ЛЕКЦИИ ПО МАТЕМАТИЧЕСКОЙ ЛОГИКЕ
И ТЕОРИИ АЛГОРИТМОВ

Н. К. Верещагин, А. Шень

ЯЗЫКИ И ИСЧИСЛЕНИЯ

Москва, 2000
МЦНМО

ББК 22.12

В31 **Н. К. Верещагин, А. Шень.** Лекции по математической логике и теории алгоритмов. Языки и исчисления. М.: МЦНМО, 2000, **???** с.

Книга написана по материалам лекций и семинаров, проводившихся авторами для студентов младших курсов мехмата МГУ. В ней рассказывается об основных понятиях математической логики (логика высказываний, языки первого порядка, выразимость, исчисление высказываний, разрешимые теории, теорема о полноте, начала теории моделей).

Тексты, составляющие книгу, являются свободно распространяемыми и доступны по адресу

`ftp://ftp.mccme.ru/users/shen/logic/firstord`

ISBN 5-900916-39-1

Книга издана при финансовой поддержке
Российского фонда фундаментальных исследований
(проект 00-01-14085)

rffi.ps

Издательство Московского Центра
непрерывного математического образования

Технический редактор В. В. Шувалов

Лицензия ЛР №071150 от 11.04.95 г.
Подписано в печать ??.??.??. Формат 84 × 108/32.
Печать офсетная. Печ. л. 5,5
Тираж ????. Заказ №?.
МЦНМО
121002, Москва, Большой Власьевский пер., 11

Оглавление

Предисловие

Нашему учителю,
ВЛАДИМИРУ АНДРЕЕВИЧУ УСПЕНСКОМУ,
к 70-летию

Предлагаемая вашему вниманию книга написана по материалам лекций для младшекурсников, которые читались авторами в разные годы на механико-математическом факультете МГУ. (В этой серии уже вышли книги «Начала теории множеств» и «Вычислимые функции».)

Центральная идея математической логики восходит ещё к Лейбницу и состоит в том, чтобы записывать математические утверждения в виде последовательностей символов и оперировать с ними по формальным правилам. При этом правильность рассуждений можно проверять механически, не вникая в их смысл.

Усилиями большого числа математиков и логиков второй половины XIX и первой половины XX века (Буль, Кантор, Фреге, Пеано, Рассел, Уайтхед, Цермело, Френкель, Гильберт, фон Нейман, Гёдель и другие) эта программа была в основном выполнена. Принято считать, что всякое точно сформулированное математическое утверждение можно записать формулой теории множеств (одной из наиболее общих формальных теорий), а всякое строгое математическое доказательство преобразовать в формальный вывод в этой теории (последовательность формул теории множеств, подчиняющуюся некоторым простым правилам). В каком-то смысле это даже стало определением: математически строгим считается такое рассуждение, которое можно перевести на язык теории множеств.

Так что же, теперь математики могут дружно уйти на пенсию, поскольку можно открывать математические теоремы с помощью компьютеров, запрограммированных в соответствии с формальными правилами теории множеств? Конечно, нет, причём сразу по нескольким причинам.

Начнём с того, что машина, выдающая с большой скоростью математические теоремы (и их доказательства), хотя и возможна, но бесполезна. Дело в том, что среди этих верных утверждений почти все будут неинтересными. Формальная логика говорит, какие правила надо соблюдать, чтобы получать верные результаты, но не говорит, в каком порядке их надо применять, чтобы получить что-то интересное.

Казалось бы, мы можем запустить машину и ждать, пока она не докажет интересующее нас утверждение (пропуская все остальные). Проблема в том, что формальное доказательство сколько-нибудь содержательной теоремы настолько длинно, что прочесть его человек не в состоянии. Представьте себе доказательство, которое состоит из миллионов формально правильных шагов, в котором мы можем проверить каждый отдельный шаг, но так и не понимаем, что происходит — много ли в нём проку?

На самом деле прок всё-таки есть: мы узнаём, что доказываемое утверждение верно, хотя так и не понимаем, почему. Так что и такая машина была бы полезна. Увы, и этого сделать не удаётся, поскольку на поиск доказательства сколько-нибудь сложного утверждения известными сейчас методами требуется астрономически большое время (даже если представить себе, что машина работает с предельно возможной по законам физики скоростью).

Можно умерить амбиции и поставить более простую задачу: пусть машина проверяет доказательства, записанные человеком по правилам формальной логики. Если машина не может помочь нам что-то открыть, пусть она хотя бы проверит, не пропустили ли мы какого-то шага рассуждения.

Из всех перечисленных задач эта выглядит наиболее реалистичной. К сожалению, пока что работы и в этом направлении не ушли далеко: формальная запись доказательства в виде, пригодном для машинной проверки, является долгим и скучным делом, на которое у математиков не хватает энтузиазма и терпения. А разработать удобные средства такой записи пока не удалось.

Короче говоря, революционная программа Лейбница построения формальных оснований математики осуществилась, но незаметно: под здание математики подвели новый (и довольно прочный) фундамент, но большинство жильцов про это до сих пор не знают.

Так что же, математическая логика бесполезна? Ни в коем случае: она не только удовлетворяет естественный философский интерес к основаниям математики, но и содержит множество красивых результатов, которые важны не только для математики, но и для computer science.

В этой книжке мы расскажем об одном из центральных понятий математической логики — языках и исчислениях первого порядка. В этих языках разрешается употреблять логические связки «и», «или», «если … то», а также кванторы «для всех» и «существует». Оказывается, что этих средств достаточно для формализации математических теорий и что можно построить простые формальные правила, полностью отражающие смысл этих логических средств.

Авторы пользуются случаем ещё раз поблагодарить своего учителя, Владимира Андреевича Успенского, лекции, тексты и высказывания которого повлияли на них (и на содержание этой книги), вероятно, даже в большей степени, чем авторы это осознают.

При подготовке текста использованы записи А. Евфимьевского и А. Ромащенко (который также прочёл предварительный вариант книги и нашёл там немало ошибок).

Оригинал-макет книги подготовлен её редактором, В. В. Шуваловым; без его настойчивости (вплоть до готовности разделить ответственность за ошибки) оригинал-макет вряд ли появился бы к какому-либо сроку. Он же вместе с М. А. Ушаковым (нашедшим несколько существенных ошибок) подготовил предметный указатель. Мы признательны также К. С. Макарычеву и Ю. С. Макарычеву, которые внимательно прочли вёрстку книги и нашли там немало опечаток.

Авторы признательны École Normale Supérieure de Lyon (Франция) за поддержку и гостеприимство во время написания этой книги.

Издание книги стало возможным благодаря Российскому фонду фундаментальных исследований, а также И. В. Ященко, который уговорил авторов подать туда заявку.

Наконец, мы благодарим сотрудников, аспирантов и студентов кафедры математической логики мехмата МГУ, а также всех участников наших лекций и семинаров и читателей предварительных вариантов этой книги.

Просим сообщать о всех ошибках и опечатках авторам (электронные адреса `ver@mccme.ru`, `shen@mccme.ru`; почтовый адрес: Москва, 121002, Большой Власьевский пер., 11, Московский центр непрерывного математического образования).

Н. К. Верещагин, А. Шень

1. Логика высказываний

1.1. Высказывания и операции

«Если число π рационально, то π — алгебраическое число. Но оно не алгебраическое. Значит, π не рационально.» Мы не обязаны знать, что такое число π, какие числа называют рациональными и какие алгебраическим, чтобы признать, что это рассуждение правильно — в том смысле, что из двух сформулированных посылок действительно вытекает заключение. Такого рода ситуации — когда некоторое утверждение верно независимо от смысла входящий в него высказываний — составляют предмет *логики высказываний*.

Такое начало (особенно если учесть, что курс логики входил в программу философского факультета, где также изучалась «диалектическая логика») настораживает, но на самом деле наши рассмотрения будут иметь вполне точный математический характер, хотя мы начнём с неформальных мотивировок.

Высказывания могут быть *истинными* и *ложными*. Например, «$2^{16}+1$ — простое число» — истинное высказывание, а «$2^{32}+1$ — простое число» — ложное (это число делится на 641). Про высказывание «существует бесконечно много простых p, для которых $p+2$ — также простое» никто не берётся сказать наверняка, истинно оно или ложно. Заметим, что «x делится на 2» в этом смысле не является высказыванием, пока не сказано, чему равно x; при разных x получаются разные высказывания, одни истинные (при чётном x), другие — ложные (при нечётном x).

Высказывания можно соединять друг с другом с помощью «логических связок». Эти связки имеют довольно странные, но традиционные названия и обозначения (табл. 1). Отметим также, что в импликации $A \Rightarrow B$ высказывание A называют *посылкой*, или *антецедентом импликации*, а B — *заключением*, или *консеквентом*.

Говорят также, что высказывание имеет *истинност-*

связка	обозначение	название
A и B	$A\&B$ $A \wedge B$ A `and` B	конъюнкция
A или B	$A \vee B$ A `or` B	дизъюнкция
не A A неверно	$\neg A$ $\sim A$ $\overline{A}$ `not` A	отрицание
из A следует B если A, то B A влечёт B B — следствие A	$A \to B$ $A \Rightarrow B$ $A \supset B$ `if` A `then` B	импликация следование

Таблица 1. Логические связки, обозначения и названия

ное значение **И** (истина), если оно истинно, или **Л** (ложь), если оно ложно. Иногда вместо **И** употребляется буква **T** (true) или число 1, а вместо **Л** — буква **F** (false) или число 0. (С первого взгляда идея произвольным образом выбрать числа 0 и 1 кажется дикой — какая бы польза могла быть от, скажем, сложения истинностных значений? Удивительным образом в последние годы обнаружилось, что такая польза есть, и если оперировать с истиной и ложью как элементами конечного поля, можно получить много неожиданных результатов. Но это выходит за рамки нашей книги.)

Логические связки позволяют составлять сложные высказывания из простых. При этом истинность составного высказывания определяется истинностью его частей в соответствии с таблицей 2.

Те же правила можно изложить словесно. Высказывание $A \wedge B$ истинно, если оба высказывания A и B истинны. Высказывание $A \vee B$ истинно, если хотя бы одно из высказываний A и B истинно. Высказывание $A \to B$ ложно в единственном случае: если A истинно, а B ложно. Наконец, $\neg A$ истинно в том и только том случае, когда A ложно.

A	B	$A \wedge B$	$A \vee B$	$A \to B$
Л	**Л**	**Л**	**Л**	**И**
Л	**И**	**Л**	**И**	**И**
И	**Л**	**Л**	**И**	**Л**
И	**И**	**И**	**И**	**И**

A	$\neg A$
Л	**И**
И	**Л**

Таблица 2. Таблицы истинности для логических связок

Из всех связок больше всего вопросов вызывает импликация. В самом деле, не очень понятно, почему надо считать, скажем, высказывания «если $2 \times 2 = 5$, то $2 \times 2 = 4$» и «если $2 \times 2 = 5$, то $3 \times 3 = 1$» истинными. (Именно так говорят наши таблицы: **Л** $\to$ **И** $=$ **Л** $\to$ **Л** $=$ $=$ **И**.) Следующий пример показывает, что в таком определении есть смысл.

Общепризнано, что если число x делится на 4, то оно делится на 2. Это означает, что высказывание

$$(x \text{ делится на } 4) \ \to \ (x \text{ делится на } 2)$$

истинно при всех x. Подставим сюда $x = 5$: обе части ложны, а утверждение в целом истинно. При $x = 6$ посылка импликации ложна, а заключение истинно, и вся импликация истинна. Наконец, при $x = 8$ посылка и заключение истинны и импликация в целом истинна. С другой стороны, обратное утверждение (если x делится на 2, то x делится на 4) неверно, и число 2 является контрпримером. При этом посылка импликации истинна, заключение ложно, и сама импликация ложна. Таким образом, если считать, что истинность импликации определяется истинностью её частей (а не наличием между ними каких-то причинно-следственных связей), то все строки таблицы истинности обоснованы. Чтобы подчеркнуть такое узко-формальное понимание импликации, философски настроенные логики называют её «материальной импликацией».

Теперь от неформальных разговоров перейдём к определениям. Элементарные высказывания (из которых составляются более сложные) мы будем обозначать маленькими латинскими буквами и называть *пропозициональными переменными*. Из них строятся *пропозициональные формулы* по таким правилам:

- Всякая пропозициональная переменная есть формула.
- Если A — пропозициональная формула, то $\neg A$ — пропозициональная формула.
- Если A и B — пропозициональные формулы, то $(A \wedge B)$, $(A \vee B)$ и $(A \to B)$ — пропозициональные формулы.

Можно ещё сказать так: формулы образуют минимальное множество, обладающее указанными свойствами (слово «минимальное» здесь существенно: ведь если бы мы объявили любую последовательность переменных, скобок и связок формулой, то эти три свойства были бы тоже выполнены).

Пусть формула φ содержит n пропозициональных переменных $p_1, p_2, \ldots, p_n$. Если подставить вместо этих переменных истинностные значения (**И** или **Л**), то по таблицам можно вычислить истинностное значение формулы в целом. Таким образом, формула задаёт некоторую функцию от n аргументов, каждый из которых может принимать значения **Л** и **И**. Значения функции также лежат в множестве $\{$**Л**, **И**$\}$, которое мы будем обозначать $\mathbb{B}$. Мы будем следовать уже упоминавшейся традиции и отождествлять **И** с единицей, а **Л** — с нулём, тем самым $\mathbb{B}$ есть $\{0, 1\}$. Формула φ задаёт отображение типа $\mathbb{B}^n \to \mathbb{B}$. Такие отображения называют также *булевыми функциями n аргументов*.

Пример. Рассмотрим формулу $(p \wedge (q \wedge \neg r))$. Она истинна в единственном случае — когда p и q истинны, а r ложно (см. таблицу 3).

Некоторые формулы выражают логические законы — составные высказывания, истинные независимо от смы-

p	q	r	$\neg r$	$(q \wedge \neg r)$	$(p \wedge (q \wedge \neg r))$
0	0	0	1	0	0
0	0	1	0	0	0
0	1	0	1	1	0
0	1	1	0	0	0
1	0	0	1	0	0
1	0	1	0	0	0
1	1	0	1	1	1
1	1	1	0	0	0

Таблица 3. Таблица истинности для $(p \wedge (q \wedge \neg r))$.

сла их частей. Такие формулы (истинные при всех значениях входящих в них переменных) называют *тавтологиями*.

Пример. Формула $((p \wedge q) \to p)$ является тавтологией (это можно проверить, например, составив таблицу). Она выражает такой логический закон: из конъюнкции утверждений следует первое из них.

1. Как выглядит симметричное утверждение для дизъюнкции и какая формула его выражает?

Две формулы называют *эквивалентными*, если они истинны при одних и тех же значениях переменных (другими словами, если они задают одну и ту же булеву функцию). Например, формула $(p \wedge (p \to q))$ истинна лишь при $p = q = \textbf{И}$, и потому эквивалентна формуле $(p \wedge q)$.

Рассмотрим формулу $((p \wedge q) \vee q)$. Она истинна, если переменная q истинна, и ложна, если переменная q ложна. Хотелось бы сказать, что она эквивалентна формуле q, но тут есть формальная трудность: она содержит две переменные и потому задаёт функцию от двух аргументов (типа $\mathbb{B} \times \mathbb{B} \to \mathbb{B}$), в то время как формула q задаёт функцию одного аргумента. Мы не будем обращать на это внимания и будем считать эти формулы эквивалентными. Вообще, если есть список переменных $p_1, \ldots, p_n$, содержащий все переменные некоторой формулы φ (и, возможно, ещё какие-то переменные), можно считать, что формула φ задаёт функцию от n аргументов, возможно, на деле зависящую не от всех аргументов (постоянную по некоторым аргументам)

После сделанных оговорок легко проверить следующий факт: формулы φ и ψ эквивалентны тогда и только тогда, когда формула $((\varphi \to \psi) \wedge (\psi \to \varphi))$ является тавтологией. Используя сокращение $(p \leftrightarrow q)$ для $((p \to q) \wedge \wedge (q \to p))$, можно записывать утверждения об эквивалентности формул в виде тавтологий. Вот несколько таких эквивалентностей:

Теорема 1. Формулы

$$\begin{aligned}
(p \wedge q) &\leftrightarrow (q \wedge p);\\
((p \wedge q) \wedge r) &\leftrightarrow (p \wedge (q \wedge r));\\
(p \vee q) &\leftrightarrow (q \vee p);\\
((p \vee q) \vee r) &\leftrightarrow (p \vee (q \vee r));\\
(p \wedge (q \vee r)) &\leftrightarrow ((p \wedge q) \vee (p \wedge r));\\
(p \vee (q \wedge r)) &\leftrightarrow ((p \vee q) \wedge (p \vee r));\\
\neg(p \wedge q) &\leftrightarrow (\neg p \vee \neg q);\\
\neg(p \vee q) &\leftrightarrow (\neg p \wedge \neg q);\\
(p \vee (p \wedge q)) &\leftrightarrow p;\\
(p \wedge (p \vee q)) &\leftrightarrow p;\\
(p \to q) &\leftrightarrow (\neg q \to \neg p);\\
p &\leftrightarrow \neg\neg p
\end{aligned}$$

являются тавтологиями.

$\triangleleft$ Первые четыре эквивалентности выражают коммутативность и ассоциативность конъюнкции и дизъюнкции. Проверим, например, вторую: левая и правая части истинны в единственном случае (когда все переменные истинны), и потому эквивалентны. (Для дизъюнкции удобнее смотреть, когда она ложна.)

Две следующие эквивалентности утверждают дистрибутивность — заметим, что в отличие от сложения и умножения в кольцах здесь верны оба свойства дистрибутивности. Проверить эквивалентность легко, если отдельно рассмотреть случаи истинного и ложного p.

Следующие два свойства, *законы Де Моргана*, легко проверить, зная, что конъюнкция истинна, а дизъюнкция ложна лишь в одном случае. Эти свойства иногда выражают словами: «конъюнкция двойственна дизъюнкции».

Далее следуют два очевидных *закона поглощения* (один из них мы уже упоминали).

За ними идёт правило *контрапозиции*, которое говорит, в частности, что утверждения «если x совершенно, то x чётно» и «если x нечётно, то x несовершенно» равносильны. Хотя оно и очевидно проверяется с помощью таблиц истинности, с ним связаны любопытные парадоксы. Вот один из них.

Биолог А выдвинул гипотезу: все вороны чёрные. Проверяя её, он вышел во двор и обнаружил на дереве ворону. Она оказалось чёрной. Биолог А радуется — гипотеза подтверждается. Биолог Б переформулировал гипотезу так: все не-чёрные предметы — не вороны (применив наше правило контрапозиции) и не стал выходить во двор, а открыл холодильник и нашёл там оранжевый предмет. Он оказался апельсином, а не вороной. Биолог Б обрадовался — гипотеза подтверждается — и позвонил биологу А. Тот удивляется — у него тоже есть апельсин в холодильнике, но с его точки зрения никакого отношения к его гипотезе апельсин не имеет ...

Другой парадокс: с точки зрения формальной логики утверждения «кто не с нами, тот против нас» и «кто не против нас, тот с нами» равносильны.

Последнее (и очевидное) правило $p \leftrightarrow \neg\neg p$ называется *снятием двойного отрицания.* $\triangleright$

2. Перечисленные эквивалентности соответствуют равенствам для множеств: например, первая гарантирует, что $P \cap Q = Q \cap P$ для любых множеств P и Q. Какие утверждения соответствуют остальным эквивалентностям?

3. Две формулы, содержащие только переменные и связки $\wedge$, $\vee$ и $\neg$, эквивалентны. Докажите, что они останутся эквивалентными, если всюду заменить $\wedge$ на $\vee$ и наоборот.

Далеко не все тавтологии имеют ясный интуитивный смысл. Например, формула $(p \to q) \vee (q \to p)$ является тавтологией (если одно из утверждений p и q ложно, то из него следует всё, что угодно; если оба истинны, то тем более формула истинна), хотя и отчасти противоречит нашей интуиции — почему, собственно, из двух никак не связанных утверждений одно влечёт другое? Ещё более загадочна тавтология

$$((p \to q) \to p) \to p$$

(хотя её ничего не стоит проверить с помощью таблиц истинности).

Отступление о пользе скобок. На самом деле наше определение истинности содержит серьёзный пробел. Чтобы обнаружить его, зададим себе вопрос: зачем нужны скобки в формулах? Представим себе, что мы изменим определение формулы, и будем говорить, что $P \wedge Q$ и $P \vee Q$ являются формулами для любых P и Q. Останутся ли наши рассуждения в силе?

Легко понять, что мы столкнёмся с трудностью при определении булевой функции, соответствующей формуле. В этом определении мы подставляли нули и единицы на место переменных и затем вычисляли значение формулы с помощью таблиц истинности для связок. Но теперь, когда мы изменили определение формулы, формула $p \wedge q \vee r$ может быть получена двумя способами — из формул $p \wedge q$ и r с помощью операции $\vee$ и из формул p и $q \vee r$ с помощью операции $\wedge$. Эти два толкования дадут разный результат при попытке вычислить значение $0 \wedge 0 \vee 1$.

Из сказанного ясно, что скобки нужны, чтобы гарантировать однозначность синтаксического разбора формулы. Точнее говоря, верно такое утверждение:

Теорема 2 (однозначность разбора). Пропозициональная формула, не являющаяся переменной, может быть представлена ровно в одном из четырёх видов $(A \wedge B)$,

$(A \vee B)$, $(A \to B)$ или $\neg A$, где A и B — некоторые формулы, причём A и B (в первых трёх случаях) восстанавливаются однозначно.

