аксиома S (см. стр. 65 — 66, 116). Здесь возможны следующие случаи.

(1) $\mathscr{A}$ есть $\mathscr{B} \supset (\mathscr{C} \supset \mathscr{B})$, т. е. $\neg \mathscr{B} \vee (\neg \mathscr{C} \vee \mathscr{B})$. Так как из замкнутости $\mathscr{A}$ следует, что формула $\mathscr{B}$ также замкнута, то, по лемме А.1, формула $\neg \mathscr{B} \vee \mathscr{B}$ выводима в S_∞. Следовательно, на основании правил ослабления и перестановки, выводима в S_∞ и формула $\neg \mathscr{B} \vee \neg \mathscr{C} \vee \mathscr{B}$.

(2) $\mathscr{A}$ есть $(\mathscr{B} \supset (\mathscr{C} \supset \mathscr{D})) \supset ((\mathscr{B} \supset \mathscr{C}) \supset (\mathscr{B} \supset \mathscr{D}))$, т. е. $\neg(\neg \mathscr{B} \vee \vee (\neg \mathscr{C} \vee \mathscr{D})) \vee \neg(\neg \mathscr{B} \vee \mathscr{C}) \vee (\neg \mathscr{B} \vee \mathscr{D})$. По лемме А.1, в S_∞ выводимы формулы $\neg(\neg \mathscr{B} \vee \mathscr{C}) \vee \neg \mathscr{B} \vee \mathscr{C}$ и $(\neg \mathscr{B} \vee \neg \mathscr{C} \vee \mathscr{D}) \vee \neg(\neg \mathscr{B} \vee \vee \neg \mathscr{C} \vee \mathscr{D})$. Теперь выводимость $\mathscr{A}$ в S_∞ легко устанавливается с помощью правил перестановки, сечения (с секущей формулой $\mathscr{C}$) и сокращения.

(3) $\mathscr{A}$ есть $(\neg \mathscr{B} \supset \neg \mathscr{C}) \supset ((\neg \mathscr{B} \supset \mathscr{C}) \supset \mathscr{B})$, т. е. $\neg(\neg \neg \mathscr{B} \vee \vee \neg \mathscr{C}) \vee \neg(\neg \neg \mathscr{B} \vee \mathscr{C}) \vee \mathscr{B}$. Прежде всего, по лемме А.1, имеем $\vdash_{S_\infty} \neg \mathscr{B} \vee \mathscr{B}$, затем с помощью правила отрицания $\vdash_{S_\infty} \neg \neg \neg \mathscr{B} \vee \mathscr{B}$ и по правилам ослабления и перестановки

(a) $\vdash_{S_\infty} \neg \neg \neg \mathscr{B} \vee \neg(\neg \neg \mathscr{B} \vee \mathscr{C}) \vee \mathscr{B}$.

Аналогично доказывается $\vdash_{S_\infty} \neg \neg \neg \mathscr{B} \vee \mathscr{B} \vee \neg \neg \mathscr{C}$ и $\vdash_{S_\infty} \neg \mathscr{C} \vee \vee \mathscr{B} \vee \neg \neg \mathscr{C}$, откуда по правилу де Моргана следует $\vdash_{S_\infty} \neg(\neg \neg \mathscr{B} \vee \mathscr{C}) \vee \vee \mathscr{B} \vee \neg \neg \mathscr{C}$. Применив теперь правило перестановки, получаем

(b) $\vdash_{S_\infty} \neg \neg \mathscr{C} \vee \neg(\neg \neg \mathscr{B} \vee \mathscr{C}) \vee \mathscr{B}$.

Из (a) и (b) снова по правилу де Моргана, получаем, наконец,

$$\vdash_{S_\infty} \neg(\neg\neg\mathscr{B} \vee \neg\mathscr{C}) \vee \neg(\neg\neg\mathscr{B} \vee \mathscr{C}) \vee \mathscr{B}.$$

(4) $\mathscr{A}$ есть $\forall x\mathscr{B}(x) \supset \mathscr{B}(t)$, т. е. $\neg\forall x\mathscr{B}(x) \vee \mathscr{B}(t)$. Формула $\mathscr{B}(t)$ замкнута, так как по условию замкнута формула $\mathscr{A}$. Сначала по лемме A.1 получаем $\vdash_{S_\infty} \neg\mathscr{B}(t) \vee \mathscr{B}(t)$, затем по правилу квантификации $\vdash_{S_\infty} \neg\forall x\mathscr{B}(x) \vee \mathscr{B}(t)$.

(5) $\mathscr{A}$ есть $\forall x(\mathscr{B} \supset \mathscr{C}) \supset (\mathscr{B} \supset \forall x\mathscr{C})$ (где x не является свободной переменной в формуле $\mathscr{B}$), т. е. $\neg\forall x(\neg\mathscr{B} \vee \mathscr{C}) \vee \neg\mathscr{B} \vee \forall x\mathscr{C}$. В силу леммы A.1, для любого натурального числа n существует вывод в S_∞ для $\neg(\neg\mathscr{B} \vee \mathscr{C}(\bar{n})) \vee \neg\mathscr{B} \vee \mathscr{C}(\bar{n})$, так как из замкнутости $\mathscr{A}$ следует замкнутость $\neg\mathscr{B} \vee \mathscr{C}(\bar{n})$. Заметим, что порядки этих выводов ограничены числом $2k+1$, где k есть общее число пропозициональных связок и кванторов в $\neg\mathscr{B} \vee \mathscr{C}(x)$ Следовательно, на основании правила квантификации, для любого n существует вывод в S_∞ для

$$\neg\forall x(\neg\mathscr{B} \vee \mathscr{C}(x)) \vee \neg\mathscr{B} \vee \mathscr{C}(\bar{n}) \quad \text{(с порядком } \leqslant 2k+2\text{)}.$$

Отсюда с помощью правил перестановки и бесконечной индукции получаем наконец $\vdash_{S_\infty} \neg\forall x(\neg\mathscr{B} \vee \mathscr{C}(x)) \vee \neg\mathscr{B} \vee \forall x\mathscr{C}(x)$ (с порядком вывода $\leqslant 2k+3$).

(S1) $\mathscr{A}$ есть $t_1 = t_2 \supset (t_1 = t_3 \supset t_2 = t_3)$, т. е. $t_1 \neq t_2 \vee t_1 \neq t_3 \vee t_2 = t_3$. Из замкнутости $\mathscr{A}$ следует, что t_1, t_2 и t_3 – постоянные термы. Применяем лемму A.2, беря в качестве $\mathscr{A}(x)$, s и t соответственно $x = t_3$, t_1 и t_2

(S2) $\mathscr{A}$ есть $t_1 = t_2 \supset (t_1)' = (t_2)'$, т. е. $t_1 \neq t_2 \vee (t_1)' = (t_2)'$. Если значения t_1 и t_2 равны, то равны и значения t_1' и t_2' и формула $(t_1)' = (t_2)'$ является корректной и, следовательно, аксиомой S_∞. С помощью правила ослабления получаем тогда $\vdash_{S_\infty} t_1 \neq t_2 \vee (t_1)' = (t_2)'$. Если же значения t_1 и t_2 не равны, то аксиомой является формула $t_1 \neq t_2$. Применяя правила ослабления и перестановки, получаем снова $\vdash_{S_\infty} t_1 \neq t_2 \vee (t_1)' = (t_2)'$.

(S3) $\mathscr{A}$ есть $0 \neq t'$. Так как 0 и t' всегда имеют различные значения, то $0 \neq t'$ является аксиомой S_∞.

(S4) $\mathscr{A}$ есть $(t_1)' = (t_2)' \supset t_1 = t_2$, т. е. $(t_1)' \neq (t_2)' \vee t_1 = t_2$. (Доказательство предоставляется читателю в качестве упражнения.)

(S5) $\mathscr{A}$ есть $t + 0 = t$. Так как $t + 0$ и t имеют одинаковые значения, то $t + 0 = t$ есть аксиома.

(S6) – (S8) проверяются аналогично с помощью рекуррентных равенств для вычисления значений постоянных термов.

(S9) $\mathscr{A}$ есть $\mathscr{B}(0) \supset (\forall x(\mathscr{B}(x) \supset \mathscr{B}(x')) \supset \forall x\mathscr{B}(x))$ или $\neg\mathscr{B}(0) \vee \neg\forall x(\neg\mathscr{B}(x) \vee \mathscr{B}(x')) \vee \forall x\mathscr{B}(x)$.

(1) В силу леммы A.1 и с помощью правил перестановки и ослабления получаем $\vdash_{S_\infty} \neg\mathscr{B}(0) \vee \neg\forall x(\neg\mathscr{B}(x) \vee \mathscr{B}(x')) \vee \mathscr{B}(0)$.

(2) Индукцией по $k \geqslant 0$ покажем, что

$$\vdash_{S_\infty} \neg\mathfrak{B}(0) \vee \neg(\neg\mathfrak{B}(0) \vee \mathfrak{B}(\bar{1})) \vee \ldots$$
$$\ldots \vee \neg(\neg\mathfrak{B}(\bar{k}) \vee \mathfrak{B}(\bar{k}')) \vee \mathfrak{B}(\bar{k}').$$

(a) $k = 0$. В силу леммы А. 1 и по правилам ослабления и перестановки $\vdash_{S_\infty} \neg\neg\mathfrak{B}(0) \vee \neg\mathfrak{B}(0) \vee \mathfrak{B}(\bar{1})$. Аналогично, $\vdash_{S_\infty} \neg\mathfrak{B}(\bar{1}) \vee \vee \neg\mathfrak{B}(0) \vee \mathfrak{B}(\bar{1})$. Отсюда по правилу де Моргана $\vdash_{S_\infty} \neg(\neg\mathfrak{B}(0) \vee \vee \mathfrak{B}(\bar{1})) \vee \neg\mathfrak{B}(0) \vee \mathfrak{B}(\bar{1})$ и далее с помощью правила перестановки

$$\vdash_{S_\infty} \neg\mathfrak{B}(0) \vee \neg(\neg\mathfrak{B}(0) \vee \mathfrak{B}(\bar{1})) \vee \mathfrak{B}(\bar{1}).$$

(b) Допустим, что

$$\vdash_{S_\infty} \neg\mathfrak{B}(0) \vee \neg(\neg\mathfrak{B}(0) \vee \mathfrak{B}(\bar{1})) \vee \ldots$$
$$\ldots \vee \neg(\neg\mathfrak{B}(\bar{k}) \vee \mathfrak{B}(\bar{k}')) \vee \mathfrak{B}(\bar{k}').$$

Тогда по правилам перестановки, отрицания и ослабления получаем

$$\vdash_{S_\infty} \neg\neg\mathfrak{B}(\bar{k}') \vee \neg\mathfrak{B}(0) \vee \neg(\neg\mathfrak{B}(0) \vee \mathfrak{B}(\bar{1})) \vee \ldots$$
$$\ldots \vee \neg(\neg\mathfrak{B}(\bar{k}) \vee \mathfrak{B}(\bar{k}')) \vee \mathfrak{B}(\bar{k}'').$$

Применим лемму А.1 к формуле $\mathfrak{B}(\bar{k}'')$ и затем правила ослабления и перестановки:

$$\vdash_{S_\infty} \neg\mathfrak{B}(\bar{k}'') \vee \neg\mathfrak{B}(0) \vee \neg(\neg\mathfrak{B}(0) \vee \mathfrak{B}(\bar{1})) \vee \ldots$$
$$\ldots \vee \neg(\mathfrak{B}(\bar{k}) \vee \mathfrak{B}(\bar{k}')) \vee \mathfrak{B}(\bar{k}'').$$

Отсюда по правилу де Моргана

$$\vdash_{S_\infty} \neg(\neg\mathfrak{B}(\bar{k}') \vee \mathfrak{B}(\bar{k}'')) \vee \neg\mathfrak{B}(0) \vee \neg(\neg\mathfrak{B}(0) \vee \mathfrak{B}(\bar{1})) \vee \ldots$$
$$\ldots \vee \neg(\neg\mathfrak{B}(\bar{k}) \vee \mathfrak{B}(\bar{k}')) \vee \mathfrak{B}(\bar{k}'')$$

и наконец с помощью правила перестановки

$$\vdash_{S_\infty} \neg\mathfrak{B}(0) \vee \neg(\neg\mathfrak{B}(0) \vee \mathfrak{B}(\bar{1})) \vee \ldots$$
$$\ldots \vee \neg(\neg\mathfrak{B}(\bar{k}) \vee \mathfrak{B}(\bar{k}')) \vee \neg(\neg\mathfrak{B}(\bar{k}') \vee \mathfrak{B}(\bar{k}'')) \vee \mathfrak{B}(\bar{k}''),$$

чем и завершается индукционный шаг.

Применим теперь правила перестановки и квантификации k раз к формуле, выводимость которой в S_∞ доказана только что в (2). В результате получим, что при любом $k \geqslant 0$

$$\vdash_{S_\infty} \neg\mathfrak{B}(0) \vee \forall x(\neg\mathfrak{B}(x) \vee \mathfrak{B}(x')) \vee \ldots$$
$$\ldots \vee \neg\forall x(\neg\mathfrak{B}(x) \vee \mathfrak{B}(x')) \vee \mathfrak{B}(\bar{k}'),$$

и после применений правила сокращения

$$\vdash_{S_\infty} \neg\mathscr{B}(0) \vee \neg\forall x(\neg\mathscr{B}(x) \vee \mathscr{B}(x')) \vee \mathscr{B}(\bar{k}').$$

Таким образом, вместе с (1) получаем, что при любом $k \geqslant 0$

$$\vdash_{S_\infty} \neg\mathscr{B}(0) \vee \neg\forall x(\neg\mathscr{B}(x) \vee \mathscr{B}(x')) \vee \mathscr{B}(\bar{k}).$$

Применив теперь правило бесконечной индукции, окончательно заключаем, что

$$\vdash_{S_\infty} \neg\mathscr{B}(0) \vee \neg\forall x(\neg\mathscr{B}(x) \vee \mathscr{B}(x')) \vee \forall x\mathscr{B}(x).$$

Таким образом, мы доказали, что все замкнутые аксиомы системы S выводимы в S_∞.

Предположим теперь, что $n > 0$. Здесь имеются две возможности.

(i) Формула $\mathscr{A}$ появляется при выводе по правилу modus ponens из формул $\mathscr{B}$ и $\mathscr{B} \supset \mathscr{A}$, занумерованных в дереве вывода порядковыми числами $< n$. По условию формула замкнута. Можно, очевидно, предполагать, что и $\mathscr{B}$ не содержит свободных переменных, так как в противном случае вместо всякой входящей в $\mathscr{B}$ свободной переменной можно было бы подставить 0 как в формулу $\mathscr{B}$, так и в ее последовательные предшественники в дереве вывода системы S. Тогда, в силу индуктивного предположения, $\vdash_{S_\infty} \mathscr{B}$ и $\vdash_{S_\infty} \mathscr{B} \supset \mathscr{A}$, т. е. $\vdash_{S_\infty} \neg\mathscr{B} \vee \mathscr{A}$. С помощью правила сечения отсюда получаем $\vdash_{S_\infty} \mathscr{A}$.

(ii) $\mathscr{A}$ есть $\forall x\mathscr{B}(x)$ и получается из $\mathscr{B}(x)$ по правилу Gen. Продвигаясь обратно от $\mathscr{B}(x)$ по дереву вывода системы S и заменяя подходящие свободные вхождения x на $\bar{k}$, можно получить вывод $\mathscr{B}(\bar{k})$ того же порядка, что и первоначальный вывод $\mathscr{B}(x)$. Так как это верно для любого k, то, в силу индуктивного предположения для любого k, верно $\vdash_{S_\infty} \mathscr{B}(\bar{k})$. Тогда, на основании правила бесконечной индукции, получаем $\vdash_{S_\infty} \forall x\mathscr{B}(x)$, т. е. $\vdash_{S_\infty} \mathscr{A}$.

Следствие А.4. *Если система* S_∞ *непротиворечива, то непротиворечива и теория* S.

Доказательство. Если теория S противоречива, то $\vdash_S 0 \neq 0$. Тогда, по лемме А.3, $\vdash_{S_\infty} 0 \neq 0$. Но, с другой стороны, $\vdash_{S_\infty} 0 = 0$, так как формула $0 = 0$ корректна. Поэтому для любой формулы $\mathscr{A}$ по правилу ослабления получаем $\vdash_{S_\infty} 0 \neq 0 \vee \mathscr{A}$, а вместе с $\vdash_{S_\infty} 0 = 0$ по правилу сечения — и $\vdash_{S_\infty} \mathscr{A}$. Итак, из противоречивости теории S следует, что в S_∞ выводима любая формула, т. е. следует противоречивость S_∞.

В силу следствия А.4, для того чтобы доказать непротиворечивость S, достаточно доказать непротиворечивость S_∞.

Лемма А.5. *Правила де Моргана, отрицания и бесконечной индукции обратимы, т. е. по всякому выводу формулы* $\mathscr{A}$, *которая сле-*

дует из некоторых посылок в силу одного из этих правил, можно построить вывод самих посылок (порядок и степень такого вывода не больше порядка и степени первоначального вывода для $\mathscr{A}$).

Доказательство. (1) Правило де Моргана. Формула $\mathscr{A}$ имеет вид $\neg(\mathscr{B} \vee \mathscr{C}) \vee \mathscr{D}$. Рассмотрим вывод $\mathscr{A}$. Проследим все те вхождения подформул $\neg(\mathscr{B} \vee \mathscr{C})$ в формулы этого дерева вывода, которые соответствуют выделенному вхождению $\neg(\mathscr{B} \vee \mathscr{C})$ в заключительную формулу $\mathscr{A}$. Двигаясь, таким образом, в обратном направлении от $\mathscr{A}$, мы пройдем через всякий случай применения слабого правила и через те случаи применения сильного правила, когда $\neg(\mathscr{B} \vee \mathscr{C})$ является подформулой боковой формулы. Остановка произойдет только тогда, когда мы столкнемся с применением правила ослабления вида $\dfrac{\mathscr{F}}{\neg(\mathscr{B} \vee \mathscr{C}) \vee \mathscr{F}}$ или правила де Моргана вида $\dfrac{\neg\mathscr{B} \vee \mathscr{F}\ \neg\mathscr{C} \vee \mathscr{F}}{\neg(\mathscr{B} \vee \mathscr{C}) \vee \mathscr{F}}$. Совокупность прослеживаемых таким образом вхождений формулы $\neg(\mathscr{B} \vee \mathscr{C})$ в дерево вывода назовем *историей формулы* $\neg(\mathscr{B} \vee \mathscr{C})$. Если все вхождения формулы $\neg(\mathscr{B} \vee \mathscr{C})$ в ее истории заменить на $\neg\mathscr{B}$, то (после удаления ненужных формул) в результате получится новое дерево вывода с формулой $\neg\mathscr{B} \vee \mathscr{D}$ в качестве заключительной формулы. Аналогичная замена $\neg(\mathscr{B} \vee \mathscr{C})$ на $\neg\mathscr{C}$ даст нам вывод формулы $\neg\mathscr{C} \vee \mathscr{D}$.

(2) Правило отрицания. $\mathscr{A}$ есть $\neg\neg\mathscr{B} \vee \mathscr{D}$. Определим историю $\neg\neg\mathscr{B}$ аналогично тому, как это было сделано выше для $\neg(\mathscr{B} \vee \mathscr{C})$ в (1). Заменив все вхождения $\neg\neg\mathscr{B}$ в истории этой формулы на $\mathscr{B}$, получим вывод $\mathscr{B} \vee \mathscr{D}$.

(3) Бесконечная индукция. $\mathscr{A}$ есть $\forall x \mathscr{B}(x) \vee \mathscr{D}$. Снова, как и в (1), определим историю $\forall x \mathscr{B}(x)$ и заменим всюду в ней $\forall x \mathscr{B}(x)$ на $\mathscr{B}(\bar{k})$ (если при этом какое-нибудь из начальных в этой истории вхождений $\forall x \mathscr{B}(x)$ является следствием по правилу бесконечной индукции из некоторых посылок, то удалим деревья над всеми этими посылками, кроме посылки $\mathscr{B}(\bar{k})$). Таким образом, для всякого k мы получим вывод $\mathscr{B}(\bar{k}) \vee \mathscr{D}$.