$\triangleleft$ Формальное доказательство можно провести так: назовём *скобочным итогом* разницу между числом открывающихся и закрывающихся скобок. Индукцией по построению формулы легко доказать такую лемму:

Лемма. Скобочный итог формулы равен нулю. Скобочный итог любого начала формулы неотрицателен и равен нулю, лишь если это начало совпадает со всей формулой, пусто или состоит из одних символов отрицания.

Слова «индукцией по построению» означают, что мы проверяем утверждение для переменных, а также доказываем, что если оно верно для формул A и B, то оно верно и для формул $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ и $\neg A$.

После того как лемма доказана, разбор формулы проводится так: если она начинается с отрицания, то может быть образована лишь по третьему правилу. Если же она начинается со скобки, то надо скобку удалить, а потом искать непустое начало, имеющее нулевой скобочный итог и не оканчивающееся на знак логической операции. Такое начало единственно (как легко проверить, используя лемму). Это начало и будет первой частью формулы. Тем самым формула разбирается однозначно. $\triangleright$

Нет смысла вдаваться в подробности этого (несложного) рассуждения: вообще-то алгоритмы разбора формул — это отдельная большая и практически важная тема (в первую очередь в связи с компиляторами). Приведённый нами алгоритм далеко не оптимален. С другой стороны, мы вообще можем обойти эту проблему, потребовав, чтобы при записи формул левая и правая скобки, окружающие формулу, связывались линией — тогда однозначность разбора формулы не вызывает вопросов, и больше ничего нам не надо.

В дальнейшем мы будем опускать скобки, если они либо не играют роли (например, можно написать конъюнкцию трёх членов, не указывая порядок действий в силу ассоциативности), либо ясны из контекста.

4. Польский логик Лукасевич предлагал обходиться без скобок, записывая в формулах сначала знак операции, а потом операнды (без пробелов и разделителей). Например, $(a+b) \times \times (c+(d \times e))$ в его обозначениях запишется как $\times{+}ab{+}c{\times}de$. Эту запись ещё называют *польской* записью. Обратная польская запись отличается от неё тем, что знак операции идёт после операндов. Покажите, что в обоих случаях порядок действий восстанавливается однозначно.

1.2. Полные системы связок

Рассматриваемая нами система пропозициональных связок ($\wedge$, $\vee$, $\to$, $\neg$) *полна* в следующем смысле:

Теорема 3 (Полнота системы связок). Любая булева функция n аргументов может быть записана в виде пропозициональной формулы.

$\lhd$ Проще всего пояснить это на примере. Пусть, например, булева функция $\varphi(p,q,r)$ задана таблицей 4.

p	q	r	$\varphi(p,q,r)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

$$(\neg p \wedge \neg q \wedge \neg r) \vee \\ \vee (\neg p \wedge q \wedge r) \vee \\ \vee (p \wedge q \wedge r)$$

Таблица 4. Булева функция и задающая её формула.

В таблице есть три строки с единицами в правой колонке — три случая, когда булева функция истинна (равна 1). Напишем три конъюнкции, каждая из которых покрывает один случай (а в остальных строках ложна), и соединим их дизъюнкцией. Нужная формула построена.

Ясно, что аналогичная конструкция применима для любой таблицы (с любым числом переменных). $\rhd$

Для формул подобного вида есть специальное название: формулы в *дизъюнктивной нормальной форме*. Более подробно: *литералом* называется переменная или отрицание переменной, *конъюнктом* называется произвольная конъюнкция литералов, а дизъюнктивной нормальной формой называется дизъюнкция конъюнктов. В нашем случае в каждый конъюнкт входит n литералов (где n — число переменных), а число конъюнктов равно числу строк с единицами и может меняться от нуля (тогда, правда, получается не совсем формула, а «пустая дизъюнкция», и её можно заменить какой-нибудь всегда ложной формулой типа $p\wedge\neg p$) до 2^n (если булева функция всегда истинна).

5. Длина построенной в доказательстве теоремы 3 формулы зависит от числа единиц: формула будет короткой, если единиц в таблице мало. А как написать (сравнительно) короткую формулу, если в таблице мало нулей, а в основном единицы?

Иногда полезна *конъюнктивная нормальная форма*, которая представляет собой конъюнкцию *дизъюнктов*. Каждый дизъюнкт состоит из литералов, соединённых дизъюнкциями. Теорему 3 можно теперь усилить так:

Теорема 4. Всякая булева функция может быть выражена формулой, находящейся в дизъюнктивной нормальной форме, а также формулой, находящейся в конъюнктивной нормальной форме.

◁ Первая часть утверждения уже доказана. Вторая часть аналогична первой, надо только для каждой строки с нулём написать подходящий дизъюнкт.

Можно также представить функцию $\neg\varphi$ в дизъюнктивной нормальной форме, а затем воспользоваться законами Де Моргана, чтобы внести отрицание внутрь. ▷

6. Проведите второй вариант рассуждения подробно.

Вообще говоря, определение нормальной формы не требует, чтобы в каждом конъюнкте (или дизъюнкте) встречались все переменные. (Повторять переменную больше одного раза смысла нет; если, например, переменная и её отрицание входят в одну конъюнкцию, то эта конъюнкция всегда ложна и её можно выбросить.)

7. Приведите пример булевой функции n аргументов, у которой любая дизъюнктивная или конъюнктивная нормальная форма содержит лишь члены длины n. (Указание: рассмотрите функцию, которая меняет своё значение при изменении значения любой переменной.)

Заметим, что при доказательстве теоремы 3 мы обошлись без импликации. Это и не удивительно, так как она выражается через дизъюнкцию и отрицание:

$$(p \to q) \ \leftrightarrow \ (\neg p \vee q)$$

(проверьте!). Мы могли бы обойтись только конъюнкцией и отрицанием, так как

$$(p \vee q) \ \leftrightarrow \ \neg(\neg p \wedge \neg q),$$

или только дизъюнкцией и отрицанием, так как

$$(p \wedge q) \ \leftrightarrow \ \neg(\neg p \vee \neg q)$$

(обе эквивалентности вытекают из законов Де Моргана; их легко проверить и непосредственно). Как говорят, система связок $\wedge, \neg$, а также система связок $\vee, \neg$ являются *полными*. (По определению это означает, что с их помощью можно записать любую булеву функцию.)

8. Докажите, что система связок $\neg, \to$ полна. (Указание: как записать через них дизъюнкцию?)

А вот без отрицания обойтись нельзя. Система связок $\wedge, \vee, \to$ неполна — и по очень простой причине: если все переменные истинны, то любая их комбинация, содержащая только указанные связки, истинна. (Как говорят, все эти связки «сохраняют единицу».)

9. Легко понять, что любая формула, составленная только с помощью связок $\wedge$ и $\vee$, задаёт монотонную булеву функцию (в том смысле, что от увеличения значения любого из аргументов значение функции может только возрасти — или остаться прежним). Покажите, что любая монотонная булева функция может быть выражена формулой, содержащей только $\wedge$ и $\vee$.

10. Пусть $\varphi \to \psi$ — тавтология. Покажите, что найдётся формула τ, которая включает в себя только общие для φ и ψ переменные, для которой формулы $(\varphi \to \tau)$ и $(\tau \to \psi)$ являются тавтологиями. (Более общий вариант этого утверждения, в котором рассматриваются формулы с кванторами, называется *леммой Крейга*.)

В принципе мы не обязаны ограничиваться четырьмя рассмотренными связками. Любая булева функция может играть роль связки. Например, можно рассмотреть связку (p `notand` q), задаваемую эквивалентностью

$$(p \ \texttt{notand}\ q) \ \leftrightarrow\ \neg(p \wedge q)$$

(словами: (p `notand` q) ложно, лишь если p и q истинны). Через неё выражается отрицание (p `notand` p), после чего можно выразить конъюнкцию, а затем, как мы знаем, и вообще любую функцию. (Знакомые с цифровыми логическими схемами малого уровня интеграции хорошо знакомы с этим утверждением: достаточно большой запас схем И-НЕ позволяет реализовать любую требуемую зависимость выхода от входов.)

Другая интересная полная система связок — сложение по модулю 2, конъюнкция и константа 1 (которую можно считать 0-арной связкой, задающей функцию от нуля аргументов). Представленные в этой системе булевы функции становятся полиномами с коэффициентами в кольце вычетов по модулю 2. Идея рассматривать булевы функции как полиномы (оказавшаяся неожиданно плодотворной в последние годы) была высказана в 1927 г. российским математиком Иваном Ивановичем Жегалкиным.

Назовём *мономом* конъюнкцию любого набора переменных или константу 1 (которую естественно рассматривать как конъюнкцию нуля переменных). Название это естественно, так как при наших соглашениях (1 обозначает истину, 0 — ложь) конъюнкция соответствует умножению.

Назовём *полиномом* сумму таких мономов по модулю 2 (это значит, что $0 \oplus 0 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$ и $1 \oplus 1 = 0$). Ясно, что два повторяющихся монома можно сократить (ведь сложение по модулю 2), так что будем рассматривать только полиномы без повторяющихся мономов. При этом, естественно, порядок членов в мономе (как и порядок мономов в полиноме) роли не играет, их можно переставлять.

Теорема 5 (о полиномах Жегалкина). Всякая булева функция однозначно представляется таким полиномом.

$\triangleleft$ Существование искомого полинома следует из теоремы 4, так как конъюнкция есть умножение, отрицание — прибавление единицы, а дизъюнкцию можно через них выразить (получится $p + q + pq$). Надо только заметить, что степени не нужны: переменные принимают значения 0 и 1, так что x^n можно заменить на x.

Можно также сослаться на известное из алгебры утверждение о том, что всякая функция с аргументами из конечного поля (в данном случае это двухэлементное поле вычетов по модулю 2) задаётся полиномом. (Отсюда, кстати, получается новое доказательство теоремы 3.)

Далее можно заметить, что полиномов столько же, сколько булевых функций, а именно 2^{2^n}. В самом деле, булева функция может принимать любое из двух значений в каждой из 2^n точек булева куба $\mathbb{B}^n$, а многочлен может включать или не включать любой из 2^n мономов. (Мономов ровно 2^n, потому что каждый моном включает или не включает любую из n переменных.) Поэтому избытка полиномов нет, и если любая функция представима полиномом, то единственным образом.

Можно и не ссылаться на сведения из алгебры и теорему 4, а дать явную конструкцию. Это удобно сделать индукцией по n. Пусть мы уже умеем представлять любую булеву функцию от $n-1$ аргументов с помощью полинома. Тогда $\varphi(p_1, \ldots, p_n)$ можно представить как

$$\begin{aligned}\varphi(p_1, \ldots, p_n) = \varphi(0, p_2, \ldots, p_n) &+ \\ &+ [\varphi(0, p_2, \ldots, p_n) + \varphi(1, p_2, \ldots, p_n)]p_1\end{aligned}$$

(проверьте). Остаётся заметить, что правую часть можно представить полиномом по предположению индукции.

Для единственности также есть другое доказательство: пусть два многочлена (имеющие степень 1 по каждой переменной) равны при всех значениях переменных. Тогда их сумма (или разность — вычисления происходят по модулю 2) является ненулевым многочленом (содержит какие-то мономы), но тождественно равна нулю. Так не бывает, и это легко доказать по индукции. В самом деле, любой многочлен $A(p_1, \ldots, p_n)$ можно представить в виде

$$A(p_1, \ldots, p_n) = B(p_2, \ldots, p_n) + p_1 C(p_2, \ldots, p_n),$$

где B и C — многочлены от меньшего числа переменных. Подставляя сначала $p_1 = 0$, а затем $p_1 = 1$, убеждаемся, что многочлены B и C равны нулю во всех точках, и потому (согласно предположению индукции) равны нулю как многочлены (не содержат мономов). $\triangleright$

11. Пусть F — произвольное поле. Назовём *мультилинейной* функцией полином от n переменных с коэффициентами из F, в котором все показатели степеней равны либо 0, либо 1. (Таким образом, каждый моном в ней есть произведение коэффициента и некоторого набора переменных без повторений.) Будем рассматривать $\mathbb{B} = \{0, 1\}$ как подмножество F. Докажите, что всякая булева функция $\mathbb{B}^n \to \mathbb{B}$ однозначно продолжается до мультилинейной функции $F^n \to F$, и коэффициенты мультилинейной функции можно считать целыми числами.

Если рассматривать произвольные булевы функции в качестве связок, возникает вопрос: в каком случае набор булевых функций образует полный базис? (Это значит, что любая булева функция представляется в виде композиции функций из набора, т. е. записывается в виде формулы, где связками служат функции набора.) Подобные вопросы вызывали в своё время большой интерес и были хорошо изучены. Начальным этапом явилось такое утверждение:

Теорема 6 (критерий Поста). Набор булевых функций тогда и только тогда является полным, когда он не содержится целиком ни в одном из пяти следующих «предполных классов»:

- монотонные функции;
- функции, сохраняющие нуль;
- функции, сохраняющие единицу;
- линейные функции;
- самодвойственные функции.

(Функция f *монотонна*, если она монотонно неубывает по каждому из своих аргументов. Функция f *сохраняет нуль/единицу*, если $f(0,\ldots,0) = 0$ (соответственно $f(1,\ldots,1) = 1$). Функция f *линейна*, если она представима многочленом, в котором все мономы содержат не более одной переменной. Наконец, функция f называется *самодвойственной*, если $f(1-p_1,\ldots,1-p_n) = 1-f(p_1,\ldots,p_n)$.)

$\triangleleft$ Если набор содержится в одном из классов, то и все композиции также не выходят за пределы этого класса (легко проверить для каждого из классов в отдельности) и поэтому набор не является полным. Докажем обратное утверждение. Пусть для каждого класса выбрана какая-то функция, в нём не лежащая. Убедимся, что с помощью комбинаций выбранных функций можно получить все булевы функции.

У нас есть функция, не сохраняющая нуль. Подставим вместо всех аргументов одну и ту же переменную. Получится функция от одного аргумента, отображающая нуль в единицу, то есть либо константа 1, либо отрицание. Сделав то же самое с функцией, не сохраняющей единицу, получим либо константу нуль, либо отрицание. Таким образом, у нас либо есть отрицание, либо обе константы 0 и 1.

Если есть обе константы, то всё равно можно получить отрицание. Возьмём немонотонную функцию. Легко понять, что она должна менять значение с единицы на нуль при изменении какого-то одного аргумента с нуля на единицу (в самом деле, будем увеличивать аргументы по одному, в какой-то момент значение функции уменьшится.) Зафиксировав значения остальных аргументов (ведь мы считаем, что константы есть), получаем отрицание.

Имея отрицание и несамодвойственную функцию, легко получить константы (если их не было). В самом деле, несамодвойственность означает, что $f(x_1,\ldots,x_n) = f(1-x_1,\ldots,1-x_n)$ для каких-то значений $x_1,\ldots,x_n \in \{0,1\}$. Вместо нулевых значений переменных $x_1,\ldots,x_n$ подставим p, вместо единиц подставим $\neg p$, получится одна из констант. Вторая получится отрицанием.

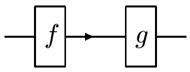
Теперь у нас есть константы, отрицание и нелинейная функция $f(p_1,\ldots,p_n)$. Нелинейность означает, что в её представлении в виде многочлена есть моном, состоящий более чем из одной переменной. Пусть, например, этот моном содержит переменные p_1 и p_2. Сгруппируем члены по четырём группам и получим выражение

$$p_1p_2A(p_3,\ldots) + p_1B(p_3,\ldots) + p_2C(p_3,\ldots) + D(p_3,\ldots).$$

При этом многочлен $A(p_3,\ldots)$ заведомо отличен от нуля, поэтому можно так подставить константы вместо $p_3,\ldots,p_n$, чтобы первое слагаемое не обратилось в нуль. Тогда получим либо $p_1p_2 + d$, либо $p_1p_2 + p_1 + d$, либо $p_1p_2 + p_2 + d$, либо $p_1p_2 + p_1 + p_2 + d$. Свободный член d можно менять, если нужно (у нас есть отрицание), так что получается либо p_1p_2 (конъюнкция, и всё доказано), либо $p_1p_2 + p_1 = p_1(p_2+1) = p_1 \wedge \neg p_2$ (убираем отрицание, получаем конъюнкцию, всё доказано), либо $p_1p_2 + p_2$ (аналогично), либо $p_1p_2 + p_1 + p_2 = (1+p_1)(1+p_2) - 1 = \neg(\neg p_1 \wedge \neg p_2) = p_1 \vee p_2$ (дизъюнкция, всё доказано). $\triangleright$

1.3. Схемы из функциональных элементов

Формулы представляют собой способ записи композиции функций. Например, если мы сначала применяем функцию f, а потом функцию g, это можно записать формулой $g(f(x))$. Но есть и другой способ: можно изобразить каждую функцию в виде прямоугольника с «входом» и «выходом» и соединить выход функции f со входом функции g (рис. 1).



$g(f(x))$

Рис. 1. Два способа изобразить композицию $g \circ f$.

Такое представление отнюдь не является чисто теоретическим. В течении нескольких десятков лет электронная промышленность выпускает микросхемы, которые выполняют логические операции. Такая микросхема имеет электрические контакты, напряжение на которых кодирует логические значения **И** и **Л**. Конкретное напряжение зависит от типа схемы, но обычно это несколько вольт, и высокий потенциал (относительно заземления) считается единицей, а низкий нулём.

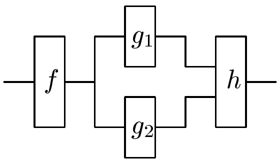
Одной из типичных схем является схема И-НЕ, она имеет два входа и один выход. Сигнал на выходе является отрицанием конъюнкции сигналов на входе. Другими словами, на выходе появляется высокий потенциал (сигнал 1) тогда и только тогда, когда на одном из входов потенциал низкий (0). Из такой схемы легко получить схему НЕ (изменяющую уровень сигнала на противоположный), соединив проводом два входа. При этом на оба входа поступает один и тот же сигнал, и операция И его не меняет ($p \wedge p = p$), а НЕ меняет на противоположный. Взяв два элемента И-НЕ и используя второй из них в качестве элемента НЕ, инвертирующего сигнал с выхода первого элемента, получаем схему, которая реализует функцию И. А если поставить два элемента НЕ перед каждым из входов элемента И-НЕ, получим схему, реализующую функцию ИЛИ: $\neg(\neg p \wedge \neg q) \leftrightarrow (p \vee q)$.

Теорема 3 о полноте системы связок теперь гарантирует, что любую булеву функцию можно реализовать в виде схемы. Надо иметь в виду, однако, что предлагаемая в её доказательстве конструкция (дизъюнктивная нормальная форма) имеет скорее теоретический интерес, поскольку приводит к схемам очень большого размера даже для простых функций (если число аргументов велико). Например, схема, сравнивающая два 16-битных числа, должна иметь 32 входа и поэтому в её реализации с помощью дизъюнктивной нормальной формы будет порядка 2^{32} элементов — что мало реально. (Между тем такую схему можно построить гораздо проще, из нескольких сотен элементов.)

Поэтому вопрос о том, сколько элементов нужно для реализации той или иной функции, представляет большой интерес — как практический, так и философский. (Одна из центральных проблем математики и информатики, так называемая «проблема перебора», может быть сформулирована в этих терминах.)

Мы сейчас дадим более формальное определение схемы и реализуемой ей булевой функции. Но прежде всего ответим на такой вопрос — почему мы вообще говорим о схемах? Ведь можно записать композицию булевых функций в виде формулы, не будет ли это то же самое?

Оказывается, не совсем, и разницу легко увидеть на примере (рис. 2).



$h(g_1(f(x)), g_2(f(x)))$

Рис. 2. Элемент входит в формулу дважды.

Здесь один и тот же элемент схемы (f) приходится указывать в формуле дважды, поскольку его выход используется в качестве входа двух других элементов. Схемы, в которых такого ветвления нет (на практике ветвление вполне возможно, хотя и ограничено «нагрузочной способностью выхода», как говорят инженеры), как раз и соответствуют формулам. Но в общем случае полученная из данной схемы формула может быть длинной, даже если схема содержит небольшое число элементов, поскольку число копий может расти экспоненциально с ростом глубины схемы.

Хотя идея образования схемы из функциональных элементов, реализующих булевы функции, достаточно наглядна, дадим более формальное определение. Фиксируем некоторый набор булевых функций B. Пусть имеется n булевых (принимающих значения 0 и 1) переменных $x_1, \ldots, x_n$, называемых *входами.* Пусть также имеется некоторое число булевых переменных $y_1, \ldots, y_m$, называемых *проводниками.* Пусть для каждого проводника схемы задана булева функция из B, выражающая его значение через другие проводники и входы. При этом требуется, чтобы не было циклов (цикл образуется, когда y_i зависит от y_j, которое зависит от y_k, ..., которое зависит от y_i). Пусть, кроме того, среди проводников выделен один, называемый *выходом.* В таком случае говорят, что задана *схема из функциональных элементов в базисе B* с n входами. Число m называют *размером* схемы. (С точки зрения инженера размер — это число использованных элементов, а базис B — это ассортимент доступных ему элементов.)