Лемма А. 6 (Шютте [1951]: Reduktionssatz.) *Если для формулы $\mathscr{A}$ в S_∞ существует вывод положительной степени m и порядка α, то для этой же формулы $\mathscr{A}$ существует вывод в S_∞ со степенью меньшей, чем m, и порядком, равным 2^α* (см. стр. 197)

Доказательство. Докажем лемму трансфинитной индукцией по порядковому числу α, являющемуся порядком данного вывода $\mathscr{A}$. Если $\alpha = 0$, то вывод не может содержать сечений и его степень равна 0. Предположим, что лемма верна для всех выводов порядков, меньших α. Исходя из заключительной формулы $\mathscr{A}$ данного нам дерева вывода порядка α, будем продвигаться по нему, пока не встретим первое применение сильного правила или правила сечения. Рассмотрим случай сильного правила. Его посылки занумерованы порядковыми числами $\alpha_i < \alpha$. Согласно индуктивному предположению, для каждой из этих посылок $\mathscr{F}$ существует дерево вывода со степенью $< m$ и порядком 2^{α_i}. Заменим

таким деревом со степенью $< m$ то поддерево данного дерева вывода для $\mathscr{A}$, заключительной формулой которого служит рассматриваемое вхождение $\mathscr{F}$. Поступив так со всеми посылками рассматриваемого применения сильного правила, мы получим новое дерево для $\mathscr{A}$, если заключительной формуле $\mathscr{A}$ отнесем порядковое число 2^{α}, которое заведомо больше всех чисел $2^{\alpha i}$ (см. предложение 4.30(9)).

Обратимся теперь к случаю правила сечения. Пусть первый встретившийся нам случай применения не слабого правила вывода имеет вид

$$\frac{\mathscr{C} \vee \mathscr{B} \quad \neg \mathscr{B} \vee \mathscr{D}}{\mathscr{C} \vee \mathscr{D}},$$

и пусть α_1, α_2 — порядковые числа, которыми занумерованы соответственно $\mathscr{C} \vee \mathscr{B}$ и $\neg \mathscr{B} \vee \mathscr{D}$. Согласно индуктивному предположению, для $\mathscr{C} \vee \mathscr{B}$ и $\neg \mathscr{B} \vee \mathscr{D}$ существуют выводы степеней меньших, чем m, и порядков соответственно 2^{α_1} и 2^{α_2}. Рассмотрим теперь возможные случаи строения главной формулы $\mathscr{B}$ этого сечения.

(a) $\mathscr{B}$ есть элементарная формула. Одна из формул $\mathscr{B}$ и $\neg \mathscr{B}$ является аксиомой. Пусть $\mathscr{K}$ есть та из этих формул, которая не есть аксиома. Согласно индуктивному предположению, поддерево основного дерева вывода для $\mathscr{A}$, заключительной формулой которого является рассматриваемое вхождение посылки, содержащей $\mathscr{K}$, может быть заменено некоторым деревом вывода той же посылки степени, меньшей m, и порядка $2^{\alpha i}$ ($i = 1$ или $i = 2$). В этом новом дереве вывода для посылки, в которую входит $\mathscr{K}$, рассмотрим историю $\mathscr{K}$ (определяемую, как в доказательстве леммы A.5). Начальные формулы в этой истории могут возникнуть только по правилу ослабления. Поэтому удаление из истории $\mathscr{K}$ всех вхождений $\mathscr{K}$ приводит к построению дерева вывода для $\mathscr{C}$ или для $\mathscr{D}$ порядка $2^{\alpha i}$. Отсюда с помощью правила ослабления получаем дерево вывода для $\mathscr{C} \vee \mathscr{D}$ порядка 2^{α}. Степень этого нового дерева вывода меньше m.

(b) $\mathscr{B}$ есть $\neg \mathscr{E}$, т. е. рассматриваемый случай применения правила сечения имеет вид

$$\frac{\mathscr{C} \vee \neg \mathscr{E} \quad \neg\neg \mathscr{E} \vee \mathscr{D}}{\mathscr{C} \vee \mathscr{D}}.$$

Существует дерево вывода для $\neg\neg \mathscr{E} \vee \mathscr{D}$ степени $< m$ и порядка 2^{α_2}. В силу леммы A.5, существует дерево вывода для $\mathscr{E} \vee \mathscr{D}$ степени $< m$ и порядка 2^{α_2}. Существует, кроме того, дерево вывода степени $< m$ и порядка 2^{α_1} для $\mathscr{C} \vee \neg \mathscr{E}$. Из этих двух последних деревьев вывода построим новое дерево вывода по схеме:

$$\dfrac{\dfrac{\dfrac{\vdots}{\mathscr{E} \vee \mathscr{D}}\ \text{перестановка}}{\mathscr{D} \vee \mathscr{E}} \qquad \dfrac{\dfrac{\vdots}{\mathscr{C} \vee \neg \mathscr{E}}\ \text{перестановка}}{\neg \mathscr{E} \vee \mathscr{C}}}{\dfrac{\mathscr{D} \vee \mathscr{C}}{\mathscr{C} \vee \mathscr{D}}\ \text{перестановка}}\ \text{сечение}$$

Степень выделенного здесь сечения на единицу меньше общего числа пропозициональных связок и кванторов в $\neg\neg\mathscr{E}$, которое само не превосходит m. Формуле $\mathscr{C} \vee \mathscr{D}$, очевидно, можно отнести в качестве номера порядковое число 2^α. Итак, мы имеем новое дерево вывода для $\mathscr{C} \vee \mathscr{D}$ степени, меньшей m, и порядка 2^α.

(c) $\mathscr{B}$ есть $\mathscr{E} \vee \mathscr{F}$, и рассматриваемое сечение имеет вид

$$\frac{\mathscr{C} \vee \mathscr{E} \vee \mathscr{F} \quad \neg(\mathscr{E} \vee \mathscr{F}) \vee \mathscr{D}}{\mathscr{C} \vee \mathscr{D}}.$$

Существует дерево вывода для $\neg(\mathscr{E} \vee \mathscr{F}) \vee \mathscr{D}$ степени $< m$ и порядка 2^{α_2}. По лемме A.5, существуют деревья вывода степеней $< m$ и порядка 2^{α_2} для $\neg\mathscr{E} \vee \mathscr{D}$ и $\neg\mathscr{F} \vee \mathscr{D}$. Существует также дерево вывода для $\mathscr{C} \vee \vee \mathscr{E} \vee \mathscr{F}$ степени, меньшей m, и порядка 2^{α_1}. Из последних трех деревьев построим новое дерево вывода по схеме:

$$\dfrac{\dfrac{\dfrac{\mathscr{C} \vee \mathscr{E} \vee \mathscr{F} \quad \neg\mathscr{F} \vee \mathscr{D}}{\text{сечение}\ \ \mathscr{C} \vee \mathscr{E} \vee \mathscr{D}}}{\text{перестановка}\ \ \mathscr{C} \vee \mathscr{D} \vee \mathscr{E}} \quad \neg\mathscr{E} \vee \mathscr{D}}{\begin{array}{c}\text{сечение}\\ \mathscr{C} \vee \mathscr{D} \vee \mathscr{D}\end{array}}$$

$$\begin{array}{c}\text{перестановка}\\ \text{и сокращение}\\ \mathscr{C} \vee \mathscr{D}\end{array}$$

Выделенные здесь сечения имеют степени $< m$; следовательно, и все новое дерево вывода имеет степень $< m$. Формуле $\mathscr{C} \vee \mathscr{E} \vee \mathscr{D}$ можно в этом дереве вывода отнести порядковое число $2^{\max(\alpha_1, \alpha_2)} +_0 1$, а формулам $\mathscr{C} \vee \mathscr{D} \vee \mathscr{D}$ и $\mathscr{C} \vee \mathscr{D}$ — порядковое число 2^α.

(d) $\mathscr{B}$ есть $\forall x\mathscr{E}$. Тогда рассматриваемое сеченние имеет вид

$$\frac{\mathscr{C} \vee \forall x\mathscr{E} \quad (\neg\forall x\mathscr{E}) \vee \mathscr{D}}{\mathscr{C} \vee \mathscr{D}}.$$

Согласно индуктивному предположению дерево вывода для $\mathscr{C} \vee \forall x\mathscr{E}$, являющееся поддеревом основного дерева вывода для $\mathscr{A}$, может быть заменено другим деревом вывода для $\mathscr{C} \vee \forall x\mathscr{E}$ степени, меньшей m, и порядка 2^{α_1}. В силу леммы A.5 и замечания в начале доказательства леммы A.2, для любого постоянного терма t существует вывод степени $< m$ и порядка 2^{α_1} для формулы $\mathscr{C} \vee \mathscr{E}(t)$.

Содержащийся в основном дереве вывода для $\mathscr{A}$ вывод формулы $(\neg\forall x\mathscr{E}) \vee \mathscr{D}$ может быть, согласно индуктивному предположению, заменен некоторым новым выводом степени, меньшей m, и порядка 2^{α_2}. История $\neg\forall x\mathscr{E}$ в этом новом выводе восходит либо к применению правила ослабления, либо к применениям правила квантификации

с $\neg\forall x\mathscr{E}$ в качестве главной формулы:

$$\neg\mathscr{E}(t_i) \vee \mathscr{G}_i,$$
$$(\neg\forall x\mathscr{E}) \vee \mathscr{G}_i,$$

где t_i — некоторые постоянные термы

Заменим каждое такое применение правила квантификации сечением

$$\mathscr{C} \vee \mathscr{E}(t_i) \qquad (\neg\mathscr{E}(t_i)) \vee \mathscr{G}_i$$
$$\mathscr{C} \vee \mathscr{G}_i$$

используя для левой посылки указанный выше вывод. Все остальные вхождения $\neg\forall x\mathscr{E}(x)$ в историю этой формулы также заменим на $\mathscr{C}$. В результате мы снова получим некоторое дерево вывода, заключительной формулой которого является $\mathscr{C} \vee \mathscr{D}$. Степень этого дерева меньше m, поскольку общее число пропозициональных связок и кванторов в $\neg\mathscr{E}(t_i)$ меньше, чем в $\neg\forall x\mathscr{E}(x)$. Нумерацию этого дерева построим следующим образом. Номера формул в выводах левых посылок $\mathscr{C} \vee \mathscr{E}(t_i)$ оставим без изменения, а прежние номера β всех остальных формул полученного дерева вывода заменим на $2^{\alpha_1} +_0 \beta$. Если β было номером посылки $\neg\mathscr{E}(t_i) \vee \mathscr{G}_i$ заменяемого применения правила квантификации, а γ — номер его заключения $(\neg\forall x\mathscr{E}) \vee \mathscr{G}_i$, то в нововведенном сечении посылки $\mathscr{C} \vee \mathscr{E}(t_i)$ и $\neg\mathscr{E}(t_i) \vee \mathscr{G}_i$ нумеруются соответственно порядковыми числами 2^{α_1} и $2^{\alpha_1} +_0 \beta$, а заключение $\mathscr{C} \vee \mathscr{G}_i$ — порядковым числом $2^{\alpha_1} +_0 \gamma > \max(2^{\alpha_1}, 2^{\alpha_1} +_0 \beta)$. Так как из $\delta <_0 \mu$ следует $2^{\alpha_1} +_0 \delta < 2^{\alpha_1} +_0 +_0 \mu$, то и всюду в этом новом дереве всякое заключение имеет номер, больший чем соответствующие ему посылки. Наконец, правая посылка $(\neg\forall x\mathscr{E}) \vee \mathscr{D}$, имевшая номер α_2, превращается теперь в заключительную формулу $\mathscr{C} \vee \mathscr{D}$ порядка $2^{\alpha_1} +_0 2^{\alpha_1} \leqslant 2^{\max(\alpha_1, \alpha_2)} +_0 2^{(\max \alpha_1, \alpha_2)} = = 2^{\max(\alpha_1, \alpha_2)} \times_0 2 = 2^{\max(\alpha_1, \alpha_2)+_0 1} \leqslant 2^{\alpha}$. Если при этом оказывается, что $2^{\alpha_1} +_0 2^{\alpha_2} <_0 2^{\alpha}$, то номер $\mathscr{C} \vee \mathscr{D}$ всегда можно увеличить до 2^{α}.

Следствие А.7. *Всякий вывод в* S_∞ *произвольной формулы* $\mathscr{A}$ *может быть заменен выводом той же формулы* $\mathscr{A}$, *не содержащим сечений, т. е. выводом степени* 0. *Если при этом* α — *порядок первоначального вывода, то порядок нового вывода можно выбрать равным некоторому порядковому числу вида* $2^{2^{\cdot^{\cdot^{2^{\alpha}}}}}$.

Предложение А.8. *Система* S_∞ *непротиворечива.*

Доказательство. Рассмотрим произвольную формулу $\mathscr{A}$ вида $0 \neq 0 \vee 0 \neq 0 \vee \ldots \vee 0 \neq 0$. Если бы такая формула $\mathscr{A}$ была выводима в S_∞, то она была бы выводима в S_∞ и без применения правила сечения. Просматривая остальные правила вывода, мы видим, что в таком случае $\mathscr{A}$ может быть следствием только формулы того же типа, что и она сама. Отсюда следует, что одна из формул вида $0 \neq 0 \vee \vee \ldots \vee 0 \neq 0$ должна была бы быть аксиомой, чего, однако, в действительности нет. Поэтому формула $\mathscr{A}$ невыводима в S_∞ и, следовательно, эта система непротиворечива.

Упражнение

Если ничем не ограничивать класс порядковых чисел, используемых для нумерации вершин деревьев вывода, то можно доказать также следующие два утверждения. 1) Система S_∞ ω-непротиворечива. (Указание. Следствие A.7, предложение A.8 и правило бесконечной индукции.) 2) Всякая замкнутая формула системы S_∞, истинная в стандартной модели, выводима в S_∞, и, следовательно, система S_∞ полна.

Чтобы несколько ослабить неконструктивность вышеизложенного доказательства непротиворечивости, можно следующим образом ограничить класс порядковых чисел, используемых в нумерации формул деревьев вывода. Рассмотрим множество порядковых чисел $\{\omega, \omega^\omega, \omega^{\omega^\omega}, \ldots\}$ (его можно задать индуктивно равенствами $\gamma_0 = \omega$ и $\gamma_{n+1} = \omega^{\gamma_n}$). Пусть ε_0 — наименьшая верхняя грань этого множества. Если мы будем применять в упомянутом смысле только порядковые числа, меньшие ε_0, то все приведенные выше доказательства останутся в силе (ибо из $\delta <_0 \varepsilon_0$ следует $2^\delta <_0 \varepsilon_0$). Кроме того, порядковые числа $<_0 \varepsilon_0$ допускают представление в некоторой стандартной «полиномиальной» форме: (i) порядковые числа, меньшие ω^ω, допускают представление в форме

$$(\omega^{k_1} \times_0 n_1) +_0 (\omega^{k_2} \times_0 n_2) +_0 \ldots +_0 (\omega^{k_l} \times_0 n_l),$$

где $k_1, k_2, \ldots, k_l$ — убывающая последовательность конечных порядковых чисел и $n_1, n_2, \ldots, n_l$ — конечные порядковые числа; (ii) порядковые числа, заключенные между ω^ω и ω^{ω^ω}, допускают представление в форме

$$(\omega^{\alpha_1} \times_0 n_1) +_0 (\omega^{\alpha_2} \times_0 n_2) +_0 \ldots +_0 (\omega^{\alpha_l} \times_0 n_l),$$

где $\alpha_1, \alpha_2, \ldots, \alpha_l$ — убывающая последовательность порядковых чисел, меньших ω^ω, и $n_1, n_2, \ldots, n_l$ — конечные порядковые числа, и т. д. (см. Бахман [1955], III; Генцен [1938b]).

Основным неконструктивным моментом рассмотренного здесь доказательства непротиворечивости является применение трансфинитной индукции в доказательстве леммы A.6. Принцип трансфинитной индукции до заданного порядкового числа был формализован и изучен Генценом [1943] и Шютте [1951], [1960]; как и следовало ожидать, принцип трансфинитной индукции до ε_0 невыводим в S. Что же касается вопроса о том, можно ли считать те или иные понятия и принципы (такие, как понятие счетного порядкового числа и принцип трансфинитной индукции до ε_0) действительно конструктивными, то здесь, как нам кажется, мы имеем дело, в конечном счете, с проблемой субъективной природы.

Дальнейшие детали и обсуждение затронутых здесь вопросов, в дополнение к уже цитированным работам, можно найти также у Гильберта и Бернайса [1939], Россера [1937], Мюллера [1961] и Шёнфильда [1959].

Литература *)

Здесь перечисляются не только книги и статьи, упоминаемые в тексте, но также и некоторые другие публикации, которые будут полезны при дальнейшем изучении математической логики. Дополнительные ссылки могут быть найдены в рефератах в Journal of Symbolic Logic и в Mathematical Reviews **).

Аккерман (Ackermann W.)

[1928] Zum Hilbertschen Aufbau der reelen Zahlen, Math. Ann. **99**, 118—133.

[1940] Zur Widerspruchsfreiheit der Zahlentheorie, Math. Ann. **117**, 162—194.

[1951] Konstruktiver Aufbau eines Abschnittes der zweiten Cantorschen Zahlenklasse, Math. Z. **53**, 403—413.

[1954] Solvable Cases of the Decision Problem, Amsterdam.

Ассер (Asser G.)

[1955] Das Repräsentantenproblem im Prädikatenkalkül der ersten Stufe mit Identität, Z. math. Logik Grundl. Math. **1**, 252—263.

[1959] Turing-Maschinen und Markowsche Algorithmen, Z. math. Logik Grundl. Math. **5**, 346—365.

Бахман (Bachman H.)

[1955] Transfinite Zahlen, Berlin.

Бернайс (Bernays P.)

[1937–1954] A system of axiomatic set theory. J. Symbolic Logic. I, **2** (1937), 65—77; II, **6** (1941), 1—17; III, **7** (1942), 65—89; IV, **7** (1942), 133—145; V, **8** (1943), 89—106; VI, **13** (1948), 65—79; VII, **19** (1954), 81—96.

[1957] Реферат статьи Майхилла [1955], J. Symbolic Logic **22**, 73—76.

[1958] Axiomatic Set Theory, Amsterdam.

[1961] Zur Frage der Unendlichkeitsschemata in der axiomatischen Mengenlehre, Essays on the Foundations of Mathematics, Jerusalem, 3—49.

Бет (Beth E.)

[1951] A topological proof of the theorem of Löwenheim — Skolem — Gödel, Indag. Math. **13**, 436—444.

[1953] Some consequences of the theorem of Löwenheim — Skolem — Gödel — Malcev, Indag. Math. **15**, 66—71.

---

*) В библиографию автора мы добавили ряд работ советских математиков (А. А. Маркова, А. А. Мучника и П. С. Новикова), получивших важные результаты, аналогичные цитируемым автором результатам зарубежных математиков. Как указывает сам автор, его библиография не претендует на полноту, и для получения более полной информации все равно нужно обращаться к реферативным журналам. Поэтому мы не нашли целесообразным продолжать библиографию автора на период после 1962 г. Исключение сделано лишь для выдающихся работ П. Коэна и П. Вопенки по проблеме независимости аксиомы выбора и континуум-гипотезы, а также для некоторых книг по математической логике и основаниям математики, изданных в последнее время на русском языке. Работы, добавленные к библиографии автора при переводе, отмечены кружочком °. (*Прим. ред.*).