Отсутствие циклов гарантирует, что есть проводник, зависящий только от входов (иначе можно было бы найти цикл: возьмём какой-то проводник, затем возьмём тот проводник, от которого он зависит и т. д.). Значение этого проводника, таким образом, однозначно определяется сигналами на входах. Среди оставшихся проводников также нет цикла, поэтому можно найти один из них, зависящий только от уже известных, и определить его значение. Перенумеровав проводники в таком порядке, мы можем записать последовательность присваиваний

$$\begin{aligned} y_1 &:= f_1(\ldots); \\ y_2 &:= f_2(\ldots); \\ &\ldots \\ y_m &:= f_m(\ldots), \end{aligned}$$

в правых частях которых стоят функции из B, применённые ко входам и уже найденным значениям. При этом можно считать, что результат схемы есть y_m (все последующие присваивания уже не нужны). Такая программа определяет y_m при известных значениях входов, и тем самым *вычисляет* некоторую булеву функцию.

Теперь набор булевых функций B можно назвать *полным*, если любая булева функция может быть задана схемой из B-элементов (существует программа, её вычисляющая, при этом в правых частях присваиваний стоят функции из B). Ясно, что это определение полноты равносильно прежнему, то есть возможности записать булеву функцию в виде формулы со связками из B (как мы говорили, разница только в том, что один и тот же элемент будет фигурировать в формуле многократно).

Сложностью булевой функции f относительно B называют минимальный размер схемы из B-элементов, вычисляющей функцию f. Его обозначают $\mathrm{size}_B(f)$.

Теорема 7. Пусть B_1 и B_2 — два полных набора булевых функций. Тогда соответствующие меры сложности отличаются не более чем на постоянный множитель: найдётся такое число C, что $\mathrm{size}_{B_1}(f) \leqslant C\,\mathrm{size}_{B_2}(f)$ и $\mathrm{size}_{B_2}(f) \leqslant C\,\mathrm{size}_{B_1}(f)$ для любой функции f.

$\triangleleft$ Утверждение почти очевидно: поскольку наборы B_1 и B_2 полны, то каждая функция одного из наборов может быть вычислена какой-то схемой, составленной из элементов другого набора. Теперь можно взять в качестве C наибольший размер таких схем, и неравенства будут выполняться: каждую строку программы можно заменить на C (или меньше) строк с использованием функций другого набора. $\triangleright$

Что можно сказать о сложности произвольной булевой функции n аргументов? Следующая теорема показывает, что она экспоненциально зависит от n (для «наугад взятой» функции).

Теорема 8. (**а**) Пусть $c > 2$. Тогда сложность любой булевой функции n аргументов не превосходит c^n для всех достаточно больших n. (**б**) Пусть $c < 2$. Тогда сложность большинства булевых функций n аргументов не меньше c^n для всех достаточно больших n.

$\triangleleft$ Прежде всего заметим, что по предыдущей теореме не имеет значения, какой полный базис выбрать (изменение значения c более существенно, чем умножение сложности на константу).

Первое утверждение теоремы очевидно: размер схемы, реализующей дизъюнктивную нормальную форму с n переменными, есть $O(n2^n)$, поскольку имеется не более 2^n конъюнктов размера $O(n)$. (Напомним смысл O-обозначений: $O(n2^n)$ означает, что существует верхняя оценка вида $Cn2^n$ для некоторой константы C.) Осталось заметить, что $O(n2^n) < c^n$ при достаточно больших n (напомним, что $c > 2$).

Чтобы доказать второе утверждение, оценим число различных схем (скажем, в базисе И, ИЛИ, НЕ) размера N с n аргументами. Каждая такая схема может быть описана последовательностью из N присваиваний, выражающих одну из переменных через предыдущие. Для каждого присваивания есть не более $3(N+n)^2$ вариантов (три типа операций — конъюнкция, дизъюнкция, отрицание, и каждый из не более чем двух аргументов выбирается среди не более чем $N+n$ вариантов). Отсюда легко получить оценку $2^{O(N\log N)}$ на число всех функций сложности не более N (считая $N \geqslant n$).

Всего булевых функций с n аргументами имеется 2^{2^n}. Из сравнения этих формул видно, что что при $c < 2$ и при достаточно больших n булевы функции сложности меньше c^n составляют меньшинство, так как $2^{O(c^n \log c^n)}$ много меньше 2^{2^n}. $\triangleright$

12. Проведите вторую часть рассуждения более подробно и покажите, что при некотором $\varepsilon > 0$ сложность большинства булевых функций с n аргументами не меньше $\varepsilon 2^n/n$.

Верхнюю оценку в теореме 8 можно усилить и показать, что сложность любой булевой функции n аргументов не превосходит $O(2^n/n)$.

13. (**а**) Покажите, что можно построить схему размера $O(2^m)$ с 2^m выходами, реализующую все 2^m возможных конъюнктов длины m (для каждого — свой выход). (Указание: такую схему можно построить индуктивно.) (**б**) Покажите, что можно построить схему размера $O(2^{2^m})$ с 2^{2^m} выходами, реализующую все 2^{2^m} булевых функций m аргументов. (Указание: эту схему также можно построить индуктивно.) (**в**) Пусть $\varphi(x_1, \ldots, x_k, y_1, \ldots, y_l)$ — булева функция, аргументы которой разбиты на две группы. Покажите, что её можно записать в виде дизъюнкции 2^k членов, каждый из которых имеет вид $C(x_1, \ldots, x_k) \wedge D(y_1, \ldots, y_l)$, где C — конъюнкт, а D — произвольная булева функция. Вывести отсюда упомянутую выше оценку $O(2^n/n)$. (Указание: разумно положить $k = n - \log n + c$, $l = \log n - c$. См. также [9] и [33].)

Теорема 8, однако, ничего не говорит о сложности конкретных булевых функций. Ситуация здесь такова. Есть разнообразные методы и приёмы получения верхних оценок. Но про нижние оценки неизвестно практически ничего. Про многие функции мы подозреваем, что их сложность велика (экспоненциально зависит от числа входов), но доказать это пока не удаётся. Весьма нетривиальные идеи позволяют доказывать экспоненциальные нижние оценки для некоторых специальных классов схем, например, схем из монотонных элементов или схем ограниченной глубины (использующих элементы И и ИЛИ с произвольным числом входов). Получение экспоненциальных оценок для более общих схем — один из возможных подходов к знаменитой *проблеме перебора*, центральной проблеме теории сложности вычислений.

Мы не будем углубляться в эту теорию, а приведём лишь несколько верхних оценок для конкретных задач. При этом мы не претендуем на полноту, а хотим лишь показать несколько интересных идей и приёмов.

Рассмотрим функцию сравнения двух n-битовых чисел. Она имеет $2n$ аргументов (n для одного числа и n для другого); её значение равно 1, если первое число больше второго, и 0 в противном случае.

Обозначим эту функцию Comp_n.

Теорема 9. Пусть B — полный набор функций. Существует такая константа C, что $\mathrm{size}_B(\mathrm{Comp}_n) \leqslant Cn$.

$\triangleleft$ Заметим, что поскольку в формулировке теоремы оценка размера проводится с точностью до константы, то выбор конкретного базиса не имеет значения. Другими словами, мы можем предполагать, что любое конечное число необходимых нам функций в этом базисе есть.

Схема сравнения чисел будет рекурсивной (чтобы сравнить два числа, мы отдельно сравниваем их левые и правые половины, а затем объединяем результаты). При этом, как часто бывает, надо усилить утверждение, чтобы индукция прошла. А именно, мы будем строить схему с $2n$ входами $x_1, \ldots, x_n, y_1, \ldots, y_n$ и двумя выходами, которая указывает, какой из трёх случаев $x < y$, $x = y$ или $x > y$ имеет место. (Здесь x, y — числа, записываемое в двоичной системе как $x_1 \ldots x_n$ и $y_1, \ldots, y_n$.) Два выходных бита кодируют четыре возможности, а нужно только три, так что есть некоторый запас. Для определённости можно считать, что первый выходной бит истинен, если числа равны, а второй — если $x < y$. Тогда возможны три варианта сигналов на выходе: 10 (равенство), 01 (при $x < y$) и 00 (при $x > y$).

Объясним теперь, как собрать, скажем, схему сравнения двух 16-разрядных чисел. Соберём отдельно схему сравнения старших 8 разрядов и младших 8 разрядов. Каждая из них даст ответ в форме двух битов. Теперь из этих четырёх битов надо собрать два. (Если в старших разрядах неравенство, то оно определяет результат сравнения; если старшие разряды равны, то результат сравнения определяется младшими разрядами.) Написанная в скобках фраза определяет булеву функцию с четырьмя битами на входе и двумя битами на выходе, и может быть реализована некоторой схемой фиксированного размера. Таким образом, если через $T(n)$ обозначить размер схемы, сравнивающей n-битовые числа, то получаем оценку

$$T(2n) \leqslant 2T(n) + c,$$

где c — некоторая константа, зависящая от выбора базиса. Отсюда следует, что $T(2^k) \leqslant c'2^k$ при некотором c'. В самом деле, для достаточно большого c' можно доказать по индукции, что

$$T(2^k) \leqslant c'2^k - c$$

(мы должны усилить неравенство, вычтя из правой части c, чтобы индуктивный шаг прошёл; база индукции остается верной, если c' достаточно велико).

Ту же самую оценку можно объяснить и наглядно. Наша схема имеет вид иерархического дерева. На каждом уровне из двух двухбитовых сигналов получается один. Остаётся вспомнить, что в полном двоичном дереве число внутренних вершин (которое определяет размер схемы) на единицу меньше числа листьев. (В турнире по олимпийской системе число игр на единицу меньше числа команд, так как после каждой игры одна команда выбывает.)

Все внутренние вершины и все листья (где сравниваются два бита) представляют собой схемы ограниченного размера, откуда и вытекает оценка $T(2^k) \leqslant c'2^k$.

Осталось лишь сказать, что делать, если размер чисел (который мы обозначали через n) не есть точная степень двойки. В этом случае можно увеличить размер до ближайшей сверху степени двойки (не более чем в два раза) и подать на старшие разряды входов нули. Оба действия приводят к увеличению размера схемы не более чем в константу раз. $\triangleright$

Перейдём к сложению двух n-разрядных чисел. (Строго говоря, тут возникает не булева функция, а функция $\mathbb{B}^n \times \mathbb{B}^n \to \mathbb{B}^{n+1}$, но все наши определения очевидно переносятся на этот случай.)

Теорема 10. Существует схема размера $O(n)$, осуществляющая сложение двух n-битовых чисел.

$\lhd$ Напомним смысл обозначения $O(n)$: нам надо построить схему сложения n-битовых чисел, имеющую размер не более cn для некоторого c и для всех n.

Вспомним, как складывают числа в столбик:

$$\begin{array}{r} 0\,1\,1 \\ 1\,0\,0\,1 \\ 1\,0\,1\,1 \\ \hline 1\,0\,1\,0\,0 \end{array}$$

Верхняя строка — биты переноса, нижняя — результат. Заметим, что каждый из битов переноса или результата определяется тремя другими битами (бит результата равен сумме двух битов слагаемых и бита переноса по модулю 2, а бит переноса равен 1, если хотя бы два из этих трёх битов равны 1). Поэтому можно составить схему, которая вычисляет эти биты справа налево и имеет размер $O(n)$. $\rhd$

Заметим, что теорему 9 легко вывести из теоремы 10: чтобы сравнить числа x и y, сложим число $(2^n - 1) - x$ (то есть число x, в котором все единицы заменены нулями и наоборот) и число y. Если в старшем разряде появится единица, то $y > x$, а если нет, то $y \leqslant x$. Остаётся заметить, что и сложение, и обращение битов в числе x требуют схем линейного размера. Таким образом, сравнение чисел сводится к вычислению бита переноса. Верно и обратное: вычисление бита переноса сводится к сравнению двух чисел (обратим в одном из слагаемых все биты).

Тем не менее конструкция, использованная при доказательстве теоремы 9, имеет некоторые преимущества. Назовём *глубиной* схемы максимальное число элементов на пути от входа к выходу. Если представить себе, что сигнал на выходе элемента появляется не сразу после подачи сигналов на входы, а с некоторой задержкой, то глубина схемы определяет суммарную задержку. Легко понять, что рекурсивная схема сравнения имела глубину

$O(\log n)$ (число уровней пропорционально логарифму размера входа), в то время как построенная только что схема сложения имеет глубину, пропорциональную n (биты переноса вычисляются последовательно, справа налево). Но можно соединить эти два результата:

Теорема 11. Существует схема сложения двух n-битовых чисел размера $O(n)$ и глубины $O(\log n)$.

$\triangleleft$ Как мы видели, проблема в том, что биты переноса вычисляются последовательно, а не параллельно. Если удастся их все вычислить схемой размера $O(n)$ и глубины $O(\log n)$, то дальнейшее очевидно.

Как мы упоминали, вычисление битов переноса равносильно сравнению, так что для доказательства теоремы достаточно научиться сравнивать параллельно все «суффиксы» двух n-битовых чисел $x_1 \ldots x_n$ и $y_1 \ldots y_n$, т. е. для каждого i сравнить числа $x_i x_{i+1} \ldots x_n$ и $y_i y_{i+1} \ldots y_n$.

Вспомним, что мы делали при сравнении чисел (скажем, длины 8). На нижнем уровне мы сравнивали биты:

$$\begin{matrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ y_1 & y_2 & y_3 & y_4 & y_5 & y_6 & y_7 & y_8 \end{matrix}$$

На следующем уровне мы сравнивали двузначные числа

$$\begin{matrix} x_1x_2 & x_3x_4 & x_5x_6 & x_7x_8 \\ y_1y_2 & y_3y_4 & y_5y_6 & y_7y_8 \end{matrix}$$

затем четырёхзначные

$$\begin{matrix} x_1x_2x_3x_4 & x_5x_6x_7x_8 \\ y_1y_2y_3y_4 & y_5y_6y_7y_8 \end{matrix}$$

и, наконец, восьмизначные:

$$\begin{matrix} x_1x_2x_3x_4x_5x_6x_7x_8 \\ y_1y_2y_3y_4y_5y_6y_7y_8 \end{matrix}$$

Таким образом, для суффиксов длины 8, 4, 2 и 1 результаты сравнения уже есть. Для суффикса длины 6 результат можно получить, комбинируя результат сравнения

$x_3x_4?y_3y_4$ и $x_5x_6x_7x_8?y_5y_6y_7y_8$. После этого у нас есть информация о суффиксах всех чётных длин, и соединяя её с информацией с первого этапа, получаем сведения про все суффиксы. Например, для сравнения суффиксов длины 7, то есть $x_2 \ldots x_8$ и $y_2 \ldots y_8$, мы соединяем результаты сравнения x_2 и y_2 с результатами сравнения суффиксов длины 6, то есть $x_3 \ldots x_8$ и $y_3 \ldots y_8$.

В общем случае картина такая: после «сужающегося дерева» мы строим «расширяющееся»; за k шагов до конца мы знаем результаты сравнения всех суффиксов, длины которых кратны 2^k. Это дерево имеет размер $O(n)$ и глубину $O(\log n)$, что завершает доказательство. $\triangleright$

14. Покажите, что вычитание двух n-битовых чисел по модулю 2^n выполняется схемой размера $O(n)$ и глубины $O(\log n)$. (Указание: вычитание легко сводится к сложению, если заменить нули на единицы и наоборот.)

Теперь займёмся умножением. Схема умножения двух n-разрядных чисел имеет $2n$ входов (по n для каждого множителя) и $2n$ выходов для произведения.

Посмотрим, какие оценки даёт обычный способ умножения чисел столбиком. В нём умножение двух n-разрядных чисел сводится к сложению n копий первого числа (частично заменённых на нули в зависимости от цифр второго числа) со сдвигами.

Получение этих копий требует схемы размера $O(n^2)$ (общее число цифр в копиях) и глубины $O(1)$. Сложение двух $2n$-разрядных чисел мы можем выполнить с помощью схемы размера $O(n)$ и глубины $O(\log n)$, так что необходимые $n-1$ сложений можно выполнить схемой размера $O(n^2)$ и глубины $O(\log^2 n)$ (если складывать сначала попарно, потом результаты снова попарно и т. д.). Оказывается, этот результат можно улучшить. Наиболее экономные способы основаны на преобразовании Фурье (о них можно прочесть в книге [1]). С их помощью, например, можно построить схему умножения n-битовых чисел, имеющую размер $n \log^c n$.

Эти методы далеко выходят за рамки нашего обсуждения, но два улучшения мы приведём.

Теорема 12. Существует схема умножения двух n-разрядных чисел размера $O(n^2)$ и глубины $O(\log n)$.

$\lhd$ Как мы уже говорили, умножение двух n-разрядных чисел сводится к сложению n таких чисел, и остаётся выполнить такое сложение схемой размера $O(n^2)$ и глубины $O(\log n)$. Ключевым моментом здесь является сведение сложения трёх чисел к сложению двух с помощью простой схемы размера $O(n)$ и глубины $O(1)$. В самом деле, пусть есть три числа x, y и z. Если мы будем складывать отдельно в каждом разряде, то в разряде может накопиться любая сумма от 0 до 3, то есть в двоичной записи от 00 до 11. Сформируем из младших битов этих двухбитовых сумм число u, а из старших (сдвинутых влево) — число v. Тогда, очевидно, $x + y + z = u + v$. Получение цифр числа u и v происходит параллельно во всех разрядах и требует размера $O(n)$ и глубины $O(1)$.

Теперь, если надо сложить n чисел, можно разбить их на тройки и из каждых трёх чисел получить по два. В следующий круг, таким образом, выйдут $(2/3)n$ чисел (примерно — граничные эффекты большой роли не играют). Их снова можно сгруппировать по тройкам и т. д. С каждым уровнем число слагаемых убывает в полтора раза, так что глубина схемы будет логарифмической. Каждое преобразование трёх слагаемых в два требует схемы размера $O(n)$ и уменьшает число слагаемых на единицу, так что потребуется n таких преобразований. Итак, эта конструкция имеет общий размер $O(n^2)$ и глубину $O(\log n)$. Надо только отметить, что в конце у нас получается не одно число, а два, и их напоследок надо сложить — что мы умеем делать с глубиной $O(\log n)$ и размером $O(n)$. $\rhd$

15. Докажите, что схема, вычисляющая булеву функцию f от n аргументов, у которой ни один аргумент не является фиктивным, имеет размер не менее cn и глубину не менее $c \log n$, где $c > 0$ — некоторая константа, зависящая от выбранного набора элементов. (Аргумент функции называют *фиктивным*, если от него значение функции не зависит.)

Эта задача показывает, что если в процессе умножения двух n-разрядных чисел мы суммируем n слагаемых размера n, то оценки $O(n^2)$ для размера и $O(\log n)$ для глубины, полученные при доказательстве теоремы 12, существенно улучшить нельзя.

Однако никто не обязывает нас следовать традиционному способу умножения столбиком — отказавшись от него, мы можем уменьшить размер схемы.

Теорема 13. Существует схема умножения двух n-разрядных чисел размера $O(n^{\log_2 3})$ и глубины $O(\log^2 n)$.

$\lhd$ Начнём с такого замечания. Вычисляя произведение двух комплексных чисел

$$(a+bi)(c+di) = (ac-bd) + (ad+bc)i$$

обычным способом, мы делаем четыре умножения. Но можно обойтись и тремя с помощью такого трюка: вычислить ac, bd и $(a+b)(c+d)$, а потом найти $ad+bc$ как разность $(a+b)(c+d)-ac-bd$.

Аналогичный фокус можно проделать и для целых чисел. Разобьём $2n$-битовое число на две n-битовые части, то есть представим его в виде $a2^n+b$. Теперь запишем произведение двух таких чисел:

$$(a2^n+b)(c2^n+d) = ac2^{2n} + (ad+bc)2^n + bd.$$

Теперь видно, что достаточно найти три произведения ac, bd и $(a+b)(c+d)$, чтобы определить все три слагаемых в правой части равенства. Получается, что умножение двух $2n$-разрядных чисел сводится к трём умножениям n-разрядных и к нескольким сложениям и вычитаниям. (На самом деле при умножении $(a+b)$ на $(c+d)$ сомножители могут быть $(n+1)$-разрядными, но это не страшно, так как обработка лишнего разряда сводится к нескольким сложениям.)

Для размера схемы, таким образом, получается рекурсивная оценка

$$S(2n) \leqslant 3S(n) + O(n),$$

из которой следует, что $S(n) = O(n^{\log_2 3})$. В самом деле, для умножения n-разрядных чисел требуется дерево рекурсивных вызовов глубины $\log_2 n$ и степени ветвления 3. Заметим, что размер схемы в вершине пропорционален числу складываемых битов. При переходе от одного уровня к следующему (более близкому к корню) размер слагаемых растёт вдвое, а число вершин уменьшается втрое, поэтому общее число элементов на этом уровне уменьшается в полтора раза. Таким образом, при движении по уровням от листьев к корню получается убывающая геометрическая прогрессия со знаменателем $2/3$, сумма которой всего лишь втрое превосходит её первый член. Остаётся заметить, что число листьев равно $3^{\log_2 n} = n^{\log_2 3}$.

Оценка глубины также очевидна: на каждом уровне мы имеем схему сложения глубины $O(\log n)$, а число уровней есть $O(\log n)$. $\triangleright$

На этом мы завершаем знакомство со схемами из функциональных элементов, выполняющими арифметические операции. О них можно прочесть в главе 29 учебника Кормена, Лейзерсона и Ривеста [18] и в книге Ахо, Хопкрофта и Ульмана [1].

Рассмотрим теперь функцию «голосования» (majority). Она имеет нечётное число аргументов, и значение её равно 0 или 1 в зависимости от того, какое из двух значений чаще встречается среди входов.

Теорема 14. Существует схема размера $O(n)$ и глубины $O(\log n \log\log n)$, вычисляющая функцию голосования.