**) Русский читатель может использовать с этой целью также реферативный журнал «Математика». (*Прим. перев.*)

[1959] The Foundations of Mathematics, Amsterdam.
[1962] Formal Methods, New York.
Биркгоф (Birkhoff G.)
[1948] Lattice Theory, New York. [Русский перевод: Биркгоф Г., Теория структур, ИЛ, 1952.]
де Брёйн (Bruijn N. G. de) и Эрдёш (Erdös P.)
[1951] A colour problem for infinite graphs and a problem in the theory of relations, Indag. Math. **13**, 369—373.
Бриттон (Britton J. L.)
[1958] The word problem for groups, Proc. London Math. Soc. **8**, 493—506.
Бун (Boon W.)
[1959] The word problem, Ann. Math. **70**, 207—265.
Бурбаки (Bourbaki N.)
[1947[Algèbre, Livre II, Chap. II, Paris. [Русский перевод: Бурбаки Н., Элементы математики. Алгебра (алгебраические структуры, линейная и полилинейная алгебра), Физматгиз, 1962.]
Вайсберг (Wajsberg M.)
[1933] Untersuchungen über den Funktionenkalkül für endliche Individuenbereiche, Math. Ann. **108**, 218—228.
Ван дер Варден (van der Waerden B.)
[1930—1931] Moderne Algebra, Berlin, Springer (второе издание, 1940; третье издание, 1950). [Русский перевод: Ван дер Варден Б. Л., Современная алгебра, Гостехиздат, 1947.]
Ван Хао (Wang Hao)
[1951 a] Arithmetic translations of axiom systems, Trans. Amer. Math. Soc. **71**, 283—291.
[1951 b] Arithmetic models for formal systems, Methodos **3**, 217—232.
[1954] The formalization of mathematics, J. Symbolic Logic **19**, 241—266.
[1955] Undecidable sentences generated by semantical paradoxes, J. Symbolic Logic **20**, 31—43.
[1957 a] The axiomatization of arithmetic, J. Symbolic Logic **22**, 145—158.
[1957 b] Remarks on constructive ordinals and set theory, Summer Inst. Symb. Logic, Cornell, 383—390.
[1957 c] A variant to Turing's theory of computing machines, J. Assoc. Comp. Mach. **4**, 63—92.
[1959] Ordinal numbers and predicative set theory, Z. math. Logic Grundl. Math. **5**, 216—239.
Ван Хао (Wang Hao) и Мак-Нотон (McNaughton R.)
[1953] Les systèmes axiomatiques de la théorie des ensembles, Paris. [Русский перевод: Ван Хао и Мак-Нотон Р., Аксиоматические системы теории множеств, ИЛ, 1963.]
Виноградов И. М.
[1952] Основы теории чисел, 6-е изд., Гостехиздат.
Воот (Vaught R.)
[1954] Applications of the Löwenheim — Skolem — Tarski theorem to problems of completeness and decidability, Indag. Math. **16**, 467—472.
[1959] Sentences true in all constructive models, J. Symbolic Logic **24**, 1—15.
[1961] Denumerable models of complete theories, Infinitistic Methods, Warszawa, 303—321.
[1962] Cobham's theorem on undecidable theories, Logic, Methodology and Philosophy of Science (Proc. Int. Cong., 1960), Stanford, 14—25. [Русский перевод; Воот Р. Л., О теореме Кобхама, касающейся неразрешимых теорий, сб. «Математическая логика и ее применения», «Мир», 1965, 9—22.]
Вопенка (Vopěnka P.)
°[1965 a] The limits of sheaves and applications on constructions of models, Bull. Acad. Polon. Sci., Ser. Math. **13**, 189—192.

°[1965 b] Properties of ∇-models, там же, 441—444.
°[1966] ∇-models in which the generalized continuum hypothesis does not hold, там же **14**, 95—99.
Галлер (Galler B. A.)
[1957] Cylindric and polyadic algebras, Proc. Amer. Math. Soc. **8**, 176—183.
Гёдель (Gödel K.)
[1930] Die Vollständigkeit der Axiome des logischen Funktionenkalküls, Monatsh. Math. Phys. **37**, 349—360.
[1931] Ueber formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I, там же **38**, 173—198.
[1933] Zum intuitionistischen Aussagenkalkül; Zur intuitionistischen Arithmetik und Zahlentheorie, Ergeb. math. Koll. **4**, 34—38, 40.
[1934] On undecidable propositions of formal mathematical systems, Princeton.
[1936] Über die Länge der Beweise, Ergeb. math. Koll. **7**, 23—24.
[1940] The consistency of the axiom of choice and of the generalized continuum hypothesis with the axioms of set theory, Princeton. [Русский перевод: Гёдель К., Совместимость аксиомы выбора и обобщенной континуум-гипотезы с аксиомами теории множеств, УМН **3**, № 1 (1948), 96—149.]
[1944] Russel's Mathematical Logic, в книге «The Philosophy of Bertrand Russell» под ред. Шильпа, Chicago, 123—153.
[1947] What is Cantor's continuum problem? Amer. Math. Monthly **54**, 515—525.
[1953] Über eine bisher noch nicht benutzte Erweiterung des finiten Standpunkts, Dialectica **12**, 280—287. [Русский перевод: Гёдель К., Об одном еще не использованном расширении финитной точки зрения, сб. «Математическая теория логического вывода», «Наука», 1967, 299—305.]
Гейтинг (Heyting A.)
[1956] Intuitionism, Amsterdam. [Русский перевод: Гейтинг А., Интуиционизм, «Мир», 1965.]
Генкин (Henkin L.)
[1949] The completeness of the first-order functional calculus, J. Symbolic Logic **14**, 159—166.
[1950] Completeness in the theory of types, там же **15**, 81—91.
[1953] Some interconnections between modern algebra and mathematical logic. Trans. Amer. Math. Soc. **74**, 410—427.
[1954] Boolean representation through propositional calculus, Fundam. Math, **41**, 89—96.
[1955 a] The representation theorem for cylindrical algebras, Mathematical interpretations of Formal Systems, Amsterdam, 85—97.
[1955 b] On a theorem of Vaught, J. Symbolic Logic **20**, 92—93.
[1956] La structure algébrique des théories mathématiques, Paris.
Генкин (Henkin L.) и Тарский (Tarski A.)
[1961] Cylindric Algebras, Proc. Symp. Pure Math. A. M. S., II, Lattice Theory, 83—113.
Генцен (Gentzen G.)
[1934] Untersuchungen über das logische Schliessen, Math. Z. **39**, 176—210, 405—431. [Русский перевод: Генцен Г., Исследования логических выводов, сб. «Математическая теория логического вывода», «Наука», 1967, 9—74.]
[1936] Die Widerspruchsfreiheit der reinen Zahlentheorie, Math. Ann. **112**, 493—565. [Русский перевод: Генцен Г., Непротиворечивость чистой теории чисел, сб. «Математическая теория логического вывода», «Наука», 1967, 77—153.]
[1938 a] Die gegenwärtige Lage in der mathematischen Grundlagenforschung, Forschungen zur Logik, N. Folge, Heft 4, 5—18.

[1938 b] Neue Fassung des Widerspruchsfreiheitsbeweises für die reine Zahlentheorie, там же, 19—44. [Русский перевод: Генцен Г., Новое изложение доказательства непротиворечивости для чистой теории чисел, сб. «Математическая теория логического вывода», «Наука», 1967, 154—190.]
[1943] Beweisbarkeit und Unbeweisbarkeit von Anfangsfällen der transfiniten Induktion in der reinen Zahlentheorie, Math. Ann. **119**, 140—161.

Гермес (Hermes H.)
[1961] Aufzählbarkeit, Entscheidbarkeit, Berechenbarkeit, Berlin — Göttingen — Heidelberg.

Гжегорчик (Grzegorczyk A.)
[1956] Some proofs of undecidability of arithmetic, Fundam. Math. **43**, 166—177.

Гжегорчик (Grzegorczyk A.), Мостовский (Mostowski A.) и Рыль-Нардзевский (Ryll-Nardzewski C.)
[1958] The classical and the ω-complete arithmetic, J. Symbolic Logic **23**, 188—206.

Гильберт (Hilbert D.) и Аккерман (Ackermann W.)
[1938] Grundzüge der theoretischen Logik, Berlin. [Русский перевод: Гильберт Д. и Аккерман В., Основы теоретической логики, ИЛ, 1947.]

Гильберт (Hilbert D.) и Бернайс (Bernays P.)
[1934], [1939]. Grundlagen der Mathematik, т. I (1934), т. II (1939), Berlin.

Девис (Davis M.)
[1958] Computability and Unsolvability, New York.

Девис (Davis M.), Путнам (Putnam H.) и Робинсон (Robinson J.)
[1961] The decision problem for exponential diophantine equations, Ann. Math. **74**, 425—436. [Русский перевод: Девис М., Путнам Х., Робинсон Дж., Проблема разрешимости для показательно-диофантовых уравнений, Математика (сб. переводов) **9**, № 5 (1965), 69—79.]

Дедекинд (Dedekind R.)
[1901] Essays on the theory of numbers, Chicago.

Деккер (Dekker J.)
[1953] Two notes on recursively enumerable sets, Proc. Amer. Math. Soc. **4**, 495—501.
[1955] Productive sets, Trans. Amer. Math. Soc. **78**, 129—149.

Деккер (Dekker J.) и Майхилл (Myhill J.)
[1960] Recursive Equivalence Types, Univ. Calif. Publ. Math. **3**, 67—213.

Детловс В. К.
[1958] Эквивалентность нормальных алгорифмов и рекурсивных функций, Тр. Матем. ин-та АН СССР им. В. А. Стеклова **LII**, Изд-во АН СССР, 66—69.

Диксон (Dickson L. E.)
[1929] Introduction to the theory of numbers, Chicago.

Дребен (Dreben B.)
[1952] On the completeness of quantification theory, Proc. Nat. Acad. Sci. U. S. A. **38**, 1047—1052.

Зейденберг (Seidenberg A.)
[1954] A new decision method for elementary algebra, Ann. Math. **60**, 365—374.

Зиман (Zeeman E. C.)
[1955] On direct sums of free cycles, J. London Math. Soc. **30**, 195—212.

Кальмар (Kalmár L.)
[1936] Zurückführung des Entscheidungsproblems auf den Fall von Formeln mit einer einzigen binären Funktionsvariablen, Comp. Math. **4**, 137—144

Камке (Kamke E.)
[1950] Theory of sets, New York.

Карнап (Carnap R.)
[1934] Logische Syntax der Sprache, Wien.
[1939] Foundations of logic and mathematics, «International Encyklopedia of Unified Science» I, № 3, Chicago.
[1942—1943] Studies in Semantics. Introduction to Semantics and Formalization of Logic, Cambridge, Mass.
[1950] Logical foundations of probability, Chicago.
[1958] Introduction to symbolic logic, New York.
Карри (Curry H. B.)
[1950] A theory of formal deducibility, Notre Dame.
[1951] Outlines of a Formalist Philosophy of Mathematics, Amsterdam.
[1952] Leçons de logique algébrique, Paris—Louvain.
°[1963] Foundations of Mathematical Logic, New York. [Русский перевод: Карри Х. Б., Основания математической логики, «Мир», 1969.]
Карри (Curry H. B.) и Фейс (Feys R.)
[1958] Combinatory logic, Amsterdam.
Кемени (Kemeny J.)
[1948] Models of logical systems, J. Symbolic Logic **13**, 16—30.
[1958] Undecidable problems of elementary number theory, Math. Ann. **135**, 160—169.
Клини (Kleene S. C.)
[1936 a] General recursive functions of natural numbers, Math. Ann. **112**, 727—742.
[1936 b] λ-definability and recursiveness, Duke Math. J. **2**, 340—353.
[1938] On notation for ordinal numbers, J. Symbolic Logic **3**, 150—155.
[1943] Recursive predicates and quantifiers, Trans. Amer. Math. Soc. **53**, 41—73.
[1944] On the forms of the predicates in the theory of constructive ordinals, Amer. J. Math. **66**, 41—58.
[1945] On the interpretation of intuitionistic number theory, J. Symbolic Logic **10**, 109—124.
[1952] Introduction to Metamathematics, Van Nostrand, Princeton. [Русский перевод: Клини С. К., Введение в метаматематику, ИЛ, 1957.]
[1955 a] Hierarchies of number-theoretic predicates, Bull. Amer. Math. Soc. **61**, 193—213.
[1955 b] Arithmetical predicates and function quantifiers, Trans. Amer. Math. Soc. **79**, 312—340.
[1955 c] On the form of the predicates in the theory of constructive ordinals II, Amer. J. Math. **77**, 405—428.
[1960] Mathematical logic: constructive and non-constructive operations, Proc. Int. Cong. Math., Edinburgh, 1958, 137—153.
Клини (Kleene S. C.) и Пост (Post E.)
[1954] The upper semi-lattice of degrees of recursive unsolvability, Ann. Math. **59**, 379—407.
Коэн (Cohen P. J.)
°[1963—1964] The independence of the continuum hypothesis, Proc. Nat. Acad. Sci. U. S. A. **50**, № 6, 1143—1148; **51**, № 1, 105—110. [Русский перевод: Коэн П. Дж., Независимость континуум-гипотезы, Математика (сб. переводов) **9**, № 4 (1965), 142—155.]
°[1966] Set theory and the continuum hypothesis. New York—Amsterdam. [Русский перевод: Коэн П. Дж., Теория множеств и континуум-гипотеза, «Мир», 1969.]
Крейг (Craig W.)
[1953] On axiomatizability within a system, J. Symbolic Logic **18**, 30—32.
[1957 a] Linear reasoning. A new form of the Herbrand—Gentzen theorem, J. Symbolic Logic **22**, 250—268.
[1957 b] Three uses of the Herbrand—Gentzen theorem in relating model theory and proof theory, J. Symbolic Logic **22**, 269—285.

Крейдер (Kreider D. L.) и Роджерс (Rogers H., Jr.)
[1961] Constructive versions of ordinal number classes, Trans. Amer. Math. Soc. **100**, 325—369.
Крейсел (Kreisel G.)
[1950] Note on arithmetic models for consistent formulae of the predicate calculus, Fundam. Math. **37**, 265—285.
[1951—1952] On the interpretation of non-finitist proofs, J. Symbolic Logic **16**, 241—267; **17**, 43—58.
[1952 a] On the concepts of the completeness and interpretation of formal systems, Fundam. Math. **39**, 103—127.
[1952 b] Some concepts concerning formal systems of number theory, Math. Z. **57**, 1—12.
[1953 a] A variant to Hilbert's theory of the foundations of arithmetic, British J. Phil. of Science **4**, 107—129.
[1953 b] On a problem of Henkin's, Indag. Math. **15**, 405—406.
[1955] Models, translations and interpretations, Mathematical Interpretations of Formal Systems, Amsterdam, 26—50.
[1958 a] Mathematical significance of consistency proofs, J. Symbolic Logic **23**, 155—182.
[1958 b] Hilbert's programme, Dialectica **12**, 346—372.
[1960] Ordinal logics and characterization of informal concepts of proof, Proc. Int. Cong. Math., Edinburgh, Cambridge, 289—299.
Крейсел (Kreisel G.) и Ван Хао (Wang Hao)
[1955] Some applications of formalized consistency proofs, Fundam. Math. **42**, 101—110.
Куайн (Quine W. V.)
[1937] New foundations for mathematical logic, Amer. Math. Monthly **44**, 70—80.
[1938] On the theory of types, J. Symbolic Logic **3**, 125—139.
[1950] Methods of logic, New York.
[1951] Mathematical logic, Cambridge, Mass.
[1953] From the logical point of view, Cambridge, Mass.
[1955] On Frege's way out, Mind **64**, 145—159.
Ладриер (Ladrière J.)
[1957] Les limitations internes des formalismes, Paris.
Ландау (Landau E.)
[1930] Grundlagen der Analysis, Leipzig. [Русский перевод: Ландау Э. Основы анализа, ИЛ, 1947.]
Лёб (Löb M. H.)
[1955] Solution of a problem of Leon Henkin, J. Symbolic Logic **20**, 115—118.
Лёвенгейм (Löwenheim L.)
[1915] Über Möglichkeiten im Relativkalkül, Math. Ann. **76**, 447—470.
Леви (Levy A.)
[1960] Axiom schemata of strong infinity, Pacific J. Math. **10**, 223—238.
Ленгфорд (Langford C. H.)
[1927] Some theorems of deducibility, Ann. Math. I, **28**, 16—40; II, **28**, 459—471.
Линдон (Lyndon R. C.)
[1959] Properties preserved under algebraic construction, Bull. Amer. Math. Soc. **65**, 143—299.
Лойхли (Läuchli H.)
[1962] Auswahlaxiom in der Algebra, Comment. Math. Helvetici **37**, 1—18.
Лоренцен (Lorenzen P.)
[1951] Algebraische und logistische Untersuchungen über freie Verbände, J. Symbolic Logic **16**, 81—106.
[1955] Einführung in die operative Logik und Mathematik, Berlin—Göttingen—Heidelberg.

Лось (Loś J.)
[1954 a] Sur la théorème de Gödel pour les théories indénombrables, Bull. de l'Acad. Polon. des Sci. III, **2**, 319—320.
[1954 b] On the existence of linear order in a group, там же, 21—23.
[1954 c] On the cathegoricity in power of elementary deductive systems and some related problems, Coll. Math. **3**, 58—62.
[1955] The algebraic treatement of the methodology of elementary deductive systems, Studia Logica **2**, 151—212.
Лось (Loś J.) и Рылль-Нардзевский (Ryll-Nardzewski C.)
[1954] Effectiveness of the representation theory for Boolean algebras, Fundam. Math. **41**, 49—56.
Люксембург (Luxemburg W. A. J.)
[1962] Non-standard analysis, Pasadena.
Майхилл (Myhill J.)
[1955] Creative sets, Z. math. Logik Grundl. Math. **1**, 97—108.
Макдоуэлл (Macdowell R.) и Шпеккер (Specker E.)
[1961] Modele der Arithmetik, Infinitistic Methods, Warszawa, 257—263.
Мак-Кинси (McKinsey J. C. C.) и Тарский (Tarski A.)
[1948] Some theorems about the sentential calculi of Lewis and Heyting, J. Symbolic Logic **13**, 1—15.
Маклафлин (Maclaughlin T.)
[1961] A muted variation on a theme of Mendelson, Z. math. Logic Grundl. Math. **17**, 57—60.
Мальцев А. И.
[1936] Untersuchungen aus dem Gebiet der mathematischen Logik, Матем. сб. **5**, № 1, 323—336.
°[1965] Алгоритмы и рекурсивные функции, «Наука».
Марквальд (Markwald S.)
[1954] Zur Theorie der konstruktiven Wohlordnungen, Math. Ann. **127**, 135—149.
Марков А. А.
°[1947 a] Невозможность некоторых алгорифмов в теории ассоциативных систем, ДАН СССР **55**, 587—590.
°[1947 b] Невозможность некоторых алгорифмов в теории ассоциативных систем, ДАН СССР **58**, 353—356.
[1954] Теория алгорифмов, Тр. Матем. ин-та АН СССР им. В. А. Стеклова **XLII**, Изд-во АН СССР.
Матиясевич Ю. В.
°[1970] Диофантовость перечислимых множеств, ДАН СССР **191**, 279—282.
Мендельсон (Mendelson E.)
[1956 a] Some proofs of independence in axiomatic set theory, J. Symbolic Logic **21**, 291—303.
[1956 b] The independence of weak axiom of choice, там же, 350—366.
[1958] The axiom of Fundierung and the axiom of choice, Arch. Math. Logik Grundlagenforsch. **4**, 65—70.
[1961] On non-standard models for number theory, Essays on the Foundations of Mathematics, Jerusalem, 259—268.
Мередит (Meredith C. A.)
[1953] Single axioms for the systems (C, N), (C, O) and (A, N) of the two-valued propositional calculus, J. Compt. Syst. **3**, 155—164.
Монтегю (Montague R.) и Воот (Vaught R. L.)
[1959] Natural models of set theories, Fundam. Math. **47**, 219—242.
Мостовский (Mostowski A).
[1939] Über die Unabhängigkeit des Wohlordnungssatzes vom Ordnungsprinzip, Fundam. Math. **32**, 201—252.
[1947 a] On definable sets of positive integers, Fundam. Math. **34**, 81—112.
[1947 b] On absolute properties of relations, J. Symbolic Logic **12**, 33—42.
[1949] An undecidable arithmetic statement, Fundam. Math. **36**, 143—164.

[1951 a] Some impredicative definitions in the axiomatic set theory, Fundam. Math. **37**, 111—124 (также **38** (1952), стр. 238).
[1951 b] A classification of logical systems, Studia Philosophica **4**, 237—274.
[1952 a] Sentences undecidable in formalized arithmetic, Amsterdam.
[1952 b] On models of axiomatic systems, Fundam. Math. **39**, 133—158.
[1952 c] On direct powers of theories, J. Symbolic Logic **17**, 1—31.
[1955] The present state of investigations on the foundations of mathematics, Rozprawy Math. **9**. [Русский перевод: Мостовский А., Современное состояние исследований по основаниям математики, УМН **9**, № 3 (61) (1954).]
[1956] Concerning a problem of Scholz, Z. math. Logik Grundl. Math. **2**, 210—214.
[1957] On generalization of quantifiers, Fundam. Math. **44**, 12—36.
[1958] Quelques observations sur l'usage des méthodes nonfinitistes dans la métamathématique, Colloq. Int. Cent. Nat. Rech. Sci., Paris.
[1961] A generalization of the incompleteness theorem, Fundam. Math. **49**, 205—232.

Мучник А. А.
°[1956] Неразрешимость проблемы сводимости теории алгоритмов, ДАН СССР **108**, 194—197.
°[1958] Решение проблемы сводимости Поста и некоторых других проблем теории алгоритмов, Тр. Моск. матем. о-ва **7**, 391—405.

Мюллер (Müller G.)
[1961] Über die unendliche Induktion, Infinitistic Methods, Warszawa, 75—95.

Нагорный Н. М.
[1953] К усилению теоремы приведения теории алгорифмов, ДАН СССР **90**, 341—342.

фон Нейман (von Neumann J.)
[1925] Eine Axiomatizierung der Mengenlehre, J. für Math. **154**, 219—240. (Исправления, там же **155** (1926), стр. 128.)
[1928] Die Axiomatizierung der Mengenlehre, Math. Z. **27**, 669—752.