$\triangleleft$ На самом деле можно даже вычислить общее число единиц среди входов. Это делается рекурсивно: считаем отдельно для каждой половины, потом складываем. Получается логарифмическое число уровней. На верхнем уровне надо складывать числа размера $\log n$, на следующем — размера $(\log n - 1)$ и так до самого низа, где складываются однобитовые числа (то есть биты входа). Какой средний размер складываемых чисел? Половина вершин в дереве приходится на нижний уровень (числа длины 1), четверть — на следующий (числа длины 2) и т. д. Вспоминая, что ряд $\sum(k/2^k)$ сходится, видим, что средний размер складываемых чисел есть $O(1)$ и общий размер схемы есть $O(n)$. А общая глубина есть $O(\log n \log\log n)$, так как на каждом из $\log n$ уровней стоит схема глубины $O(\log\log n)$. $\triangleright$

Заметим, что хотя функция голосования конотонна, построенная схема её вычисления содержит немонотонные элементы (поскольку операция сложения не монотонна). Мы уже говорили, что всякую монотонную функцию можно составить из конъюнкций и дизъюнкций. Для функции голосования есть очевидный способ это сделать: написать дизъюнкцию всех конъюнкций размера $(n+1)/2$ (напомним, что число входов n предполагается нечётным). Однако при этом получится схема экспоненциального по n размера.

Теорема 15. Существует схема размера $O(n^c)$ и глубины $O(\log n)$, составленная только из элементов И и ИЛИ (с двумя входами), вычисляющая функцию голосования.

$\triangleleft$ Для начала заметим, что ограничение на размер является следствием ограничения на глубину, так как элементы И и ИЛИ имеют только два входа и число элементов в схеме глубины d есть $O(2^d)$.

Схема будет строиться из элементов большинства с тремя входами. (Каждый из них можно собрать из конъюнкций и дизъюнкций по формуле $(a\wedge b)\vee(a\wedge c)\vee(b\wedge c)$.) Выход схемы будет большинством из трёх значений, каждое из которых есть большинство из трёх значений и т. д. (рис. 3).

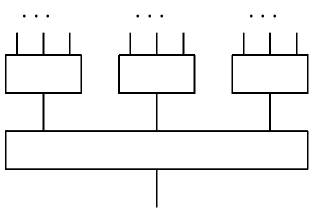


Рис. 3. Дерево из элементов 3-большинства.

Продолжая эту конструкцию на k уровнях, мы получим схему с 3^k входами. (Отметим, что эта схема не будет вычислять большинство среди своих входов — по той же причине, по которой результат непрямого голосования может отличаться от мнения большинства.) Но мы сделаем вот какую странную вещь: возьмём k равным $c \log n$ при достаточно большом коэффициенте пропорциональности c (при этом число входов такой схемы будет полиномиально зависеть от n) и напишем на входах случайно выбранные переменные из данного нам набора $x_1, \ldots, x_n$. (Переменные, записываемые на разных входах, выбираются независимо.) Оказывается, что с ненулевой вероятностью эта схема будет вычислять функцию большинства среди $x_1, \ldots, x_n$, если константа c достаточно велика. Следовательно, искомая схема существует.

Обратите внимание: нам удастся доказать существование интересующей нас схемы, не предъявив её явно. (Такое использование вероятностных методов в комбинаторных рассуждениях часто бывает полезно.)

Итак, почему же схема с положительной вероятностью вычисляет функцию большинства? Это доказывается так: рассмотрим какой-то один набор значений на входах и докажем, что на этом конкретном наборе случайная схема выдаёт правильный ответ с вероятностью, очень близкой к единице (равной $1-\varepsilon$ при очень малом ε).

Если число ε настолько мало, что остаётся меньшим единицы даже после умножения на число возможных входов (2^n), то получаем требуемое (каждое из 2^n событий имеет вероятность не меньше $1-\varepsilon$, значит их пересечение имеет вероятность не меньше $1 - 2^n\varepsilon > 0$).

Итак, осталось оценить вероятность того, что случайная схема даст правильный ответ на данном входе. Пусть доля единиц среди всех входов равна p. Тогда на каждый входной провод схемы подаётся единица с вероятностью p и нуль с вероятностью $1-p$ (выбор случайной переменной даёт единицу с вероятностью p), причём сигналы на всех входах независимы.

Если на трёх входах элемента 3-большинства сигналы независимы, и вероятность появления единицы на каждом входе есть p, то вероятность появления единицы на выходе есть $\varphi(p) = 3p^2(1-p) + p^3 = 3p^2 - 2p^3$. На следующих уровнях вероятность появления единицы будет равна $\varphi(\varphi(p)), \varphi(\varphi(\varphi(p))), \ldots$ График функции $\varphi(x)$ на отрезке $[0,1]$ (рис. 4) показывает, что при итерациях функции φ дисбаланс (отклонение от середины) нарастает и последовательность стремится к краю отрезка. Надо только оценить число шагов.

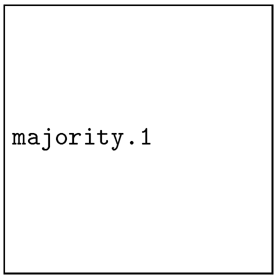


Рис. 4. Итерируемая функция φ.

Если вначале единицы составляют большинство из n аргументов (напомним, n нечётно), то их как минимум $(n+1)/2$, так что $p \geqslant (n+1)/2n = 1/2 + 1/(2n)$. Таким образом, начальный дисбаланс составляет как минимум $1/2n$. А в конце нам нужно приблизиться к краю отрезка на расстояние 2^{-n}.

Итак, нам осталось доказать такую лемму (относящуюся скорее к математическому анализу):

Лемма. Пусть последовательность $x_k \in [0,1]$ задана рекуррентной формулой $x_{k+1} = \varphi(x_k)$, где

$$\varphi(x) = 3x^2 - 2x^3.$$

Пусть $x_0 \geqslant 1/2 + 1/(2n)$. Тогда последовательность x_k монотонно возрастает и приближается к 1 на расстояние 2^{-n} за $O(\log n)$ шагов. [Симметричное утверждение верно и при $x_0 \leqslant 1/2 - 1/(2n)$.]

Идея доказательства: посмотрим на функцию вблизи точки $1/2$ и у краёв отрезка. В точке $1/2$ производная больше 1, поэтому удаление от $1/2$ растёт как геометрическая прогрессия, и точка перейдёт какую-то фиксированную границу (например, 0,51) не позднее чем за $O(\log n)$ шагов. Затем потребуется $O(1)$ шагов, чтобы дойти, скажем, до 0,99. В единице первая производная функции равна нулю, поэтому расстояние до единицы каждый раз примерно возводится в квадрат, и потому для достижения погрешности 2^{-n} потребуется $O(\log n)$ шагов (как в методе Ньютона отыскания корня). Всего получается $O(\log n) + O(1) + O(\log n)$ шагов, что и требовалось. $\triangleright$

На самом деле справедливо гораздо более сильное утверждение: существует схема размера $O(n \log n)$ и глубины $O(\log n)$, состоящая только из элементов И и ИЛИ, которая имеет n входов и n выходов и осуществляет сортировку последовательности n нулей и единиц (это означает, что на выходе столько же единиц, сколько на входе, причём выходная последовательность всегда невозрастающая). Ясно, что средний бит выхода в такой ситуации реализует функцию большинства.

При кажущейся простоте формулировки единственная известная конструкция такой схемы (сортирующая сеть AKS, придуманная Айтаи, Комлошом и Сцемереди сравнительно недавно, в 1983 году) весьма сложна, и появление какой-то более простой конструкции было бы замечательным достижением.

Многие нетривиальные результаты теории алгоритмов можно переформулировать в терминах сложности каких-то булевых функций. Например, есть вероятностный алгоритм проверки простоты большого числа (применяемый в системах шифрования для проверки простоты чисел из нескольких тысяч цифр). Используя этот алгоритм, можно доказать такой факт: существует схема проверки простоты n-битового числа (на вход подаются n цифр, на выходе появляется единица, если число простое, и нуль, если число составное), размер которой ограничен полиномом от n.

Вернёмся к общим утверждениям о схемах и формулах. Мы уже говорили, что с точки зрения измерения размера схемы и формулы — это разные вещи (схемы экономичнее, так как в них одинаковые подформулы учитываются только один раз). Оказывается, что размер формулы можно связать с глубиной схемы.

Будем называть *размером* формулы число логических связок в ней. Мы предполагаем, что формула использует конъюнкции, дизъюнкции и отрицания, и в схемах будем использовать такие же элементы. Напомним, что размером схемы мы называли число элементов, а сложностью булевой функции — минимальный размер схемы, её вычисляющей. Сложность функции h обозначалась $\mathrm{size}(h)$ (точнее $\mathrm{size}_B(h)$, где B — набор разрешённых функциональных элементов, но сейчас мы договорились использовать конъюнкции, дизъюнкции и отрицания и опускаем индекс B).

Минимальный размер формулы, выражающей функцию h, будем обозначать $\mathrm{fsize}(h)$. Очевидно, $\mathrm{size}(h) \leqslant \mathrm{fsize}(h)$. Более интересно, однако, следующее утверждение, связывающее размер схемы с глубиной формулы. Обозначим через $\mathrm{depth}(h)$ минимальную глубину схемы, вычисляющей функцию h.

Теорема 16. Имеют место оценки $\mathrm{fsize}(h) \leqslant c_1^{\mathrm{depth}(h)}$ и $\mathrm{depth}(h) \leqslant c_2 \log \mathrm{fsize}(h)$ (для некоторых констант c_1 и c_2 и для всех h). Другими словами, меры сложности depth и $\log \mathrm{fsize}$ отличаются не более чем в константу раз.

$\triangleleft$ Первая оценка очевидна: если мы скопируем повторяющиеся фрагменты схемы, чтобы развернуть её в дерево, то глубина не изменится. Если она равна k, то в полученном дереве будет не больше 2^k-1 элементов и соответствующая формула имеет размер не более 2^k-1. (Напомним, что элементами являются конъюнкции, дизъюнкции и отрицания, и потому ветвление не больше 2.)

То же самое можно сказать индуктивно. Пусть глубина схемы равна k. Выход схемы является выходом некоторого элемента. Тогда на его входы подаются булевы функции глубины не больше $k-1$. По предположению индукции их можно записать формулами размера $2^{k-1}-1$. Таких формул максимум две, так что общий размер не превосходит $2(2^{k-1}-1)+1=2^k-1$.

Вторая оценка сложнее. Если мы будем преобразовывать формулу в схему естественным образом (введя вспомогательную переменную для каждой подформулы), то глубина получившейся схемы может быть близка к размеру формулы, а не к его логарифму. Например, если формула имеет вид $(\ldots((p_1 \land p_2) \land p_3) \land \ldots p_n)$, то у нас получится цепочка элементов И, у которых каждый следующий подвешен к левому входу предыдущего, и глубина равна $n-1$. Конечно, если использовать ассоциативность конъюнкции, скобки можно переставить и получить более сбалансированное дерево глубины примерно $\log n$, как и требуется. Но как выполнить такое преобразование в случае произвольной формулы?

Обозначим данную нам формулу через F. Выберем у неё некоторую подформулу G (как именно, мы объясним позже). Рассмотрим формулу F_0, которая получится, если вместо G подставить 0 (ложь), а также формулу F_1, которая получится, если подставить 1. Легко понять, что F равносильна формуле

$$((F_0 \land \neg G) \lor (F_1 \land G)).$$

Если теперь удастся заменить формулы F_0, F_1, G схемами глубины не больше k, то для F получится схема глубины не больше $k+3$.

Такое преобразование полезно, если все три формулы F_1, F_0, G имеют заметно меньший размер, чем исходная формула F.

Лемма. У любой формулы размера n (при достаточно больших n) есть подформула размера от $n/4$ до $3n/4$.

Доказательство. Каждая формула есть конъюнкция двух подформул, дизъюнкция двух подформул или отрицание подформулы. Начав со всей формулы, будем переходить к её подформулам, на каждом шаге выбирая из двух подформул наибольшую. Тогда на каждом шаге размер убывает не более чем в два раза, и потому мы не можем миновать промежуток $[n/4, 3n/4]$, концы которого отличаются втрое. (На самом деле тут есть небольшая неточность: размер формулы может убывать чуть быстрее, чем вдвое, так как размер формулы на единицу больше суммы размеров частей, но у нас есть запас, поскольку концы промежутка отличаются втрое, а не вдвое.) Лемма доказана.

Выбирая подформулу G с помощью этой леммы, мы гарантируем, что размер всех трёх формул F_0, F_1, G не превосходит $3/4$ размера исходной формулы (подстановка нуля или единицы может только уменьшить размер формулы — некоторые части можно будет выбросить).

Применим ко всем трём формулам F_0, F_1 и G тот же приём, выделим в них подформулы среднего размера и так далее, пока мы не спустимся до формул малого размера, которые можно записать в виде схем как угодно. В итоге получится дерево с логарифмическим числом уровней, на каждом из которых стоят схемы глубины 3, а в листьях находятся схемы глубины $O(1)$.

Другими словами, индукцией по размеру формулы, выражающей некоторую функцию h, легко получить оценку $\operatorname{depth}(h) = O(\log \operatorname{fsize}(h))$. $\triangleright$

16. Определим глубину формулы как максимальное число вложенных пар скобок; для единообразия будем окружать отрицание скобками и писать $(\neg A)$ вместо $\neg A$. Покажите, что при этом не получится ничего нового: минимальная глубина формулы, записывающей некоторую функцию f, совпадает с минимальной глубиной схемы, вычисляющей f.

Определение формульной сложности $\operatorname{fsize}(h)$ зависит от выбора базиса. Оказывается, что здесь (в отличие от схемной сложности) выбор базиса может изменить $\operatorname{fsize}(h)$ более чем в константу раз.

17. Объясните, почему доказательство теоремы 7 не переносится на случай формул.

Так происходит с функцией $p_1 \oplus p_2 \oplus \ldots \oplus p_n$ (знак $\oplus$ обозначает сложение по модулю 2). Эта функция имеет формульную сложность $O(n)$, если сложение по модулю 2 входит в базис. Однако в базисе И, ИЛИ, НЕ она имеет большую сложность, как доказала Б. А. Субботовская. Идея доказательства такова: если заменить случайно выбранную переменную в формуле с конъюнкциями и дизъюнкциями на случайно выбранное значение 0 или 1, то формула упростится (не только эта переменная пропадёт, но с некоторой вероятностью пропадут и другие). Если делать так многократно, то от формулы останется небольшая часть — с другой стороны, эта часть всё равно должна реализовывать сложение оставшихся аргументов по модулю 2.

18. Докажите, что функция большинства может быть вычислена не только схемой, но и формулой полиномиального размера, содержащей только связки И и ИЛИ.

19. Докажите, что значения $\mathrm{fsize}_1(h)$ и $\mathrm{fsize}_2(h)$ для одной булевой функции h и различных полных базисов полиномиально связаны: существует полином P (зависящий от выбора базисов), для которого $\mathrm{fsize}_2(h) \leqslant P(\mathrm{fsize}_1(h))$ при всех h. (Указание: использовать теорему 16.)

2. Исчисление высказываний

Напомним, что тавтологией мы называли пропозициональную формулу, истинную при всех значениях переменных. Оказывается, что все тавтологии можно получить из некоторого набора «аксиом» с помощью «правил вывода», которые имеют чисто синтаксический характер и никак не апеллируют к смыслу формулы, её истинности и т. д. Эту задачу решает так называемое *исчисление высказываний*. В этой главе мы перечислим аксиомы и правила вывода этого исчисления, и приведём несколько доказательств *теоремы о полноте* (которая утверждает, что всякая тавтология выводима в исчислении высказываний).

2.1. Исчисление высказываний (ИВ)

Каковы бы ни были формулы A, B, C, следующие формулы называют *аксиомами исчисления высказываний*:

(1) $A \to (B \to A)$;
(2) $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$;
(3) $(A \land B) \to A$;
(4) $(A \land B) \to B$;
(5) $A \to (B \to (A \land B))$;
(6) $A \to (A \lor B)$;
(7) $B \to (A \lor B)$;
(8) $(A \to C) \to ((B \to C) \to (A \lor B \to C))$;
(9) $\neg A \to (A \to B)$;
(10) $(A \to B) \to ((A \to \neg B) \to \neg A)$;
(11) $A \lor \neg A$.

Как говорят, мы имеем здесь одиннадцать «схем аксиом»; из каждой схемы можно получить различные конкретные аксиомы, заменяя входящие в неё буквы на пропозициональные формулы.

Единственным правилом вывода исчисления высказываний является правило со средневековым названием «modus ponens» (MP). Это правило разрешает получить (вывести) из формул A и $(A \to B)$ формулу B.

Выводом в исчислении высказываний называется конечная последовательность формул, каждая из которых есть аксиома или получается из предыдущих по правилу modus ponens.

Вот пример вывода (в нём первая формула является частным случаем схемы (1), вторая — схемы (2), а последняя получается из двух предыдущих по правилу modus ponens):

$$(p \to (q \to p)),$$
$$(p \to (q \to p)) \to ((p \to q) \to (p \to p)),$$
$$((p \to q) \to (p \to p)).$$

Пропозициональная формула A называется *выводимой* в исчислении высказываний, или *теоремой* исчисления высказываний, если существует вывод, в котором последняя формула равна A. Такой вывод называют выводом формулы A. (В принципе можно было бы и не требовать, чтобы формула A была последней — все дальнейшие формулы можно просто вычеркнуть.)

Как мы уже говорили, в исчислении высказываний выводятся все тавтологии и только они. Обычно это утверждение разбивают на две части: простую и сложную. Начнём с простой:

Теорема 17 (о корректности ИВ). Всякая теорема исчисления высказываний есть тавтология.

$\lhd$ Несложно проверить, что все аксиомы — тавтологии. Для примера проделаем это для самой длинной аксиомы (точнее, схемы аксиом) — для второй. В каком случае формула

$$(A \to (B \to C)) \to ((A \to B) \to (A \to C))$$

(где A, B, C — некоторые формулы) могла бы быть ложной? Для этого посылка $A \to (B \to C)$ должна быть истинной, а заключение $(A \to B) \to (A \to C)$ — ложным. Чтобы заключение было ложным, формула $A \to B$ должна быть истинной, а формула $A \to C$ — ложной. Последнее означает, что A истинна, а C ложна. Таким образом, мы знаем, что A, $(A \to B)$ и $(A \to (B \to C))$ истинны. Отсюда следует, что B и $(B \to C)$ истинны, и потому C истинна — противоречие. Значит, наша формула не бывает ложной.

Корректность правила MP также очевидна: если формулы $(A \to B)$ и A всегда истинны, то по определению импликации формула B также всегда истинна. Таким образом, все формулы, входящие в выводы (все теоремы) являются тавтологиями. $\triangleright$

Гораздо сложнее доказать обратное утверждение.

Теорема 18 (о полноте ИВ). Всякая тавтология есть теорема исчисления высказываний.

$\triangleleft$ Мы предложим несколько альтернативных доказательств этой теоремы. Но прежде всего мы должны приобрести некоторый опыт построения выводов и использования аксиом.

Лемма 1. Какова бы ни была формула D, формула $(D \to D)$ является теоремой.

Докажем лемму, предъявив вывод формулы $(D \to D)$ в исчислении высказываний.

1. $(D \to ((D \to D) \to D)) \to$
   $\to ((D \to (D \to D)) \to (D \to D))$
   [аксиома 2 при $A = D$, $B = (D \to D)$, $C = D$];
2. $D \to ((D \to D) \to D)$ [аксиома 1];
3. $(D \to (D \to D)) \to (D \to D)$ [из 1 и 2 по правилу MP];
4. $D \to (D \to D)$ [аксиома 1];
5. $(D \to D)$ [из 3 и 4 по правилу MP].

Как видно, вывод даже такой простой тавтологии, как $(D \to D)$, требует некоторой изобретательности. Мы облегчим себе жизнь, доказав некоторое общее утверждение о выводимости.

Часто мы рассуждаем так: предполагаем, что выполнено какое-то утверждение A, и выводим различные следствия. После того как другое утверждение B доказано, мы вспоминаем, что использовали предположение A, и заключаем, что мы доказали утверждение $A \to B$. Следующая лемма, называемая иногда «леммой о дедукции», показывает, что этот подход правомерен и для исчисления высказываний.

Пусть Γ — некоторое множество формул. *Выводом из* Γ называется конечная последовательность формул, каждая из которых является аксиомой, принадлежит Γ или получается из предыдущих по правилу МР. (Другими словами, мы как бы добавляем формулы из Γ к аксиомам исчисления высказываний — именно как формулы, а не как схемы аксиом.) Формула A *выводима из* Γ, если существует вывод из Γ, в котором она является последней формулой. В этом случае мы пишем $\Gamma \vdash A$. Если Γ пусто, то речь идёт о выводимости в исчислении высказываний, и вместо $\varnothing \vdash A$ пишут просто $\vdash A$.

Лемма 2 (о дедукции). Пусть Γ — множество формул. Тогда $\Gamma \vdash A \to B$ тогда и только тогда, когда $\Gamma \cup \{A\} \vdash B$.

В одну сторону утверждение почти очевидно: пусть $\Gamma \vdash (A \to B)$. Тогда и $\Gamma, A \vdash (A \to B)$. (Для краткости мы опускаем фигурные скобки и заменяем знак объединения запятой.) По определению $\Gamma, A \vdash A$, откуда по МР получаем $\Gamma, A \vdash B$.