Никод (Nicod J. G.)
[1917] A reduction in the number of primitive propositions of logic, Proc. Cambridge Phil. Soc. **19**, 32—41.

Новак (Novak I. L. (Gál L. N.))
[1951] A construction for models of consistent systems, Fundam. Math. **37**, 87—110.

Новиков П. С.
°[1943] On the consistency of certain logical calculus, Матем. сб. **12** (**54**), 231—261.
[1955] Об алгоритмической неразрешимости проблемы тождества слов в теории групп, Тр. Матем. ин-та АН СССР им. В. А. Стеклова **XLIV**, Изд-во АН СССР.
°[1959] Элементы математической логики, Физматгиз.

Ори (Orey S.)
[1956] On ω-consistency and related properties, J. Symbolic Logic **21**, 246—252.
[1961] Relative interpretations, Z. math. Logik Grundl. Math. **7**, 146—153.

Пеано (Peano G.)
[1891] Sul concetto di numero, Rivista di Mat. **1**, 87—102.

Петер (Péter R.)
[1935] Konstruktion nichtrekursiver Funktionen, Math. Ann. **111**, 42—60.
[1951] Rekursive Funktionen, Budapest; второе расширенное издание, Budapest, 1957. [Русский перевод: Петер Р., Рекурсивные функции, ИЛ, 1954.]

Пост (Post E.)
[1921] Introduction to a general theory of elementary propositions, Amer. J. Math. **43**, 163—185.

[1936] Finite combinatory processes — formulation 1, J. Symbolic Logic **1**, 103—105.
[1943] Formal reductions of the general combinatorial decision problem, Amer. J. Math. **65**, 197—215.
[1944] Recursively enumerable sets of positive integers and their decision problems, Bull. Amer. Math. Soc. **50**, 284—316.
[1947] Recursive unsolvability of a problem of Thue, J. Symbolic Logic **12**, 1—11.

Пресбургер (Presburger M.)
[1929] Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen in welchem die Addition als einzige Operation hervortritt, Comptes Rendus, I Congrès des Math. des Pays Slaves, Warszawa, 192—201, 395.

Путнам (Putnam H.)
[1957] Decidability and essential undecidability, J. Symbolic Logic **22**, 39—54.

Рабин (Rabin M.)
[1958] On recursively enumerable and arithmetic models of set theory, J. Symbolic Logic **23**, 408—416.
[1959] Arithmetical extensions with prescribed cardinality, Indag. Math. **21**, 439—446.
[1960] Computable algebra, general theory and theory of computable fields, Trans. Amer. Math. Soc. **95**, 341—360.
[1961] Non-standard models and independence of the induction axiom, Essays in the Foundations of Mathematics, Jerusalem, 287—299.
[1962] Diophantine equations and non-standard models of arithmetic, Logic, Methodology and Philosophy of Science (Proc. Int. Congr., 1960), Stanford, 151—158. [Русский перевод: Рабин М., Диофантовы уравнения и нестандартные модели арифметики, сб. «Математическая логика и ее применения», «Мир», 1965, 176—184.]

Райс (Rice H. G.)
[1953] Classes of recursively enumerable sets and their decision problems, Trans. Amer. Math. Soc. **74**, 358—366.

Расёва (Rasiowa H.)
[1951] Algebraic treatment of the functional calculi of Heyting and Lewis, Fundam. Math. **38**, 99—126.
[1955] Algebraic models of axiomatic theories, там же **41**, 291—310.
[1956] On the ε-theorems, там же **43**, 156—165.

Расёва (Rasiowa H.) и Сикорский (Sikorski R.)
[1951] A proof of the completeness theorem of Gödel, Fundam. Math. **37**, 193—200.
[1952] A proof of the Skolem — Löwenheim theorem, там же **38**, 230—232.
[1953] Algebraic treatment of the notion of satisfiability, там же **40**, 62—95

Рассел (Russell B.)
[1908] Mathematical logic as based on the theory of types, Amer. J. Math. **30**, 222—262.

Рассел (Russell B.) и Уайтхед (Whitehead A. N.)
[1910—1913] Principia Mathematica, тт. I—III, Cambridge Univ. Press.

Робинсон А. (Robinson A.)
[1951] On the metamathematics of algebra, Amsterdam.
[1952] On the application of symbolic logic to algebra, Int. Cong. Math., Cambridge, Mass. I, 686—694.
[1955] On ordered fields and definite functions, Math. Ann. **130**, 257—271.
[1956] Complete theories, Amsterdam.
[1961] Model theory and non-standard arithmetic, Infinitistic Methods, Warszawa, 266—302.
[1963] Introduction to model theory and to the metamathematics of algebra, Amsterdam. [Русский перевод: Робинсон А., Введение в теорию моделей и метаматематику алгебры, «Наука», 1967.]

Робинсон Дж. (Robinson J.)
[1949] Definability and decision problem in arithmetic, J. Symbolic Logic **14**, 98—114.
[1950] General recursive functions, Proc. Amer. Math. Soc. **1**, 703—718.
[1952] Existential definability in arithmetic, Trans. Amer. Math. Soc. **72**, 437—449. [Русский перевод: Робинсон Дж., Экзистенциальная выразимость в арифметике, Математика (сб. переводов) **8**, № 5 (1964), 3—14.]
Робинсон Р. (Robinson R. M.)
[1937] The theory of classes. A modification of von Neumann's system, J. Symbolic Logic **2**, 69—72.
[1947] Primitive recursive functions, Bull. Amer. Math. Soc. **53**, 925—942.
[1948] Recursion and double recursion, там же **54**, 987—993.
[1950] An essentially undecidable axiom system, Proc. Int. Cong. Math., Cambridge, 1950, **1**, 729—730.
[1956] Arithmetical representation of recursively enumerable sets, J. Symbolic Logic **21**, 162—186. [Русский перевод: Робинсон Р. М., Арифметическое представление рекурсивно-перечислимых множеств, Математика (сб. переводов) **8**, № 5 (1964), 23—47.]
Роджерс (Rogers H., Jr.)
[1956] Theory of recursive functions and effective computability, тт. I—II, MIT, Cambridge, Mass.
[1958] Gödel numberings of partial recursive functions, J. Symbolic Logic **23**, 331—341.
[1959] Computing degrees of unsolvability, Math. Ann. **138**, 125—140.
Розенблюм (Rosenbloom P.)
[1950] Elements of mathematical logic, New York.
Россер (Rosser J. B.)
[1936a] Constructibility as a criterion for existence, J. Symbolic Logic **1**, 36—39.
[1936b] Extensions of some theorems of Gödel and Church, там же, 87—91.
[1937] Gödel theorems for non-constructive logics, J. Symbolic Logic **2**, 129—137.
[1939a] On the consistency of Quine's «New foundations for mathematical logic», J. Symbolic Logic **4**, 15—24.
[1939b] An informal exposition of proofs of Gödel's theorem and Church's theorem, там же, 53—60.
[1953] Logic for Mathematicians, New York.
[1954] The relative strength of Zermelo's set theory and Quine's New Foundations, Proc. Int. Cong. Math., Amsterdam, III, 289—294.
[1955] Deux esquisses de logique, Paris.
Россер (Rosser J. B.) и Ван Хао (Wang Hao)
[1950] Non-standard models for formal logics, J. Symbolic Logic **15**, 113—129.
Россер (Rosser J. B.) и Тюркетт (Turquette A.)
[1952] Many-valued logics, Amsterdam.
Рылль-Нардзевский (Ryll-Nardzewski C.)
[1953] The role of the axiom of induction in elementary arithmetic, Fundam. Math. **39**, 239—263.
Саппс (Suppes P.)
[1957] Introduction to logic, Van Nostrand, Princeton.
[1960] Axiomatic set theory, Van Nostrand, Princeton.
Серпинский (Sierpiński W.)
[1947] L'hypothèse généralisée du continu et l'axiome du choix, Fundam. Math. **34**, 1—5.
[1958] Cardinal and ordinal numbers, Warszawa.
Сикорский (Sikorski R.)
[1960] Boolean algebras, Berlin — Göttingen — Heidelberg, второе издание,

1964. [Русский перевод: Сикорский Р., Булевы алгебры, «Мир», 1969.]

Сколем (Skolem T.)

[1919] Logisch-kombinatorische Untersuchungen über die Erfüllbarkeit oder Beweisbarkeit mathematischer Sätze nebst einem Theoreme über dichte Mengen, Skrifter Vidensk, Kristiania, 1, 1—36.

[1934] Über die Nicht-Charakterisierbarkeit der Zahlenreihe mittels endlich oder abzählbar unendlich vieler Aussagen mit ausschliesslich Zahlenvariablen, Fundam. Math. **23**, 150—161.

[1955] Peano's axioms and models of arithmetic, Mathematical Interpretations of Formal Systems, Amsterdam, 1—14.

Скотт (Scott D.)

[1961] On constructing models for arithmetic, Infinitistic Methods, Warszawa, 235—255.

Спектор (Spector C.)

[1955] Recursive well-orderings, J. Symbolic Logic **20**, 151—163.

[1956] On degrees of recursive unsolvability, Ann. Math. **64**, 581—592.

Стоун (Stone M.)

[1936] The representation theorem for Boolean algebras, Trans. Amer. Math. Soc. **40**, 37—111.

Тарский (Tarski A.)

[1925] Sur les ensembles finis, Fundam. Math. **6**, 45—95.

[1933] Einige Betrachtungen über die Begriffe der ω-Widerspruchsfreiheit und der ω-Vollständigkeit, Monatsh. Math. Phys. **40**, 97—112.

[1936] Der Wahrheitsbegriff in den formalisierten Sprachen, Studia Philos. **1**, 261—405. [Также в [1956].]

[1938] Über unerreichbare Kardinalzahlen, Fundam. Math. **30**, 68—89.

[1944] The semantic conception of truth and the foundations of semantics, Philos. and Phenom. Res. **4**, 341—376.

[1951] A decision method for elementary algebra and geometry, Berkeley.

[1952] Some notions and methods on the borderline of algebra and metamathematics, Int. Cong. Math., Cambridge, Mass., 705—720.

[1954—1955] Contributions to the theory of models, Indag. Math. **16**, 572—588; **17**, 56—64.

[1956] Logic, Semantics, Metamathematics, Oxford.

Тарский (Tarski A.) и Воот (Vaught R.)

[1957] Arithmetical extensions of relational systems, Comp. Math. **18**, 81—102.

Тарский (Tarski A.), Мостовский (Mostowski A.) и Робинсон Р. (Robinson R.)

[1953] Undecidable theories, Amsterdam.

Тьюринг (Turing A.)

[1936—1937] On computable numbers, with an application to the Entscheidungsproblem, Proc. London Math. Soc. **42**, 230—265; **43**, 544—546.

[1937] Computability and λ-definability, J. Symbolic Logic **2**, 153—163.

[1939] Systems of logic based on ordinals, Proc. London Math. Soc. **45**, 161—228.

[1950a] The word problem in semigroups with cancellation, Ann. Math. **52**, 491—505.

[1950b] Computing Machinery and Intelligence, Mind **59**, 433—460.

Улам (Ulam S.)

[1930] Zur Masstheorie in der allgemeinen Mengenlehre, Fundam. Math. **16**, 140—150.

Успенский В. А.

[1960] Лекции о вычислимых функциях, Физматгиз.

Феферман (Feferman S.)

[1957] Degrees of unsolvability associated with classes of formalized theories, J. Symbolic Logic **22**, 161—175.

[1960a] Arithmetization of metamathematics in a general setting, Fundam. Math. **49**, 35—92.
[1960b] Transfinite recursive progressions of axiomatic theories, Tech. Report No. 2, Appl. Math. & Stat. Lab., Stanford.

Феферман (Feferman S.) и Воот (Vaught R. L.)
[1959] The first order properties of products of algebraic systems, Fundam. Math. **47**, 57—103.

Феферман (Feferman S.), Крейсел (Kreisel G.) и Ори (Orey S.)
[1961] 1-consistency and faithful interpretations, Arch. Math. Logik u. Grundlagenf. **6**, 52—63.

Фреге (Frege G.)
[1884] Grundlagen der Arithmetik, Breslau.
[1893, 1903] Grundgesetze der Arithmetik, I, II, Jena.

Френкель (Fraenkel A. A.)
[1953] Abstract set theory, Amsterdam (второе издание, 1961).

Френкель (Fraenkel A. A.) и Бар-Хиллел (Bar-Hillel Y.)
[1958] Foundations of set theory, Amsterdam. [Русский перевод: Френкель А. и Бар-Хиллел И., Основания теории множеств, «Мир», 1966.]

Фридберг (Friedberg R.)
[1957] Two recursively enumerable sets of incomparable degrees of unsolvability, Proc. Nat. Acad. Sci. U. S. A. **43**, 236—238.

Фридберг (Friedberg R.) и Роджерс (Rogers H., Jr.)
[1959] Reducibility and completeness for set of integers, Z. math. Logik Grundl. Math. **5**, 117—125.

Хазенъегер (Hasenjäger G.)
[1952] Über ω-Unvollständigkeit in der Peano-Arithmetik, J. Symbolic Logic **17**, 81—97.
[1953] Eine Bemerkung zu Henkins Beweis für Vollständigkeit des Prädikatenkalküls der ersten Stufe, J. Symbolic Logic **18**, 42—48.
[1960] Unabhängigkeitsbeweise in Mengenlehre und Stufenlogik der Modelle, Jahresber. Deutsch. Math. Ver. **63**, 141—162.

Хазенъегер (Hasenjäger G.) и Шольц (Scholz H.)
[1961] Grundzüge der mathematischen Logik, Berlin — Göttingen — Heidelberg.

Халмош (Halmos P.)
[1960] Naive set theory, Van Nostrand, Princeton.
[1962] Algebraic logic, New York.

Халмош (Halmos P.) и Воон (Vaughn H.)
[1950] The marriage problem, Amer. J. Math. **72**, 214—215.

Хартогс (Hartogs F.)
[1915] Über das Problem der Wohlordnung, Math. Ann. **76**, 438—443.

Хеллман (Hellman M.)
[1961] A short proof of an equivalent form of the Schröder—Bernstein theorem, Amer. Math. Monthly **68**, 770.

Хигмен (Higman G.)
[1961] Subgroups of finitely presented groups, Proc. Roy. Soc., A **262**, 455—475.

Хинтикка (Hintikka K. J.)
[1954] An application of logic to algebra, Math. Scand. **2**, 243—246.
[1955a] Form and content in quantification theory, Acta Phil. Fennica **8**, 11—55.
[1955b] Notes on the quantification theory, Comment. Phys.-Math., Soc. Sci. Fennica **17**, 1—13.
[1956] Identity, variables and impredicative definitions, J. Symbolic Logic **21**, 225—245.
[1957] Vicious circle principle and the paradoxes, J. Symbolic Logic **22**, 245—249.

Хлодовский И. Н.
[1959] Новое доказательство непротиворечивости арифметики, УМН **14**, № 6, 105—140.
Холл (Hall M., Jr.)
[1949] The word problem for semigroups with two generators, J. Symbolic Logic **14**, 115—118.
Хон (Hohn F.)
[1960] Applied Boolean algebra, New York.
Цермело (Zermelo E.)
[1908] Untersuchungen über die Grundlagen der Mengenlehre, I, Math. Ann. **65**, 261—281.
Чёрч (Church A.)
[1936a] A note on the Entscheidungsproblem, J. Symbolic Logic **1**, 40—41; исправления, там же, 101—102.
[1936b] An unsolvable problem of elementary number theory, Amer. J. Math. **58**, 345—363.
[1940] A formulation of the simple theory of types, J. Symbolic Logic **5**, 56—68.
[1941] The calculi of lambda-conversion, Princeton.
[1956] Introduction to mathematical logic, I, Princeton. Русский перевод: Чёрч А., Введение в математическую логику, том I, ИЛ, 1961.]
Чёрч (Church A.) и Клини (Kleene S. C.)
[1936] Formal definitions in the theory of ordinal numbers, Fundam. Math. **28**, 11—21.
Чёрч (Church A.) и Куайн (Quine W. V.)
[1951] Some theorems on definability and decidability, J. Symbolic Logic **17**, 179—187.
Чудновский Г. В.
°[1970] Диофантовы предикаты, УМН **25**, № 4, 185—186.
Шапиро (Shapiro N.)
[1956] Degrees of computability, Trans. Amer. Math. Soc. **82**, 281—299.
Шеннон (Shannon C.)
[1938] A symbolic analysis of relay and switching circuits, Trans. Amer. Inst. Elect. Eng. **57**, 713—723.
Шёнфильд (Shoenfield J.)
[1954] A relative consistency proof, J. Symbolic Logic **19**, 21—28.
[1958] Degrees of formal systems, J. Symbolic Logic **23**, 389—392.
[1959] On a restricted ω-rule, Bull. Acad. Pol. Sci., Ser. Sci. Math. Astr. Phys. **7**, 405—407.
Шепердсон (Shepherdson J.)
[1951—1953] Inner models for set theory, J. Symbolic Logic, I, **16**, 161—190; II, **17**, 225—237; III, **18**, 145—167.
[1961] Representability of recursively enumerable sets in formal theories, Arch. math. Logic Grundlagenf. **5**, 119—127.
Шестаков В. И.
°[1941] Алгебра двухполюсных схем, построенных исключительно из двухполюсников, Журнал физической техники **11**, вып. 6, 532—549.
Шмелева (Szmielew W.)
[1955] Elementary properties of abelian groups, Fundam. Math. **41**, 203—271.
Шмидт (Schmidt A.)
[1960] Mathematische Gesetze der Logik, I, Vorlesungen über Aussagenlogik, Berlin—Göttingen—Heidelberg.
Шмульян (Smullyan R.)
[1961] Theory of formal systems, Princeton.
Шпеккер (Specker E.)
[1949] Nicht-konstruktiv beweisbare Sätze der Analysis, J. Symbolic Logic **14**, 145—148.

[1953] The axiom of choice in Quine's «New Foundations for Mathematical Logic», Proc. Acad. Sci. U. S. A. **39**, 972—975.
[1954] Verallgemeinerte Kontinuumshypothese und Auswahlaxiom, Archiv der Math. **5**, 332—337.
[1957] Zur Axiomatik der Mengenlehre (Fundierungs- und Auswahlaxiom), Z. math. Logik Grundl. Math. **3**, 173—210.
[1962] Typical ambiguity, Logic, Methodology and Philosophy of Science (Proc. Int. Cong., 1960), Stanford, 116—124. [Русский перевод: Шпеккер Э., Типовая неопределенность, сб. «Математическая логика и ее применения», «Мир», 1965.]

Шураньи (Suranyi J.)
[1959] Reduktionstheorie des Entscheidungsproblems im Prädikatenkalkül der ersten Stufe, Budapest.

Шютте (Schütte K.)
[1951] Beweistheoretische Erfassung der unendlichen Induktion in der Zahlentheorie, Math. Ann. **122**, 369—389.
[1960] Beweistheorie, Berlin — Göttingen — Heidelberg.

Эрбран (Herbrand J.)
[1930] Recherches sur la théorie de la démonstration, Travaux de la Soc. des Sci. et des Lettres de Varsovie, III, **33**, 33—160.
[1931] Sur le problème fondamental de la logique mathématique, Comptes Rend. Warszawa, **24**, 12—56.
[1932] Sur la non-contradiction de l'arithmetique, J. f. Math. **166**, 1—8.

Эрдёш (Erdös P.) и Тарский (Tarski A.)
[1961] On some problems involving inaccessible cardinals, Essays on the Foundations of Mathematics, Jerusalem, 50—82.

Эренфойхт (Ehrenfeucht A.)
[1957a] On theories categorical in power, Fundam. Math. **44**, 241—248.
[1957b] Two theories with axiome built by means of pleonasms, J. Symbolic Logic **22**, 36—38.
[1958] Theories having at least continuum many non-isomorphic models in each infite power (abstract), Notices Amer. Math. Soc. **5**, 680.

Эренфойхт (Ehrenfeucht A.) и Мостовский (Mostowski A.)
[1957] Models of axiomatic theories admitting automorphisms, Fundam. Math. **43**, 50—68.

Эренфойхт (Ehrenfeucht A.) и Феферман (Feferman S.)
[1960] Representability of recursively enumerable sets in formal theories, Arch. math. Logik Grundlagenf. **5**, 37—41.

Яблонский С. В.
°[1958] Функциональные построения в k-значной логике, Тр. Матем. ин-та АН СССР им. В. А. Стеклова, **LI**, 5—143,

Яськовский (Jaśkowski S.)
[1936] Recherches sur le système de la logique intuitioniste, Act. Sci. Ind. **393**, Paris, 58—61.

Алфавитный указатель

Символы и обозначения