Пусть теперь $\Gamma, A \vdash B$. Нам надо построить вывод формулы $A \to B$ из Γ. Возьмём вывод $C_1, C_2, \ldots, C_n$ формулы $B = C_n$ из Γ, A. Припишем ко всем формулам этого вывода слева посылку A:

$$(A \to C_1), (A \to C_2), \ldots, (A \to C_n).$$

Эта последовательность оканчивается на $(A \to B)$. Сама по себе она не будет выводом из Γ, но из неё можно получить такой вывод, добавив недостающие формулы, и тем самым доказать лемму о дедукции.

Будем добавлять эти формулы, двигаясь слева направо. Пусть мы подошли к формуле $(A \to C_i)$. По предположению формула C_i либо совпадает с A, либо принадлежит Γ, либо является аксиомой, либо получается из двух предыдущих по правилу МР. Рассмотрим все эти случаи по очереди.

(1) Если C_i есть A, то очередная формула имеет вид

$(A \to A)$. По лемме 1 она выводима, так что перед ней мы добавляем её вывод.

(2) Пусть C_i принадлежит Γ. Тогда мы вставляем формулы C_i и $C_i \to (A \to C_i)$ (аксиома 1). Применение правила MP к этим формулам даёт $(A \to C_i)$, что и требовалось.

(3) Те же формулы можно добавить, если C_i является аксиомой исчисления высказываний.

(4) Пусть, наконец, формула C_i получается из двух предыдущих формул по правилу MP. Это значит, что в исходном выводе ей предшествовали формулы C_j и $(C_j \to C_i)$. Тогда в новой последовательности (с добавленной посылкой A) уже были формулы $(A \to C_j)$ и $(A \to (C_j \to C_i))$. Поэтому мы можем продолжить наш Γ-вывод, написав формулы

$((A \to (C_j \to C_i)) \to ((A \to C_j) \to (A \to C_i))$ (аксиома 2);
$((A \to C_j) \to (A \to C_i))$ (modus ponens);
$(A \to C_i)$ (modus ponens).

Итак, во всех четырёх случаях мы научились дополнять последовательность до вывода из Γ, так что лемма о дедукции доказана.

20. Докажите, что для любых формул A, B, C формула

$$(A \to B) \to ((B \to C) \to (A \to C))$$

выводима в исчислении высказываний. (Указание: используйте лемму о дедукции и тот факт, что $A \to B, B \to C, A \vdash C$.)

21. Докажите, что если $\Gamma_1 \vdash A$ и $\Gamma_2, A \vdash B$, то $\Gamma_1 \cup \cup \Gamma_2 \vdash B$. (Это свойство иногда называют «правилом сечения» (cut); говорят, что формула A «отсекается» или «высекается». Сходные правила играют центральную роль в теории доказательств, где формулируется и доказывается «теорема об устранении сечения» для различных логических систем.)

22. Добавим к исчислению высказываний, помимо правила modus ponens, ещё одно правило, называемое *правилом подстановки*. Оно разрешает заменить в выведенной формуле все переменные на произвольные формулы (естественно, вхождения одной переменной должны заменяться на одну и ту же формулу). Покажите, что после добавления такого правила класс выводимых формул не изменится, но теорема о дедукции перестанет быть верной.

Заметим, что мы пока что использовали только две первые аксиомы исчисления высказываний. Видно, кстати, что они специально подобраны так, чтобы доказательство леммы о дедукции прошло.

Другие аксиомы описывают свойства логических связок. Аксиомы 3 и 4 говорят, какие следствия можно вывести из конъюнкции ($A \wedge B \vdash A$ и $A \wedge B \vdash B$). Напротив, аксиома 5 говорит, как можно вывести конъюнкцию. Из неё легко следует такое правило: если $\Gamma \vdash A$ и $\Gamma \vdash B$, то $\Gamma \vdash (A \wedge B)$ (применяем эту аксиому и дважды правило MP). Часто подобные правила записывают так:

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$$

(над чертой пишут «посылки» правила, а снизу — его «заключение», вытекающее из посылок).

23. Докажите, что формула $(A \to (B \to C)) \to ((A \wedge B) \to \to C)$, так же как и обратная к ней формула (в которой посылка и заключение переставлены), являются теоремами исчисления высказываний. Докажите аналогичное утверждение про формулы $(A \wedge B) \to (B \wedge A)$ и $((A \wedge B) \wedge C) \to (A \wedge (B \wedge C))$.

Аксиомы 6–7 позволяют утверждать, что $A \vdash A \vee B$ и $B \vdash A \vee B$. Аксиома 8 обеспечивает такое правило:

$$\frac{\Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}$$

Оно соответствует такой схеме рассуждения: «Пусть выполнено $A \vee B$. Разберём два случая. Если выполнено A, то $\langle \ldots \rangle$ и потому C. Если выполнено B, то $\langle \ldots \rangle$ и потому C. В обоих случаях верно C. Значит, $A \vee B$ влечёт C.»

Обоснование: дважды воспользуемся леммой о дедукции, получив $\Gamma \vdash (A \to C)$ и $\Gamma \vdash (B \to C)$, а затем дважды применим правило MP к этим формулам и аксиоме $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$. Получив формулу $(A \vee B) \to C$, опять применим правило MP к ней и формуле $(A \vee B)$.

24. Докажите, что следующие формулы, а также обратные к ним (меняем местами посылку и заключение) являются теоремами исчисления высказываний:

$$((A \vee B) \to C) \to ((A \to C) \wedge (B \to C)),$$
$$((A \wedge C) \vee (B \wedge C)) \to ((A \vee B) \wedge C),$$
$$((A \vee C) \wedge (B \vee C)) \to ((A \wedge B) \vee C).$$

У нас остались ещё три аксиомы, касающиеся отрицания. Аксиома 9 гарантирует, что из противоречивого набора посылок можно вывести что угодно: если $\Gamma \vdash A$ и $\Gamma \vdash \neg A$, то $\Gamma \vdash B$ для любого B. Аксиома 10, напротив, объясняет, как можно вывести отрицание некоторой формулы A: надо допустить A и вывести два противоположных заключения B и $\neg B$. Точнее говоря, имеет место такое правило:

$$\frac{\Gamma, A \vdash B \qquad \Gamma, A \vdash \neg B}{\Gamma \vdash \neg A}$$

(в самом деле, дважды применяем лемму о дедукции, а затем правило MP с аксиомой 10).

Аксиомы 9 и 10 позволяют вывести некоторые логические законы, связанные с отрицанием. Докажем, например, что (для любых формул A и B) формула

$$(A \to B) \to (\neg B \to \neg A)$$

(«закон контрапозиции») является теоремой исчисления высказываний. В самом деле, по лемме о дедукции достаточно установить, что

$$(A \to B), \neg B \vdash \neg A.$$

Для этого, в свою очередь, достаточно вывести из посылок $(A \to B), \neg B, A$ какую-либо формулу и её отрицание (в данном случае формулы B и $\neg B$).

25. Выведите формулы $A \to \neg\neg A$ и $\neg\neg\neg A \to \neg A$ с помощью аналогичных рассуждений.

Последняя аксиома, называемая «законом исключённого третьего», и иногда читаемая как «третьего не дано» (tertium non datur в латинском оригинале), вызвала в первой половине века большое количество споров. (См. раздел 2.4 об интуиционистской логике, в которой этой аксиомы нет.)

Из неё можно вывести закон «снятия двойного отрицания», имеющий вид $\neg\neg A \to A$. В самом деле, достаточно показать, что $A \vee \neg A, \neg\neg A \vdash A$. По правилу разбора случаев, достаточно установить, что $A, \neg\neg A \vdash A$ (это очевидно) и что $\neg A, \neg\neg A \vdash A$ (а это верно, так как из двух противоречащих друг другу формул выводится что угодно с помощью аксиомы 8).

26. Докажите, что формула $(\neg B \to \neg A) \to (A \to B)$ является теоремой исчисления высказываний. (Указание: используйте закон исключённого третьего.)

27. Исключим из числа аксиом исчисления высказываний закон исключённого третьего, заменив его на закон снятия двойного отрицания. Покажите, что от этого класс выводимых формул не изменится.

28. Докажите, что при наличии аксиомы исключённого третьего (11) аксиома (10) является лишней — её (точнее следовало бы сказать: любой частный случай этой схемы аксиом) можно вывести из остальных аксиом.

Теперь уже можно доказать теорему о полноте: всякая тавтология выводима в исчислении высказываний. Идея доказательства состоит в разборе случаев. Поясним её на примере. Пусть A — произвольная формула, содержащая переменные p, q, r. Предположим, что A истинна, когда все три переменные истинны. Тогда, как мы докажем,

$$p, q, r \vdash A.$$

Вообще каждой строке таблицы истинности для формулы A соответствует утверждение о выводимости. Например, если A ложна, когда p и q ложны, а r истинно, то

$$\neg p, \neg q, r \vdash \neg A.$$

Если формула A является тавтологией, то окажется, что она выводима из всех восьми возможных вариантов посылок. Пользуясь законом исключённого третьего, можно постепенно избавляться от посылок. Например, из $p, q, r \vdash A$ и $p, q, \neg r \vdash A$ можно получить $p, q, (r \vee \neg r) \vdash A$, то есть $p, q \vdash A$ (поскольку $(r \vee \neg r)$ является аксиомой).

Проведём это рассуждение подробно. Для начала докажем такую лемму:

Лемма 3.

$$
\begin{array}{rcl}
P, Q \vdash (P \wedge Q) & \qquad & P, Q \vdash (P \vee Q) \\
P, \neg Q \vdash \neg(P \wedge Q) & & P, \neg Q \vdash (P \vee Q) \\
\neg P, Q \vdash \neg(P \wedge Q) & & \neg P, Q \vdash (P \vee Q) \\
\neg P, \neg Q \vdash \neg(P \wedge Q) & & \neg P, \neg Q \vdash \neg(P \vee Q)
\end{array}
$$

$$
\begin{array}{rcl}
P, Q \vdash (P \to Q) & \qquad & \\
P, \neg Q \vdash \neg(P \to Q) & & P \vdash \neg(\neg P) \\
\neg P, Q \vdash (P \to Q) & & \neg P \vdash \neg P \\
\neg P, \neg Q \vdash (P \to Q) & &
\end{array}
$$

для произвольных формул P и Q.

Эта лемма говорит, что если принять в качестве гипотез истинность или ложность формул P и Q, являющихся частями конъюнкции, дизъюнкции или импликации, то можно будет доказать или опровергнуть всю формулу (в зависимости от того, истинна она или ложна). Последняя часть содержит аналогичное утверждение про отрицание.

После предпринятой нами тренировки доказать эти утверждения несложно. Например, убедимся, что $\neg P \vdash \neg(P \wedge Q)$. Для этого достаточно вывести два противоположных утверждения из $\neg P, (P \wedge Q)$ — ими будут утверждения P и $\neg P$.

Проверим ещё одно утверждение: $\neg P, \neg Q \vdash \neg(P \vee Q)$. Нам надо вывести два противоположных утверждения из $\neg P, \neg Q, (P \vee Q)$. Покажем, что из $\neg P, \neg Q, (P \vee Q)$ следует всё, что угодно. По правилу разбора случаев достаточно убедиться, что из $\neg P, \neg Q, P$ и из $\neg P, \neg Q, Q$ следует всё, что угодно — но это мы знаем.

Утверждения, касающиеся импликации, просты: в самом деле, мы знаем, что $Q \vdash (P \to Q)$ благодаря аксиоме 1, а $\neg P \vdash (P \to Q)$ благодаря аксиоме 9.

Остальные утверждения леммы столь же просты.

Теперь мы можем сформулировать утверждение о разборе случаев для произвольной формулы.

Лемма 4. Пусть A — произвольная формула, составленная из переменных $p_1, \ldots, p_n$. Тогда для каждой строки таблицы истинности формулы A имеет место соответствующее утверждение о выводимости: если $\varepsilon_1, \ldots, \varepsilon_n, \varepsilon \in \{0, 1\}$, и значение формулы A есть ε при $p_1 = \varepsilon_1, \ldots, p_n = \varepsilon_n$, то

$$\neg_{\varepsilon_1} p_1, \ldots, \neg_{\varepsilon_n} p_n \vdash \neg_{\varepsilon A},$$

где $\neg_u \varphi$ обозначает φ при $u = 1$ и $\neg\varphi$ при $u = 0$ (напомним, что 1 обозначает истину, а 0 — ложь).

Лемма очевидно доказывается индукцией по построению формулы A. Мы имеем посылки, утверждающие истинность или ложность переменных, и для всех подформул (начиная с переменных и идя ко всей формуле) выводим их или их отрицания с помощью леммы 3.

В случае, если формула A оказывается тавтологией, из всех 2^n вариантов посылок выводится именно она, а не её отрицание. Тогда правило разбора случаев и закон исключённого третьего позволяют избавиться от посылок: сгруппируем их в пары, отличающиеся в позиции p_1 (в одном наборе посылок стоит p_1, в другом $\neg p_1$), по правилу разбора случаев заменим их на посылку $(p_1 \vee \neg p_1)$, которую можно выбросить, так как она является аксиомой. Сделав так для вех пар, получим 2^{n-1} выводов, в посылках которых нет p_1, повторим этот процесс с посылками p_2, $\neg p_2$ и т. д. В конце концов мы убедимся, что формула A выводима без всяких посылок, что и составляет утверждение теоремы о полноте. $\triangleright$

2.2. Второе доказательство теоремы о полноте

Это доказательство, в отличие от предыдущего, обобщается на более сложные случаи (исчисление предикатов).

Начнём с такого определения: множество формул Γ называется *совместным*, если существует набор значений переменных, при которых все формулы из Γ истинны. Заметим, что формула φ является тавтологией тогда и только тогда, когда множество, состоящее из единственной формулы $\neg\varphi$, не является совместным. Для случая одной формулы есть специальный термин: формула τ *выполнима*, если существуют значения переменных, при которых она истинна, то есть если множество $\{\tau\}$ совместно. Тавтологии — это формулы, отрицания которых не выполнимы.

Множество формул Γ называется *противоречивым*, если из него одновременно выводятся формулы A и $\neg A$. Мы знаем, что в этом случае из него выводятся вообще все формулы. (В противном случае Γ называется *непротиворечивым*.)

Теорема 19 (корректность исчисления высказываний, вторая форма). Всякое совместное множество формул непротиворечиво.

$\triangleleft$ В самом деле, пусть совместное множество Γ противоречиво. Так как оно совместно, существуют значения переменных, при которых все формулы из Γ истинны. С другой стороны, из Γ выводится некоторая формула B и её отрицание. Может ли так быть?

Оказывается, что нет. Мы уже видели, что всякая выводимая формула истинна при всех значениях переменных (является тавтологией). Справедливо и несколько более общее утверждение: если $\Gamma \vdash A$ и при некоторых значениях переменных все формулы из Γ истинны, то и формула A истинна при этих значениях переменных. (Как и раньше, это легко доказывается индукцией по построению вывода A из Γ.)

В нашей ситуации это приводит к тому, что на выполняющем наборе значений переменных для Γ должны быть истинны обе формулы B и $\neg B$, что, разумеется, невозможно. $\triangleright$

Мы называем это утверждение другой формой теоремы о корректности исчисления высказываний, поскольку из него формально можно вывести, что всякая теорема является тавтологией: если A — теорема, то множество $\{\neg A\}$ противоречиво (из него выводятся A и $\neg A$), потому несовместно, значит, $\neg A$ всегда ложна, поэтому A всегда истинна.

Теорема 20 (полнота исчисления высказываний, вторая форма). Всякое непротиворечивое множество совместно.

$\triangleleft$ Нам дано непротиворечивое множество Γ, а надо найти такие значения переменных, при которых все формулы из Γ истинны. (Вообще говоря, множество Γ может быть бесконечно и содержать бесконечное число разных переменных.)

Пусть есть какая-то переменная p, встречающаяся в формулах из семейства Γ. Нам надо решить, сделать ли её истинной или ложной. Если оказалось так, что из Γ выводится формула p, то выбора нет: она обязана быть истинной в тех наборах, где формулы из Γ истинны (как мы видели при доказательстве корректности). По тем же причинам, если из Γ выводится $\neg p$, то в выполняющем наборе переменная p обязательно будет ложной.

Если оказалось так, что для любой переменной p либо она сама, либо её отрицание выводятся из Γ, то выполняющий набор значений определён однозначно, и надо только проверить, что он действительно будет выполняющим. А если для каких-то переменных нельзя вывести ни их, ни их отрицание, то мы пополним наш набор Γ так, чтобы они, как теперь модно говорить, «определились».

Проведём это рассуждение подробно. Рассмотрим все переменные, входящие в какие-либо формулы из множества Γ; обозначим множество этих переменных через V. Зафиксируем это множество и до конца доказательства теоремы о полноте будем рассматривать только формулы с переменными из множества V, не оговаривая этого особо.

Назовём непротиворечивое множество Γ *полным*, если для любой формулы F имеет место либо $\Gamma \vdash F$, либо $\Gamma \vdash \neg F$ (одновременно этого быть не может, так как Γ непротиворечиво).

Утверждение теоремы о полноте очевидно следует из двух лемм:

Лемма 1. Всякое непротиворечивое множество Γ содержится в непротиворечивом полном множестве Δ.

Лемма 2. Для всякого непротиворечивого полного множества Δ существует набор значений переменных (из V, напомним), при котором все формулы из Δ истинны.

Доказательство леммы 1. Основную роль здесь играет такое утверждение: если Γ — непротиворечивое множество, а A — произвольная формула, то хотя бы одно из множеств $\Gamma \cup \{A\}$ и $\Gamma \cup \{\neg A\}$ непротиворечиво. В самом деле, если оба множества $\Gamma \cup \{A\}$ и $\Gamma \cup \{\neg A\}$ противоречивы, то $\Gamma \vdash \neg A$ и $\Gamma \vdash \neg\neg A$, но множество Γ предполагалось непротиворечивым.

Если множество переменных V конечно или счётно, то доказательство леммы 1 легко завершить: множество всех формул тогда счётно, и просматривая их по очереди, мы можем добавлять к Γ либо саму формулу, либо её отрицание, сохраняя непротиворечивость. Получится, очевидно, полное множество. Чуть менее очевидна его непротиворечивость: оно было непротиворечиво на каждом шаге, но почему предельное множество (объединение возрастающей последовательности) будет непротиворечиво? Дело в том, что в выводе двух противоречащих друг другу формул может быть задействовано только конечное число формул из Γ (по определению выводимости: вывод есть конечная последовательность формул). Поэтому все эти формулы должны появиться на некотором конечном шаге конструкции, а это невозможно (на всех шагах множество непротиворечиво).

Для случая произвольного набора переменных V рассуждение можно завершить ссылкой на лемму Цорна: рассмотрим частично упорядоченное множество, элементами которого будут непротиворечивые множества формул, а порядком — отношение «быть подмножеством». Рассуждение предыдущего абзаца показывает, что всякая цепь в этом множестве имеет верхнюю границу (объединение линейно упорядоченного по включению семейства непротиворечивых множеств является непротиворечивым множеством). Следовательно, для любого непротиворечивого множества найдётся содержащее его максимальное непротиворечивое множество. А оно обязано быть полным (иначе его можно расширить, добавив A или $\neg A$).

Лемма 1 доказана.

Доказательство леммы 2. Пусть Γ — непротиворечивое полное множество. Тогда для каждой переменной (из множества V) ровно одна из формул p и $\neg p$ выводима из Γ. Если первая, будем считать переменную p истинной, если вторая — ложной. Тем самым появляется некоторый набор ν значений переменных, и надо только проверить, что любая формула из Γ при таких значениях переменных истинна. Это делается так: индукцией по построению формулы A мы доказываем, что

$$\begin{aligned} A \text{ истинна на наборе } \nu \ &\Rightarrow\ \Gamma \vdash A,\\ A \text{ ложна на наборе } \nu \ &\Rightarrow\ \Gamma \vdash \neg A. \end{aligned}$$

Базис индукции (когда A — переменная) обеспечивается определением истинности переменных. Для шага индукции используется та же лемма, что и при доказательстве полноты с помощью разбора случаев. Пусть, например, A имеет вид $(B \wedge C)$. Тогда есть четыре возможности для истинности B и C. В одном из них (когда B и C истинны на ν) по предположению индукции мы имеем $\Gamma \vdash B$ и $\Gamma \vdash C$, откуда $\Gamma \vdash (B \wedge C)$, то есть $\Gamma \vdash A$. В другом (B истинна, C ложна) предположение индукции даёт $\Gamma \vdash B$ и $\Gamma \vdash \neg C$, откуда $\Gamma \vdash \neg(B \wedge C)$, то есть $\Gamma \vdash \neg A$.

Аналогично разбираются и все остальные случаи и логические связки. Лемма 2 доказана, и тем самым завершено доказательство теоремы 20. $\triangleright$

Мы доказали, что всякое непротиворечивое множество формул совместно. Отсюда легко следует, что всякая тавтология является теоремой. В самом деле, если φ — тавтология, то множество $\{\neg\varphi\}$ несовместно, поэтому из $\neg\varphi$ выводится противоречие, поэтому $\vdash \neg\neg\varphi$, и по закону снятия двойного отрицания $\vdash \varphi$.

Кроме того, теорема о полноте во второй формулировке имеет такое очевидное следствие:

Теорема 21 (теорема компактности для исчисления высказываний). Пусть Γ — множество формул, всякое конечное подмножество которого совместно. Тогда и всё множество Γ совместно.

$\triangleleft$ Как мы знаем, несовместность равносильна противоречивости, а вывод противоречия по определению может использовать лишь конечное число формул. $\triangleright$

Поскольку в формулировке теоремы компактности нет упоминания об исчислении высказываний (речь идёт лишь об истинности формул, а не о выводимости), возникает вопрос, нельзя ли её доказать непосредственно.

29. Дайте прямое доказательство теоремы компактности для случая, когда переменных в множестве V конечное число. (Указание: в этом случае любое несовместное множество имеет несовместное подмножество мощности не больше $2^{|V|}$.)

Для случая счётного числа переменных можно воспользоваться компактностью (в топологическом смысле слова) канторовского пространства. Его элементами являются бесконечные последовательности нулей и единиц. Если две последовательности отличаются в n-й позиции, а все предыдущие члены совпадают, то расстояние между ними считается равным 2^{-n}. Это метрическое пространство компактно.

Пусть V содержит счётное число переменных. Последовательность значений переменных будем рассматривать как точку канторовского пространства; формуле соответствует область, состоящая из точек, где формула истинна. Поскольку формула содержит лишь конечное число переменных, эта область является замкнутым и открытым множеством одновременно. Пусть имеется множество формул, любое конечное подмножество которого совместно. Это значит, что соответствующие формулам подмножества канторовского пространства образуют, как говорят, центрированную систему (любое конечное их число имеет общую точку). А в компактном пространстве любое центрированное семейство замкнутых множеств имеет общую точку (иначе их дополнения образуют открытое покрытие, у которого нет конечного подпокрытия). Эта их общая точка и будет набором значений, на котором все формулы истинны.

То же самое рассуждение годится и для несчётного множества переменных, но тогда возникает несчётное произведение двухточечных пространств, которое является топологическим пространством (но не метрическим); надо заметить, что это пространство компактно по теореме Тихонова, после чего наше рассуждение проходит.

Для счётного набора переменных теорема компактности связана с так называемой *леммой Кёнига*. Конечные последовательности нулей и единиц (включая пустую последовательность) мы называем двоичными словами. Двоичным деревом мы называем множество двоичных слов, которое вместе со всяким словом содержит все его начала (начальные отрезки). Бесконечной ветвью двоичного дерева T мы называем бесконечную последовательность нулей и единиц, любое конечное начало которой принадлежит T.

Теорема 22 (лемма Кёнига). Любое бесконечное дерево имеет бесконечную ветвь.

$\triangleleft$ Говоря о бесконечности дерева, мы имеем в виду, что соответствующее множество бесконечно. Отсюда следует, что оно содержит слова сколь угодно большой длины. Пусть $p_1, p_2, \ldots$ — счётное множество переменных, которые принимают значения 0 или 1. Для каждого n рассмотрим формулу φ_n, которая утверждает, что слово $p_1 p_2 \ldots p_n$ принадлежит дереву T (это возможно, так как любая булева функция выразима формулой). Поскольку T — дерево, φ_i влечёт φ_j при $j < i$. Любое конечное множество формул вида φ_i равносильно, таким образом, одной формуле с максимальным i и потому совместно. Следовательно, и множество всех формул φ_i совместно, и выполняющий набор определяет бесконечную ветвь. $\triangleright$

(Конечно, мы «бьём из пушек по воробьям»: достаточно индукцией по i строить слово длины i, которое имеет бесконечное число продолжений в дереве T.)

Обычно утверждение леммы Кёнига формулируют так: если колония бактерий, возникшая из одной бактерии, никогда не вымирает полностью, то существует бесконечная последовательность бактерий, каждая следующая из которых получается при делении предыдущей. [Аналогичная формулировка про людей осложняется возможностью клонирования, наличием двух полов и проблемами политкорректности.]

2.3. Поиск контрпримера и исчисление секвенций.

В этом разделе мы построим другой вариант исчисления высказываний — так называемое *исчисление секвенций*. Такого рода исчисления изучаются в теории доказательств. Они оказываются более удобными для анализа синтаксической структуры выводов. Их называют исчислениями генценовского типа (по имени Генцена, который начал их изучать). Ранее приведённый вариант исчисления высказываний называют исчислением гильбертовского типа (по имени Гильберта, который использовал подобные исчисления в своей программе формального построения математики).

Для начала мы вообще не будем говорить ничего об аксиомах и правилах вывода, а рассмотрим задачу поиска контрпримера. Пусть дана некоторая формула A, про которую мы подозреваем, что она не является тавтологией, и хотим найти значения переменных, при которых она ложна. Как это делать? Естественно посмотреть на структуру формулы A. Например, если A имеет вид $B \to C$, то надо найти значения переменных, при которых формула B истинна, а C ложна. Если A имеет вид $B \vee C$, то надо найти значения переменных, при которых обе формулы B и C ложны. Если A имеет вид $B \wedge C$, то надо найти либо значения переменных, при которых B ложна, либо значения переменных, при которых C ложна. Тем самым задача поиска контрпримера для формулы A сводится к одной или нескольким задачам такого же или более общего вида (надо обеспечить истинность или ложность одной или нескольких формул).

Введём необходимую терминологию и обозначения. Будем называть *секвенцией* выражение $\Gamma \vdash \Delta$, где Γ и Δ — некоторые конечные множества формул. (Пока что знак $\vdash$ не имеет ничего общего с выводимостью, а только разделяет два множества формул.) С каждой секвенцией $\Gamma \vdash \Delta$ будем связывать задачу поиска таких значений переменных, при которых все формулы из Γ истинны, а все формулы из Δ ложны. Такой набор значений мы по некоторым причинам будем называть *контрпримером* к секвенции $\Gamma \vdash \Delta$. Легко проверить, что контрпримеры к секвенции $\Gamma \vdash \Delta$ — это контрпримеры к формуле

$$\wedge\Gamma \to \vee\Delta,$$

($\wedge\Gamma$ обозначает конъюнкцию формул из Γ, а $\vee\Delta$ — дизъюнкцию формул из Δ), то есть те наборы значений, при которых эта формула ложна. При этом конъюнкцию пустого множества формул мы считаем тождественно истинной, а дизъюнкцию — тождественно ложной.

Наша исходная задача поиска контрпримера к формуле A может быть теперь сформулирована как задача поиска контрпримера к секвенции $\vdash A$. (Мы позволяем себе писать так для краткости; полностью следовало бы написать $\varnothing \vdash \{A\}$.)

Задачу поиска контрпримера к секвенции можно решать с помощью следующих правил. В каждом из приведенных правил нижний заказ на контрпример выполним, если и только если выполним один из верхних заказов, т. е. нижняя секвенция имеет контрпример тогда и только тогда, когда хотя бы одна из верхних секвенций имеет контрпример.

$$\frac{\Gamma \vdash A, \Delta \qquad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta} \qquad \frac{A, B, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta}$$

$$\frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta} \qquad \frac{A, \Gamma \vdash \Delta \qquad B, \Gamma \vdash \Delta}{A \vee B, \Gamma \vdash \Delta}$$

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta} \qquad \frac{\Gamma \vdash A, \Delta \qquad \Gamma, B \vdash \Delta}{A \to B, \Gamma \vdash \Delta}$$

$$\frac{A, \Gamma \vdash \Delta}{\Gamma \vdash \neg A, \Delta} \qquad \frac{\Gamma \vdash A, \Delta}{\neg A, \Gamma \vdash \Delta}$$

Каждое из правил соответствует анализу одной из формул нижней секвенции. Правила разделены на группы в зависимости от главной связки анализируемой формулы, и согласованы с таблицами истинности для этой связки (что легко проверить). Запятая в правилах используется как сокращение: Γ, A обозначает $\Gamma \cup \{A\}$ и т. д.

Как пользоваться этими правилами? Возьмём секвенцию, к которой мы ищем контрпример. Выберем в ней одну из формул слева или справа, посмотрим на главную связку и применим соответствующее правило (написав одну или две секвенции над исходной). Затем к каждой из них снова применим одно из правил и т. д. Постепенно будет расти «дерево поиска контрпримера», причём исходная секвенция будет иметь контрпример тогда и только тогда, когда одна из верхних секвенций (стоящих в «листьях») этого дерева имеет контрпример.

Когда этот процесс обрывается? Это происходит в том случае, если все формулы в оставшихся секвенциях представляют собой переменные, тогда ни одно из наших правил поиска контрпримера не применимо. Но к этому моменту всё становится ясным: если в левой и правой части секвенции есть общая переменная, то к ней нет контрпримера (одна и та же переменная не может быть одновременно истинной и ложной). Если же левая и правая часть такой секвенции не пересекаются, то контрпример есть.

Вот как это делается с секвенцией $\vdash (p \to q) \to q$:

$$\dfrac{\dfrac{\vdash p, q \qquad q \vdash q}{(p \to q) \vdash q}}{\vdash (p \to q) \to q}$$

Контрпример найден: p и q ложны (он является контрпримером к секвенции $\vdash p, q$).

Напротив, попытка поиска контрпримера к секвенции $\vdash ((p \to q) \to p) \to p$ не даёт результата:

$$\dfrac{\dfrac{\dfrac{p \vdash p, q}{\vdash p, p \to q} \qquad p \vdash p}{(p \to q) \to p \vdash p}}{\vdash ((p \to q) \to p) \to p}$$

Здесь обе секвенции $p \vdash p, q$ и $p \vdash p$ не имеют контрпримеров. Следовательно, формула $((p \to q) \to p) \to p$ является тавтологией.

Построенный алгоритм можно одновременно рассматривать как доказательство полноты некоторого «исчисления секвенций».

Аксиомами исчисления секвенций будем называть секвенции, в левых и правых частях которых встречаются только переменные, причём некоторая переменная встречается в обеих частях.

Правилами вывода в исчислении секвенций являются правила нашей таблицы. Каждое из этих правил объявляет выводимой нижнюю секвенцию, если выводимы все верхние. (Процесс вывода естественно представлять в виде дерева, как в наших примерах, но можно развернуть и в последовательность секвенций.)

Теорема 23 (корректность и полнота исчисления секвенций). Секвенция выводима тогда и только тогда, когда она не имеет контрпримера.

$\lhd$ Аксиомы не имеют контрпримера. Если все верхние секвенции какого-то правила вывода не имеют контрпримера, то и нижняя секвенция не имеет контрпримера. (Именно так мы подбирали правила: контрпример к нижней секвенции будет контрпримером к одной из верхних.) Следовательно, все выводимые секвенции не имеют контрпримера.

Обратно, пусть секвенция не имеет контрпримера. Тогда описанный процесс поиска контрпримера обрывается на аксиомах и тем самым даёт её вывод. $\rhd$

В частности, если формула A является тавтологией, то секвенция $\vdash A$ выводима в исчислении секвенций. Это обстоятельство можно использовать для ещё одного доказательства полноты исчисления высказываний (в стандартной, гильбертовской форме). В самом деле, для каждой секвенции $\Gamma \vdash \Delta$ рассмотрим *представляющую её формулу*, то есть формулу $\wedge\Gamma \to \vee\Delta$ (в левой и правой частях стоят конъюнкция и дизъюнкция формул из Γ и Δ соответственно). Теперь индукцией по построению вывода в исчислении секвенций надо доказать такой факт: если секвенция выводима в исчислении секвенций, то представляющая её формула выводима в (обычном) исчислении высказываний.

Это требует довольно хлопотной проверки, впрочем. Сначала надо проверить, что конъюнкция и дизъюнкция доказуемо ассоциативны, и потому всё равно, как расставлять скобки в формуле, представляющей секвенцию. Затем полезно убедиться, что правила, связанные с отрицанием (два последних правила таблицы) можно применять в обе стороны, не меняя выводимости соответствующей формулы. Другими словами, надо проверить, что формулы

$$\Gamma \to (\Delta \vee A) \quad \text{и} \quad (\Gamma \wedge \neg A) \to \Delta,$$

а также формулы

$$\Gamma \to (\Delta \vee \neg A) \quad \text{и} \quad (\Gamma \wedge A) \to \Delta$$

выводимы одновременно (здесь Γ и Δ можно считать формулами, а не множествами формул, расставив скобки надлежащим образом). После этого мы можем переносить формулы из одной части в другую (меняя их на противоположные), и потому можем считать одно из множеств Γ и Δ пустым, если это нам удобно. Теперь ссылка на лемму о дедукции и уже известные нам свойства выводимости завершает рассуждение.

30. Провести это рассуждение подробно.

Естественно возникает вопрос — чем уж так интересно исчисление секвенций? Какая, собственно говоря, разница — иметь дело с секвенциями или с формулами, раз всякую секвенцию можно представить формулой? Принципиальное различие тут в следующем. Правила вывода в исчислении секвенций таковы, что в их верхнюю часть входят только подформулы формул, встречающихся в нижней части. Поэтому в выводе какой-то секвенции не может встретиться ничего принципиально нового, чего не было в самой секвенции. В гильбертовском исчислении это далеко не так: мы можем вывести формулу B из формул $A \to B$ и A, при этом формула A может быть совершенно произвольной. Это же различие объясняет, почему поиск вывода снизу вверх (как можно теперь называть то, что раньше называлось поиском контрпримера — мы находим либо контрпример, либо вывод) для исчисления секвенций происходит сравнительно однозначно (мы можем по-разному выбирать расчленяемую формулу, но и только), в то время как искать вывод в обычном исчислении высказываний, начав с интересующей нас формулы B и смотря, из чего бы она могла получиться, не удаётся (если только не перебирать все формулы подряд).

Заметим, что добавление к исчислению секвенций уже упоминавшегося правила сечения

$$\frac{\Gamma \vdash \Delta, A \qquad \Gamma, A \vdash \Delta}{\Gamma \vdash \Delta}$$

нарушает свойство «подформульности», так как формула A может быть никак не связана с нижней секвенцией. Отметим, что добавление правила сечения не нарушает корректности, как легко проверить, и не может нарушить полноты.

Задачи о поиске вывода и анализе его структуры, хотя и были одно время модными в связи с «искусственным интеллектом», представляют большой интерес, и про них есть целая наука, в которой исчисления генценовского типа играют центральную роль. Мы рассмотрели один из вариантов исчисления секвенций для классического исчисления высказываний; бывают исчисления для интуиционистских и модальных логик, для исчисления предикатов и т. д. Исходной мотивацией для рассмотрения такого рода исчислений было желание доказать непротиворечивость арифметики. Согласно знаменитой второй теореме Гёделя о неполноте без дополнительных аксиом этого сделать нельзя, но если принять схему аксиом для трансфинитной индукции по ординалу ε_0, это удаётся сделать, как показал Генцен.

2.4. Интуиционистская пропозициональная логика

Исключим из числа аксиом закон исключённого третьего $A \vee \neg A$. Полученное исчисление называется *интуиционистским исчислением высказываний.* (Обычное исчисление высказываний называют *классическим*, чтобы избежать путаницы при его сравнении с интуиционистским. Вообще математические рассуждения, опирающиеся на аксиому исключённого третьего, называют «классическими», а избегающие её — «интуиционистскими».)

Конечно, сразу же возникают естественные вопросы. Почему именно эта аксиома вызывает сомнения? Вообще-то аксиом много, и можно было бы исключить любую и смотреть, что получится без неё — но ясно, что скорее всего получится что-то странное. Как понять, какие формулы останутся теоремами без закона исключённого третьего? Раньше у исчисления высказываний была «сверхзадача» — вывести все тавтологии и только их, а теперь?

Интуиционистская логика возникла как попытка (сделанная Гейтингом) формализовать (пусть частично) методы рассуждений, практикуемые в «интуиционистской математике». Голландский математик Брауэр широко известен как автор классической (во всех смыслах) теоремы Брауэра о неподвижной точке (она утверждает, что любое непрерывное отображение многомерного шара D^n в себя имеет неподвижную точку). Но одновременно он создал целую школу в области оснований математики — математический интуиционизм. Отчего, спрашивал Брауэр, в теории множеств возникли парадоксы? Можно считать, что это оттого, что мы стали рассуждать о каких-то уж очень абстрактных объектах, которые существуют лишь в нашей (порой противоречивой) фантазии, так что следует проявлять осторожность и не подходить к опасной черте. Но Брауэр пошел дальше, говоря, что противоречия лишь симптом болезни, а надо устранить её причину. Причину он видел в том, что математические рассуждения и понятия утратили интуитивный смысл, и нужно вернуться к основам и пересмотреть смысл самих логических связок.

Что мы имеем в виду (или должны иметь в виду), говоря о том, что мы установили, что «A или B»? Это значит, по Брауэру, что либо мы установили A, либо установили B. Когда мы устанавливаем, что «A и B», это значит, что мы установили и A, и B. «Если A, то B» означает, что мы располагаем каким-то общим рассуждением, которое позволит нам установить B, как только кто-то установит нам A. Отрицание A означает, что мы располагаем рассуждением, которое приводит к противоречию предположение, что A установлено. (Как с точки зрения интуиционизма, так и с классической точки зрения, $\neg A$ во всех смыслах эквивалентно $A \to \perp$, где $\perp$ — заведомо ложное утверждение. Можно было бы вообще не использовать отрицания, а иметь константу $\perp$ — это не очень привычно, но технически удобно.)

Интуиционизм отвергает идею о том, что все высказывания делятся на истинные и ложные (пусть неизвестным нам образом). С этой точки зрения закон исключённого третьего совершенно безоснователен: $A \vee \neg A$ означает, что для произвольного утверждения A мы можем установить либо A, либо его отрицание (то есть объяснить, почему A в принципе не может быть установлено) — а почему, собственно?

Обычно, говоря об интуиционизме, приводят следующий пример рассуждения, неприемлемого с точки зрения интуиционизма. Докажем, что существуют иррациональные числа α и β, для которых α^β рационально. В самом деле, рассмотрим два случая. Если $\sqrt{2}^{\sqrt{2}}$ рационально, то можно положить $\alpha = \beta = \sqrt{2}$. Если же $\sqrt{2}^{\sqrt{2}}$ иррационально, то положим $\alpha = \sqrt{2}^{\sqrt{2}}$ и $\beta = \sqrt{2}$; легко проверить, что $\alpha^\beta = 2$. Интуиционист скажет, что это рассуждение некорректно: доказать существование чего-то означает построить этот объект, а мы так и не построили чисел α и β, поскольку не установили, какой из двух случаев имеет место. (Заметим в скобках, что специалисты по алгебраической теории чисел знают, что $\sqrt{2}^{\sqrt{2}}$ иррационально и даже трансцендентно. Кроме того, не нужно быть специалистом, чтобы заметить, что можно положить $\alpha = \sqrt{2}$ и $\beta = 2\log_2 3$.) Этот пример можно критиковать и с другой точки зрения, говоря, что само понятие действительного числа не является интуитивно ясным и требует обоснования.

Вообще интуиция — дело тонкое: если долго рассуждать, скажем, о действительных числах, то начинает казаться, что они в каком-то смысле существуют независимо от наших рассуждений. Именно поэтому психологически оправдан вопрос о том, скажем, как обстоят дела с континуум-гипотезой «на самом деле»: существует ли несчётное множество действительных чисел, не равномощное всем действительным числам, или не существует?

Мы не будем говорить о философских предпосылках интуиционизма подробно. Вкратце упрощённая история вопроса такова. Брауэр наметил планы переустройства математики на интуиционистских принципах и отстаивал их настолько горячо, что однажды Гильберт в раздражении заметил: отменить закон исключённого третьего — это всё равно что отнять у астрономов телескоп или запретить боксёрам пользоваться кулаками. Но, продолжал он, никто не может изгнать математиков из рая, который создал Кантор.

В планы Брауэра не входила формализация интуиционистской логики и математики, скорее наоборот. Тем не менее анализ принципов интуиционизма пошёл именно по этому пути, когда Гейтинг стал изучать пропозициональную логику без закона исключённого третьего. Различные спорные интуиционистские принципы стали предметом изучения с точки зрения формальной логики; были построены интуиционистские варианты формальной арифметики, теории множеств, логики предикатов, а также генценовские варианты интуиционистских систем. Были предложены различные интерпретации интуиционистской логики. Колмогоров предложил трактовать её как «логику задач», Клини предложил понятие «реализуемости», использующее теорию алгоритмов для толкования формул; были предложены топологические модели для интуиционистской логики и т. д. В СССР знамя Брауэра подхватила школа Маркова, написав на нём, впрочем, «конструктивизм» вместо идеологически сомнительного «интуиционионизма» и более последовательно ограничиваясь конечными объектами. Крипке в 1960-е годы предложил некоторую семантику (определение истинности), согласованную с интуиционистским исчислением высказываний и весьма естественную (даже странно, что её не придумали раньше); замечательным образом оказалось, что она в некотором смысле близка к методу форсинга, который примерно в это же время придумал Коэн, чтобы доказать независимость аксиомы выбора и континуум-гипотезы в теории множеств.

Возвращаясь к интуиционистскому исчислению высказываний, приведём несколько выводимых формул.

- Чтобы понять смысл формулы $(A \to B) \to (\neg B \to \to \neg A)$, вспомним, что отрицание $\neg X$ можно толковать как $(X \to \perp)$, где $\perp$ — заведомо ложное утверждение. Эта формула говорит, что если из A следует B, а из B следует заведомо ложное утверждение, то из A следует заведомо ложное утверждение (частный случай транзитивности отношения следования). Вывод её не использует закона исключённого третьего. В самом деле, по лемме о дедукции (доказательство которой остаётся тем же и для интуиционистского исчисления высказываний) достаточно доказать, что из $(A \to B)$ и $\neg B$ выводится $\neg A$. Для этого, в свою очередь, достаточно доказать, что из $(A \to B)$, $\neg B$ и A выводятся две противоречащие друг другу формулы (что очевидно: это формулы B и $\neg B$).

- Чтобы вывести формулу $(A \to \neg\neg A)$, надо показать, что из A выводится $\neg\neg A$, для чего достаточно из A и $\neg A$ вывести две противоречащие друг другу формулы (что тривиально — годятся сами формулы A и $\neg A$).

- Формула $(\neg\neg\neg A \to \neg A)$ получается из двух предыдущих: положим B равным $\neg\neg A$ в первой из них.

- Формула $(\neg A \to \neg\neg\neg A)$, с другой стороны, есть частный случай второй формулы, так что три отрицания равносильны одному.

- Коммутативность и ассоциативность операций $\wedge$

и $\vee$, так же как и два свойства дистрибутивности, не опирались на закон исключённого третьего.

- По-прежнему $((A \vee B) \to C)$ равносильно $((A \to C) \wedge \wedge (B \to C))$ (импликации в обе стороны, связывающие эти формулы, выводимы в интуиционистском исчислении высказываний).

- Взяв $\perp$ в качестве C в предыдущих формулах, мы видим, что один из законов Де Моргана (а именно, закон $\neg(A \vee B) \leftrightarrow \neg A \wedge \neg B$) не опирается на закон исключённого третьего (что легко проверить и непосредственно).

- Формулу $\neg\neg(A \vee \neg A)$ сохранившийся закон де Моргана позволяет переписать в виде $\neg(\neg A \wedge \neg\neg A)$, и нужно лишь вывести из $(\neg A \wedge \neg\neg A)$ две противоположные формулы, что очевидно.

31. Провести подробно доказательство выводимости в интуиционистском исчислении высказываний всех перечисленных формул.

С другой стороны, многие законы классической логики перестают быть выводимыми без закона исключённого третьего. Таковы, например, формулы

$$\begin{aligned}
&\neg\neg p \to p,\\
&p \vee \neg p,\\
&\neg p \vee \neg\neg p,\\
&(\neg q \to \neg p) \to (p \to q),\\
&\neg(p \wedge q) \to (\neg p \vee \neg q),\\
&((p \vee q) \to p) \vee ((p \vee q) \to q).
\end{aligned}$$

Мы пишем здесь переменные p и q, а не произвольные формулы, поскольку результат подстановки некоторых формул вместо p и q может быть выводимой формулой. Например, если вместо p в первую из перечисленных формул подставить формулу $\neg A$, то получится выводимая формула $\neg\neg\neg A \to \neg A$.

Довольно ясно, что эти формулы не согласуются с интуиционистским подходом. Например, в предпоследней формуле говорится, что если мы опровергли предположение $(p \wedge q)$, то мы можем указать на одно из предположений p и q и предъявить его опровержение. Вряд ли такой переход можно считать обоснованным с интуиционистской точки зрения. Но, разумеется, формальный вопрос о выводимости требует формального ответа.

Начнём с закона исключённого третьего.

Теорема 24. Формула $p \vee \neg p$ не выводима в интуиционистской логике.

$\triangleleft$ В классической логике каждая пропозициональная переменная может принимать два значения — истина (**И**) и ложь (**Л**). В зависимости от значений переменных каждой формуле также приписывается значение **И** или **Л**. Расширим множество истинностных значений, добавив новое значение **Н** (если угодно, можно считать это сокращением слова «неизвестно»). Мы отождествляли **И** с единицей, а **Л** — с нулём, так что логично отождествить **Н** с числом $1/2$.

Мы докажем, что интуиционистски выводимые формулы всегда принимают значение **И**, а формула $p \vee \neg p$ не такова, и потому не выводима.

Чтобы определить значения формул в трёхзначной логике, необходимо задать таблицы истинности для всех пропозициональных связок. Конъюнкцию определим как минимум из двух значений (так что, например, $\mathbf{Л} \wedge \mathbf{Н} = \mathbf{Л}$, а $\mathbf{И} \wedge \mathbf{Н} = \mathbf{Н}$), а дизъюнкцию — как максимум. Отрицание действует так: $\neg\mathbf{И} = \mathbf{Л}$, $\neg\mathbf{Л} = \mathbf{И}$, $\neg\mathbf{Н} = \mathbf{Л}$. (Последнее может показаться странным: почему бы не считать, что $\neg\mathbf{Н} = \mathbf{Н}$? Оказывается, так нельзя — например, потому, что тогда формула $\neg(p \wedge \neg p)$, которая выводима в интуиционистской логике, будет иметь значение **Н** при $p = \mathbf{Н}$.)

Сложнее всего определение истинности для импликации. Мы полагаем, что

$$(\mathbf{И} \to x) = x \quad \text{и} \quad (\mathbf{Л} \to x) = \mathbf{И}$$

для любого истинностного значения x, а также что

$$(\mathbf{Н} \to \mathbf{Л}) = \mathbf{Л}, \quad (\mathbf{Н} \to \mathbf{Н}) = \mathbf{И} \text{ и } (\mathbf{Н} \to \mathbf{И}) = \mathbf{И}.$$

Назовем формулу 3-*тавтологией*, если она принимает значение **И** при любых значениях переменных из множества $\{\mathbf{И}, \mathbf{Л}, \mathbf{Н}\}$. Теперь надо проверить две вещи: (1) все аксиомы интуиционистского исчисления являются 3-тавтологиями; (2) если посылка импликации и вся импликация являются 3-тавтологиями, то и заключение тоже является 3-тавтологией. Второе сразу ясно из определения импликации, а первое надо аккуратно проверять, составив таблицы для всех аксиом. Мы не будем этого подробно делать, поскольку это чисто механическая проверка и поскольку чуть позже мы сможем вывести это из более общего утверждения.

Следовательно, всякая интуиционистски выводимая формула является 3-тавтологией. Теперь заметим, что формула $p \vee \neg p$ принимает значение **Н** при $p = \mathbf{Н}$ и потому не является 3-тавтологией — значит, невыводима. $\triangleright$

32. Покажите, что всякая 3-тавтология является тавтологией в обычном смысле.

Использованный нами приём годится не всегда. Например, интуиционистски невыводимая формула $\neg p \vee \neg\neg p$ является 3-тавтологией, поскольку (согласно нашему определению) формула $\neg p$ может принимать только значения **И** и **Л**.

33. Какие из перечисленных нами интуиционистски невыводимых формул являются 3-тавтологиями?

Более общий способ установления недоказуемости (невыводимости) различных формул доставляют *шкалы Крипке* (или *модели Крипке*, как ещё говорят).

Чтобы задать шкалу Крипке, нужно:

- указать частично упорядоченное множество $\langle W, \leqslant \rangle$, называемое множеством *миров*;
- для каждого мира указать, какие из пропозициональных переменных считаются *истинными* в этом

мире (остальные переменные считаются *ложными* в этом мире). Если переменная x истинна в мире w, мы пишем $w \Vdash x$.

При этом требуется, чтобы было выполнено следующее: если $u \leqslant v$ и $u \Vdash x$, то $v \Vdash x$ (область истинности любой переменной наследственна вверх).

Когда шкала задана, можно определить истинность любой формулы (в данном мире) индукцией по построению формулы. Мы пишем $w \Vdash A$, если в мире w истинна формула A. Вот индуктивное определение:

- $w \Vdash A \wedge B$, если $w \Vdash A$ и $w \Vdash B$;
- $w \Vdash A \vee B$, если $w \Vdash A$ или $w \Vdash B$;
- $w \Vdash A \to B$, если в любом мире $u \geqslant w$, в котором истинна формула A, истинна также и формула B;
- $w \Vdash \neg A$, если ни в каком мире $u \geqslant w$ формула A не является истинной.

Формула, не являющаяся истинной (в данном мире), называется ложной (в нём).

Определение истинности для отрицания, как легко проверить, согласовано с пониманием $\neg A$ как $A \to \bot$, где $\bot$ — тождественно ложная (во всех мирах) формула.

Именно определение импликации (и отрицания) использует порядок на множестве миров. Если формула содержит лишь конъюнкции и дизъюнкции, то её истинность по существу определяется отдельно в каждом мире.

Индукцией по построению формулы A легко проверить, что если она истинна в каком-то мире, то истинна и во всех бо́льших мирах. В самом деле, пересечение и объединение двух наследственных вверх множеств также обладает этим свойством, так что для случая конъюнкции и дизъюнкции можно сослаться на предположение индукции. А для импликации даже и этого не нужно, достаточно посмотреть на определение.

Философский смысл шкал Крипке иногда объясняют так. Пусть W есть множество возможных состояний цивилизации (миров); $w \leqslant u$ означает, что мир u может получиться из мира w в результате развития цивилизации. Утверждение $w \Vdash A$ означает, что в мире w установлено, что высказывание A истинно. (При этом оно останется истинным и при дальнейшем развитии цивилизации.) Истинность $\neg A$ в мире w означает, что ни при каком развитии цивилизации из состояния w высказывание A не станет истинным.

Определение истинности отрицания в шкалах Крипке предвосхитил Пушкин, когда писал «нет правды на земле. Но правды нет и выше...» (Моцарт и Сальери).

34. Во что превращается определение истинности в шкале Крипке, если в ней только один мир? если в ней никакие два мира не сравнимы?

Теорема 25 (корректность интуиционистского исчисления высказываний относительно шкал Крипке). Формула, выводимая в интуиционистском исчислении высказываний, истинна во всех мирах всех шкал Крипке.

$\triangleleft$ Надо проверить, что все аксиомы истинны во всех мирах, а также что правило modus ponens сохраняет это свойство. Второе очевидно: если $A \to B$ истинна во всех мирах и A истинна во всех мирах, то по определению истинности импликации B будет истинна во всех мирах.

Осталось проверить истинность всех аксиом. Чтобы установить, что импликация $\varphi \to \psi$ истинна во всех мирах, надо проверить, что в тех мирах, где истинна формула φ, истинна и формула ψ. Для первой аксиомы $A \to (B \to A)$: если формула A истинна в некотором мире, то в силу монотонности она истинна и выше, так что $B \to A$ также истинна.

Проверим вторую аксиому $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$. Пусть $u \Vdash A \to (B \to C)$. Надо убедиться, что $u \Vdash (A \to B) \to (A \to C)$. Это означает, что если $v \geqslant u$ и $v \Vdash A \to B$, то $v \Vdash A \to C$. Последнее, в свою очередь, значит, что если $w \geqslant v$ и

$w \Vdash A$, то $w \Vdash C$. Но в силу монотонности мы знаем, что $w \Vdash A \to (B \to C)$ и $w \Vdash A \to B$. Поэтому из $w \Vdash A$ следует $w \Vdash B$, $w \Vdash (B \to C)$, и, наконец, $w \Vdash C$, что и требовалось.

Остальные аксиомы проверяются ещё проще. $\triangleright$

Таким образом, чтобы доказать, что некоторая формула не выводима в интуиционистском исчислении высказываний, достаточно предъявить шкалу Крипке, в одном из миров которой она ложна.

35. Покажите, что в этом случае есть шкала, в которой среди миров есть наименьший и в нём формула ложна.

Для формулы $p \vee \neg p$ такая шкала строится легко. Возьмём два мира, первый меньше второго. Пусть p истинна только во втором мире. Тогда $\neg p$ не будет истинна нигде, а $p \vee \neg p$ будет истинна только во втором мире.

На самом деле это доказательство в сущности совпадает с приведённым выше (с трёхзначной логикой). В самом деле, в этой шкале для формулы есть три возможности: она истинна в обоих мирах, она истинна только во втором мире, или она не истинна ни в одном из миров. Эти три возможности соответствуют трём значениям **И**, **Н** и **Л** в рассмотренной нами трёхзначной интерпретации. Легко проверить, что таблицы операций как раз соответствуют определению истинности в модели Крипке.

Теперь мы можем установить, что все перечисленные выше формулы невыводимы в интуиционистском исчислении высказываний. Для формулы $\neg\neg p \to p$ годится та же самая шкала (p истинно только в большем мире). Она же годится для формулы $(\neg q \to \neg p) \to (p \to q)$, если p истинно в обоих мирах, а q — только в большем. Для трёх оставшихся формул можно рассмотреть шкалы с тремя мирами: начальным миром u, из которого можно попасть в $v \geqslant u$ и в $w \geqslant u$; миры v и w не сравнимы. Если формула p истинна только в мире v, то формула $\neg p$ истинна только в мире w, а $\neg\neg p$ истинна только в мире v, так что в мире u обе формулы $\neg p$ и $\neg\neg p$ ложны и дизъюнкция $\neg p \vee \neg\neg p$ ложна. Чтобы построить контрмодель для формулы $\neg(p \wedge q) \to \neg p \vee \neg q$, будем считать, что p истинна только в мире v, а q истинна только в мире w. Та же шкала годится и для формулы $((p \vee q) \to p) \vee ((p \vee q) \to q)$.

Оказывается, что этот приём универсален, как показывает следующая теорема.

Теорема 26 (полноты интуиционистского исчисления высказываний относительно шкал Крипке). Для любой невыводимой в интуиционистском исчислении формулы φ можно подобрать шкалу Крипке, в которой φ ложна в некотором мире.

$\lhd$ Напомним схему доказательства полноты классического исчисления высказываний, приведённого в разделе 2.2. Пусть формула φ невыводима. Мы хотим найти значения переменных, при которых формула φ ложна, то есть формула $\neg\varphi$ истинна. Само по себе требование истинности $\neg\varphi$ не определяет значения переменных однозначно. Чтобы избавиться от произвола, мы расширяем непротиворечивое множество $\{\neg\varphi\}$ до полного множества Γ и объявляем истинными те переменные, которые входят в Γ.

Для интуиционистского случая в этой схеме требуются некоторые изменения. Раньше ложность формулы φ была равносильна истинности формулы $\neg\varphi$. В шкалах Крипке это уже не так, и мы будем отдельно говорить об истинных и ложных (не истинных) формулах.

Пусть A и B — конечные множества пропозициональных формул. Будем говорить, что пара (A, B) *совместна*, если существует шкала Крипке и её мир, в котором все формулы из A истинны, а все формулы из B ложны. Будем говорить, что пара (A, B) *противоречива*, если в интуиционистском исчислении высказываний выводима формула

$$(A_1 \wedge A_2 \wedge \ldots \wedge A_n) \to (B_1 \vee B_2 \vee \ldots \vee B_m),$$

где $A_1, \ldots, A_n$ — формулы множества A, а $B_1, \ldots, B_m$ — формулы множества B. (Без ограничения общности можно считать, что перечислены все формулы множеств A

и B, поскольку пропущенные формулы можно добавить, не нарушив выводимость.)

Пример: если одна и та же формула входит в обе части пары, то такая пара противоречива.

Легко проверить, что противоречивая пара не может быть совместна. В самом деле, если в некотором мире все формулы из A истинны, а все формулы из B ложны, то посылка импликации в этом мире истинна, а заключение ложно. Поэтому импликация ложна, что противоречит её выводимости (теорема о корректности).

Мы докажем, что верно и обратное: всякая непротиворечивая пара совместна. В частности, когда B состоит из единственной формулы, получается утверждение теоремы о полноте. (Мы предполагаем, как это обычно делается, что конъюнкция пустого множества формул есть тождественно истинная формула, а дизъюнкция — тождественно ложная. Поэтому противоречивость пары $(\varnothing, \{\varphi\})$ означает выводимость формулы φ. Заметим кстати, что противоречивость пары $(\{\varphi\}, \varnothing)$ означает выводимость формулы $\neg\varphi$.)

Итак, пусть имеется непротиворечивая пара (A, B). Как доказать её совместность? Как и в классическом случае, мы устраним произвол, расширив A и B. Основным средством здесь является такая лемма.

Лемма 1. Пусть (A, B) — непротиворечивая пара, а τ — произвольная формула. Тогда хотя бы одна из пар $(A \cup \{\tau\}, B)$ и $(A, B \cup \{\tau\})$ непротиворечива.

Доказательство леммы 1. Пусть обе пары с добавленным τ противоречивы. Надо доказать, что противоречива исходная пара. Другими словами, надо показать, что если в интуиционистском исчислении высказываний выводимы формулы

$$(A \wedge \tau) \to B,$$
$$A \to (B \vee \tau),$$

то выводима и формула $A \to B$ (для простоты мы отождествляем множества A и B с конъюнкцией и дизъюнкцией их элементов и считаем A и B формулами).

В самом деле, по лемме о дедукции достаточно доказать, что $A \vdash B$. Для этого достаточно установить, что

$$A \vdash (B \vee \tau) \to B,$$

поскольку $(B \vee \tau)$ в предположении A у нас уже есть. Для этого, в свою очередь, достаточно установить, что $A \vdash (B \to B)$ и $A \vdash (\tau \to B)$. Первое очевидно (и посылка A не нужна), второе равносильно выводимости формулы $(A \wedge \tau) \to B$, которая нам дана по условию леммы. Лемма 1 доказана.

Проведённое рассуждение, как говорят, устанавливает *допустимость* (в интуиционистской логике) *правила сечения*, позволяющего «иссечь» формулу τ из формул $(A \wedge \tau) \to B$ и $A \to (B \vee \tau)$ и получить формулу $A \to B$.

Возвращаясь к доказательству теоремы, рассмотрим произвольную непротиворечивую пару (A, B). Рассматривая по очереди различные формулы τ, мы будем добавлять их к левой или правой части. Чтобы этот процесс («пополнение») был конечным, мы ограничимся формулами из некоторого множества.

Фиксируем некоторое конечное множество формул F, которое содержит все формулы из A, B и замкнуто относительно перехода к подформулам (если формула входит в F, то все её подформулы входят в F). Например, можно включить в F все подформулы всех формул из A и из B.

Пару (X, Y), у которой $X, Y \subset F$, будем называть *полной*, если она непротиворечива и любая формула из F входит либо в X, либо в Y (то есть $X \cup Y = F$). Заметим, что из непротиворечивости следует, что $X \cap Y = \varnothing$, так что полная пара задаёт разбиение F на две части. (Более точно полные пары следовало бы называть «полными относительно F», но у нас множество F фиксировано.)

Лемма 2. Исходная пара (A, B) может быть расширена до полной: существует полная пара (X, Y), для которой $A \subset X$, $B \subset Y$.

Доказательство очевидно: применяем по очереди лемму 1 ко всем формулам из F.

Точно так же любую непротиворечивую пару, составленную из формул множества F, можно расширить до полной. (Это замечание нам впоследствии понадобится.)

Для завершения доказательства теоремы 26 нам осталось показать, что всякая полная пара (A, B) совместна (существует шкала и мир, в котором формулы из A истинны, а формулы из B ложны). В отличие от классического случая построение будет использовать не только пару (A, B), но и все полные пары.

Шкала Крипке строится так. Мирами будут полные пары (R, S) (то есть всевозможные непротиворечивые разбиения множества F на левую и правую части). Истинность переменных определяется естественным образом: всякая переменная p, входящая в одну из формул множества F, сама принадлежит множеству F (замкнутость относительно подформул); если p входит в левую часть полной пары (R, S), то p истинна в мире (R, S), если в правую — то ложна. (Впоследствии это свойство мы распространим на все формулы: любая формула из R окажется истинной в мире (R, S), а любая формула из S — ложной.)

Осталось определить порядок на множестве пар. Считаем, что $(R_1, S_1) \leqslant (R_2, S_2)$, если $R_1 \subset R_2$. (Такое определение не удивительно, если вспомнить, что истинность формул наследуется вверх.)

Лемма 3. В построенной шкале в мире (R, S) истинны все формулы из R и ложны все формулы из S.

Доказательство леммы 3 проводится индукцией по построению формул. Для переменных она верна по определению истинности. Пусть некоторая формула из F не является переменной. Тогда она есть конъюнкция, дизъюнкция, импликация или отрицание и для её частей утверждение леммы верно по предположению индукции. Рассмотрим все случаи по очереди, начав с конъюнкции и дизъюнкции (истинность которых не зависит от других миров).

($\wedge_R$) Пусть формула $\varphi \wedge \psi$ входит в R. Тогда формулы φ и ψ не могут входить в S, иначе пара (R, S) была бы противоречивой (из $\varphi \wedge \psi$ выводится φ и ψ). Значит, φ и ψ входят в R (полнота), поэтому они истинны (предположение индукции), и потому $\varphi \wedge \psi$ истинна (определение истинности).

($\wedge_S$) Пусть формула $\varphi \wedge \psi$ входит в S. Могут ли обе формулы φ и ψ входить в R? Нет, так как в этом случае пара (R, S) была бы противоречивой. Значит, хотя бы одна из формул входит в S, тогда по предположению индукции она ложна, и потому формула $\varphi \wedge \psi$ ложна в мире (R, S).

($\vee_R$) Если формула $\varphi \vee \psi$ входит в R, то формулы φ и ψ не могут одновременно входить в S, и потому хотя бы одна из них истинна, так что и вся формула $\varphi \vee \psi$ истинна.

($\vee_S$) Если формула $\varphi \vee \psi$ входит в S, то формулы φ и ψ не могут входить в R, поэтому обе они ложны и формула $\varphi \vee \psi$ ложна.

($\rightarrow_R$) Пусть формула $\varphi \rightarrow \psi$ входит в R. Проверим, что она истинна в (R, S). Это значит, что в любом мире (R', S'), который выше нашего (то есть $R' \supset R$) и в котором истинна формула φ, должна быть истинна и формула ψ. В самом деле, если φ истинна в (R', S'), то она входит в R' (предположение индукции). С другой стороны, и $\varphi \rightarrow \psi$ входит в R', поскольку $R' \supset R$. Теперь ясно, что формула ψ не может входить в S', так как в этом случае пара (R', S') была бы противоречивой (из φ и $\varphi \rightarrow \psi$ выводится ψ). Значит, ψ входит в R' и потому истинна в (R', S') по предположению индукции.

($\rightarrow_S$) Это наиболее интересный случай, где нам снова потребуется пополнение. Пусть формула $\varphi \rightarrow \psi$ входит в S. Мы должны доказать, что она ложна в мире (R, S). Согласно определению, это означает, что найдётся мир (R', S'), для которого $R' \supset R$ и в котором формула φ истинна, а формула ψ ложна (то есть $\varphi \in R'$ и $\psi \in S'$, согласно предположению индукции). Как найти такой мир?

Рассмотрим пару $(R \cup \{\varphi\}, \{\psi\})$. Эта пара непротиворечива. В самом деле, если бы формула $R \wedge \varphi \to \psi$ была бы выводима, то и формула $R \to (\varphi \to \psi)$ была бы выводима (лемма о дедукции), и потому пара (R, S) была бы противоречива. Теперь можно расширить непротиворечивую пару $(R \cup \{\varphi\}, \{\psi\})$ до полной пары (R', S'), которая и будет искомым миром.

Отрицание рассматривается аналогично импликации (как мы уже говорили, можно было бы вместо отрицания ввести тождественную ложь $\perp$ и вообще его не рассматривать).

$(\neg_R)$ Пусть формула $\neg\varphi$ входит в R. Тогда формула φ не может входить в R, так как из $\varphi \wedge \neg\varphi$ выводится любая формула и пара (R, S) была бы противоречивой. Значит, φ входит в S и потому ложна.

$(\neg_S)$ Пусть формула $\neg\varphi$ входит в S. Тогда пара $(R \cup \{\varphi\}, \varnothing)$ непротиворечива (если из R и φ выводится противоречие, то из R выводится $\neg\varphi$). Расширив её до полной, получаем высший мир (R', S'), в котором формула φ ложна.

Лемма 3 доказана. Она завершает доказательство теоремы 26. Напомним ещё раз его схему. Пусть формула φ не выводима в интуиционистском исчислении высказываний. Тогда пара $(\varnothing, \{\varphi\})$ непротиворечива. Фиксируем множество F всех подформул формулы φ. Расширим нашу непротиворечивую пару до полной (относительно F). Эта полная пара будет одним из миров шкалы Крипке (в которой мирами являются полные пары). Именно в этом мире и будет ложной формула φ. $\triangleright$

36. Покажите, что если формулы P и Q ложны в некоторых мирах некоторых шкал Крипке, то можно построить шкалу Крипке и мир в ней, для которого формула $P \vee Q$ будет ложной. (Указание: соединим шкалы, в которых ложны формулы P и Q, в одну, добавив новый мир, который меньше миров, где P и Q ложны.)

Из этой задачи и из теоремы о полноте вытекает такое следствие: если дизъюнкция двух формул выводима в интуиционистском исчислении высказываний, то хотя бы одна из формул тоже выводима. Это свойство выполнено для многих интуиционистских исчислений и соответствует начальной идее: доказать $A \vee B$ означает доказать одну из формул A или B. Подобные свойства можно доказывать и синтаксически, используя генценовские варианты интуиционистских исчислений.

37. (**а**) Покажите, что формула $\neg\neg(\varphi \vee \neg\varphi)$ выводима в интуиционистском исчислении высказываний. (**б**) Покажите, что если формулы $\neg\neg\varphi$ и $\neg\neg(\varphi \to \psi)$ выводимы в интуиционистском исчислении высказываний, то и формула $\neg\neg\psi$ выводима в интуиционистском исчислении высказываний. (**в**) Докажите, что если формула φ выводима в классическом исчислении высказываний, то формула $\neg\neg\varphi$ выводима в интуиционистском исчислении высказываний (теорема Гливенко) (**г**) Покажите, что для формул, содержащих лишь конъюнкцию и отрицание, разницы между классическим и интуиционистским исчислениями нет: из классической выводимости следует интуиционистская (теорема Гёделя).

38. Покажите, что интуиционистское исчисление высказываний разрешимо: существует алгоритм, который по произвольной формуле определяет, выводима ли она в интуиционистском исчислении высказываний. (Указание: оцените мощность контрмодели Крипке; можно обойтись и без этого, заметив, что и множество выводимых формул, и множество формул, имеющих конечные контрмодели, перечислимы.)

3. Языки первого порядка

Помимо логических связок, в математических рассуждениях часто встречаются *кванторы* «для любого» ($\forall$) и «существует» ($\exists$). Например, определение непрерывности начинается словами «для любого положительного ε найдётся положительное δ, для которого …». А одна из аксиом теории групп (существование обратного элемента) записывается так: $\forall x \exists y ((xy = 1) \wedge (yx = 1))$.

Можно сформулировать различные логические законы, включающие в себя кванторы. Например, высказывание «существует такое x, что A» (где A — некоторое свойство объекта x) логически эквивалентно высказыванию «не для всех x верно $\neg A$».

Мы будем записывать такого рода законы с помощью формул, дадим определение истинности формул (при данной интерпретации входящих в них символов) и исследуем, какого рода свойства можно выражать с помощью формул и какие нельзя.

3.1. Формулы и интерпретации

Начнём с примера. Пусть M — некоторое непустое множество, а R — бинарное отношение на нём, то есть подмножество декартова произведения $M \times M$. Вместо $\langle x, y \rangle \in R$ мы будем писать $R(x, y)$. Рассмотрим формулу

$$\forall x \, \exists y \, R(x, y).$$

Эта формула выражает некоторое свойство бинарного отношения R (для любого элемента $x \in M$ найдётся элемент, находящийся с ним в отношении R) и может быть истинна или ложна. Например, если M есть множество натуральных чисел $\mathbb{N}$, а R — отношение «строго меньше» (другими словами, R есть множество всех пар $\langle x, y \rangle$, для которых $x < y$), то эта формула истинна. А для отношения «строго больше» (на том же множестве) эта формула ложна.

Вопрос о том, будет ли истинна формула

$$\exists y\, R(x,y)$$

для данного множества M и для данного бинарного отношения R на нём, не имеет смысла, пока не уточнено, каково значение переменной x. Например, если $M = \mathbb{N}$ и $R(x,y)$ есть $x > y$, то эта формула будет истинной при $x = 3$ и ложной при $x = 0$. Для данных M и R она задаёт некоторое свойство элемента x и тем самым определяет некоторое подмножество множества M.

Перейдём к формальным определениям. Пусть M — непустое множество. Множество M^k состоит из всех последовательностей $\langle m_1, \ldots, m_k \rangle$ длины k, составленных из элементов множества M. Назовём *k-местной функцией* на множестве M любое отображение M^k в M (определённое на всём M^k). Синонимы: «функция k аргументов», «функция валентности k», «функция местности k» и даже «функция арности k» (последнее слово происходит от слов «унарная» для функций одного аргумента, «бинарная» (операция) для функций двух аргументов и «тернарная» для трёх аргументов).

Назовём *k-местным предикатом* на множестве M любое отображение M^k в множество $\mathbb{B} = \{\textbf{И}, \textbf{Л}\}$. Такой предикат будет истинным на некоторых наборах $\langle m_1, \ldots, m_k \rangle$ множества M и ложным на остальных наборах. Поставив ему в соответствие множество тех наборов, где он истинен, мы получаем взаимно однозначное соответствие между k-местными предикатами на M и подмножествами множества M^k. Говоря о предикатах, также употребляют термины «валентность», «число аргументов» и др.

Мы будем рассматривать также функции и предикаты валентности нуль. Множество M^0 одноэлементно (содержит единственную последовательность длины 0). Поэтому функции $M^0 \to M$ отождествляются с элементами множества M, а нульместных предикатов ровно два — истинный и ложный.

Естественно, что в формулы будут входить не сами функции и предикаты, а обозначения для них, которые называют *функциональными* и *предикатными символами*. В качестве символов можно использовать любые знаки. Важно лишь, что каждому символу приписана валентность, которая определяет, со сколькими аргументами он может встречаться в формуле. Произвольный набор предикатных и функциональных символов, для каждого из которых указано неотрицательное число, называемое *валентностью*, мы будем называть *сигнатурой*.

Остаётся определить три вещи: что такое формула данной сигнатуры, что такое интерпретация данной сигнатуры и когда формула является истинной (в данной интерпретации).

Фиксируем некоторый набор символов, называемых *индивидными переменными*. Они предназначены для обозначения элементов множества, на котором определены функции и предикаты; обычно в таком качестве используют латинские буквы x, y, z, u, v, w с индексами. В каждой формуле будет использоваться конечное число переменных, так что счётного набора переменных нам хватит. Мы предполагаем, что переменные отличны от всех функциональных и предикатных символов сигнатуры (иначе выйдет путаница).

Определим понятие *терма* данной сигнатуры. Термом называется последовательность переменных, запятых, скобок и символов сигнатуры, которую можно построить по следующим правилам:

- Индивидная переменная есть терм.
- Функциональный символ валентности 0 есть терм.
- Если $t_1, \ldots, t_k$ — термы, а f — функциональный символ валентности $k > 0$, то $f(t_1, \ldots, t_k)$ есть терм.

В принципе можно было не выделять функциональные символы валентности 0 (которые также называют *константами*) в отдельную группу, но тогда бы после них пришлось писать скобки (как это делается в программах на языке Си).

Если A — предикатный символ валентности k, а $t_1, \ldots, t_k$ — термы, то выражение $A(t_1, \ldots, t_k)$ считается *атомарной формулой.* Кроме того, любой предикатный символ валентности 0 считается атомарной формулой.

Формулы строятся по таким правилам:

- Атомарная формула есть формула.
- Если φ — формула, то $\neg\varphi$ — формула.
- Если φ и ψ — формулы, то выражения $(\varphi \wedge \psi)$, $(\varphi \vee \vee \psi)$, $(\varphi \to \psi)$ также являются формулами.
- Если φ есть формула, а ξ — индивидная переменная, то выражения $\forall\xi\, \varphi$ и $\exists\xi\, \varphi$ являются формулами.

Во многих случаях в сигнатуру входит двуместный предикатный символ $=$, называемый *равенством.* По традиции вместо $=(t_1, t_2)$ пишут $(t_1 = t_2)$.

Итак, понятие формулы в данной сигнатуре полностью определено. Иногда такие формулы называют *формулами первого порядка* данной сигнатуры, или формулами *языка первого порядка* с данной сигнатурой.

Наш следующий шаг — определение *интерпретации* данной сигнатуры. Пусть фиксирована некоторая сигнатура σ. Чтобы задать интерпретацию сигнатуры σ, необходимо:

- указать некоторое непустое множество M, называемое *носителем* интерпретации;
- для каждого предикатного символа сигнатуры σ указать предикат с соответствующим числом аргументов, определённый на множестве M (как мы уже говорили, 0-местным предикатным символам ставится в соответствие либо **И**, либо **Л**);
- для каждого функционального символа сигнатуры σ указать функцию соответствующего числа

аргументов с аргументами и значениями из M (в частности, для 0-местных функциональных символов надо указать элемент множества M, с ними сопоставляемый).

Если сигнатура включает в себя символ равенства, то среди её интерпретаций выделяют *нормальные* интерпретации, в которых символ равенства интерпретируется как совпадение элементов множества M.

Приведём несколько примеров сигнатур, используемых в различных теориях.

Сигнатура теории упорядоченных множеств включает в себя два двуместных предикатных символа (равенство и порядок) и не имеет функциональных символов. Здесь также вместо $\leqslant(x,y)$ по традиции пишут $x \leqslant y$.

Аксиомы порядка (рефлексивность, антисимметричность, транзитивность) могут быть записаны формулами этой сигнатуры. Например, требование антисимметричности записывается так:

$$\forall x\, \forall y(((x \leqslant y) \wedge (y \leqslant x)) \to (x = y)).$$

Иногда в сигнатуру теории упорядоченных множеств вместо символа $\leqslant$ включают символ $<$; большой разницы тут нет.

39. Как записать с помощью формулы свойство линейной упорядоченности? свойство не иметь наибольшего элемента? свойство плотности (отсутствия соседних элементов)? свойство фундированности (отсутствия бесконечных убывающих последовательностей — или, что эквивалентно, наличия минимального элемента в любом подмножестве)? свойство полной упорядоченности? (Указание: не для всех перечисленных свойств это возможно.)

Сигнатуру теории групп можно выбирать по-разному. Можно считать, что (помимо равенства) она имеет двуместный функциональный символ $\times$ (который по традиции записывают между множителями), константу (нульместный функциональный символ) 1 и одноместный функциональный символ $\mathrm{inv}(x)$ для обращения. Тогда аксиомы теории групп записываются с использованием лишь кванторов всеобщности:

$$\forall x\,\forall y\,\forall z(((x\times y)\times z)=(x\times(y\times z))),$$
$$\forall x\,(((x\times 1)=x)\wedge((1\times x)=x)),$$
$$\forall x\,(((x\times \mathrm{inv}(x))=1)\wedge((\mathrm{inv}(x)\times x)=1)).$$

Если не включать операцию обращения в сигнатуру, придётся использовать квантор существования и переписать последнюю аксиому так:

$$\forall x\,\exists y\,(((x\times y)=1)\wedge((y\times x)=1)).$$

40. Как записать аксиомы теории групп, если в сигнатуре нет константы 1? (Указание: аксиома о существовании обратного станет частью аксиомы о существовании единицы.)

41. Как записать в виде формулы требование коммутативности группы? утверждение о том, что любой элемент (кроме единицы) имеет порядок 11? конечность группы? (Указание: не всё из перечисленного можно записать, хотя пока у нас нет средств это установить.)

Сигнатура теории множеств содержит два двуместных предикатных символа: для принадлежности и для равенства. Аксиомы теории множеств можно записывать в виде формул этой сигнатуры. Чаще всего рассматривают вариант аксиоматической теории множеств, называемый теорией Цермело – Френкеля и обозначаемый ZF. Приведём для примера одну из аксиом теории ZF, называемую *аксиомой объёмности*, или *экстенсиональности*:

$$\forall x\,\forall y\,((\forall z\,((z\in x)\to(z\in y))\wedge\forall z\,((z\in y)\to(z\in x)))\to$$
$$\to(x=y)).$$

42. Сформулировать словесно эту аксиому.

43. Записать в виде формулы *аксиому регулярности*, или *фундирования*, которая говорит, что у всякого множества есть минимальный (с точки зрения отношения $\in$) элемент, то есть элемент, не пересекающийся с самим множеством.

44. Какова естественная сигнатура для теории полей? Можно ли записать в виде формулы этой сигнатуры утверждение о том, что поле имеет характеристику 2? конечную характеристику? алгебраически замкнуто?

3.2. Определение истинности

Из приведённых выше примеров, вероятно, понятен смысл формулы, то есть ясно, в каких интерпретациях данной сигнатуры и для каких элементов формула истинна. Тем не менее для любителей строгости мы приведём формальное определение истинности. (Его детали понадобятся, когда мы будем проверять истинность выводимых формул, см. раздел 4.3.)

Прежде всего, определим формально понятие *параметра* формулы (переменной, от значения которой может зависеть истинность формулы). Согласно этому определению, скажем, формула $\forall x\,\exists y\,A(x,y)$ не имеет параметров, а формулы $\exists y\,A(x,y)$ и $(A(x)\wedge\forall x\,B(x,x))$ имеют единственный параметр x. Вот как выглядит это определение:

- Параметрами терма являются все входящие в него индивидные переменные.
- Параметрами атомарной формулы являются параметры всех входящих в неё термов.
- Параметры формулы $\neg\varphi$ те же, что у формулы φ.
- Параметрами формул $(\varphi\wedge\psi)$, $(\varphi\vee\psi)$ и $(\varphi\to\psi)$ являются все параметры формулы φ, а также все параметры формулы ψ.
- Параметрами формул $\forall\xi\,\varphi$ и $\exists\xi\,\varphi$ являются все параметры формулы φ, кроме переменной ξ.

Параметры иногда называют *свободными переменными* формулы. Заметим, что формула может иметь одновременно параметр x и использовать (в другом месте) квантор $\forall x$. Как говорят в этом случае, одна и та же переменная имеет *свободные* и *связанные* вхождения. Свободное вхождение переменной — это такое вхождение, которое не входит в область действия одноимённого квантора. Если аккуратно определить эту область действия, несложно проверить, что параметры формулы — это как раз переменные, имеющие свободные вхождения.

Теперь мы хотим определить понятие формулы, истинной в данной интерпретации при данных значениях параметров. Технически проще считать, что всем индивидным переменным приписаны какие-то значения, а потом доказать, что переменные, не являющиеся параметрами, не влияют на истинность формулы.

Итак, пусть фиксирована сигнатура и некоторая интерпретация этой сигнатуры. *Оценкой* назовём отображение, которое ставит в соответствие каждой индивидной переменной некоторый элемент множества, являющегося носителем интерпретации. Этот элемент будем называть *значением переменной* при данной оценке.

Определим индуктивно *значение терма* t при данной оценке π, которое мы будем обозначать $[t](\pi)$.

- Для переменных оно уже определено.
- Если t является константой (нульместным функциональным символом), то $[t](\pi)$ не зависит от π и равно значению этой константы при данной интерпретации (напомним, в интерпретации с каждой константой сопоставляется некоторый элемент носителя).
- Если t имеет вид $f(t_1, \ldots, t_m)$, где f — функциональный символ валентности m, а $t_1, \ldots, t_m$ — термы, то $[t](\pi)$ есть $[f]([t_1](\pi), \ldots, [t_m](\pi))$, где $[f]$ есть функция, соответствующая символу f в нашей интерпретации, а $[t_i](\pi)$ есть значение терма t_i при оценке π.

Теперь можно определить *значение формулы* φ при данной оценке π в данной интерпретации, которое обозначается $[\varphi](\pi)$ и может быть равно **И** или **Л**; в первом случае формула называется *истинной*, во втором — *ложной*. Это определение также индуктивно:

- Значение атомарной формулы $A(t_1, \ldots, t_m)$ определяется как $[A]([t_1](\pi), \ldots, [t_m](\pi))$, где $[A]$ — предикат, соответствующий предикатному символу A в рассматриваемой интерпретации. Если формула представляет собой нульместный предикатный символ, то её значение не зависит от оценки и есть значение этого символа.

- $[\neg\varphi](\pi)$ определяется как $\neg[\varphi(\pi)]$, где $\neg$ понимается как операция в $\mathbb{B}$. Другими словами, формула $\neg\varphi$ истинна при оценке π тогда и только тогда, когда формула φ ложна при этой оценке.

- $[\varphi \wedge \psi](\pi)$ определяется как $[\varphi](\pi) \wedge [\psi](\pi)$, где $\wedge$ в правой части понимается как операция в $\mathbb{B}$. (Другими словами, формула $(\varphi \wedge \psi)$ истинна при оценке π тогда и только тогда, когда обе формулы φ и ψ истинны при этой оценке.) Аналогичным образом $[\varphi \vee \psi](\pi)$ определяется как $[\varphi](\pi) \vee [\psi](\pi)$, а $[\varphi \to \psi](\pi)$ — как $[\varphi](\pi) \to [\psi](\pi)$.

- Формула $\forall\xi\,\varphi$ истинна на оценке π тогда и только тогда, когда формула φ истинна на любой оценке π', которая совпадает с π всюду, кроме значения переменной ξ (которое в оценке π' может быть любым). Другими словами, если обозначить через $\pi + (\xi \mapsto m)$ оценку, при которой значение переменной ξ равно m, а остальные переменные принимают те же значения, что и в оценке π, то

  $$[\forall\xi\,\varphi](\pi) = \bigwedge_{m \in M} [\varphi](\pi + (\xi \mapsto m)).$$

  (В правой части стоит бесконечная конъюнкция, которая истинна, если все её члены истинны.)

- Формула $\exists\xi\,\varphi$ истинна на оценке π тогда и только тогда, когда формула φ истинна на некоторой оценке π', которая совпадает с π всюду, кроме значения переменной ξ (которое в оценке π' может быть любым). Другими словами,

$$[\forall\xi\,\varphi](\pi) = \bigvee_{m\in M} [\varphi](\pi + (\xi \mapsto m)).$$

(В правой части стоит бесконечная дизъюнкция, которая истинна, если хотя бы один из её членов истинен.)

Заметим, что в двух последних пунктах значение переменной ξ в оценке π не играет роли. Это позволяет легко доказать (индукцией по построению формулы) такое утверждение: если две оценки π_1 и π_2 придают одинаковые значения всем параметрам формулы φ, то $[\varphi](\pi_1) = [\varphi](\pi_2)$. Другими словами, истинность формулы определяется значениями её параметров.

45. Проведите это индуктивное рассуждение подробно.

46. Приведённые выше определения применимы к любой формуле, в том числе и к странной формуле $\forall y\, A(x)$. Какие у неё параметры? При каких значениях параметров она истинна? (Ответ: она имеет единственный параметр x и эквивалентна формуле $A(x)$.)

47. В каком случае будет истинна формула $\forall x\, \exists x\, A(x)$? Тот же вопрос для формулы $\exists x\, \forall x\, A(x)$. (Ответ: первая из этих формул эквивалентна формуле $\exists x\, A(x)$, а вторая — формуле $\forall x\, A(x)$.)

Формула называется *замкнутой*, если она не имеет параметров. Замкнутые формулы называют также *суждениями.* Как мы доказали, истинность замкнутой формулы определяется выбором интерпретации (и не зависит от значений переменных).

3.3. Выразимые предикаты

Пусть фиксирована некоторая сигнатура σ и её интерпретация с носителем M. Мы хотим определить понятие *выразимого* (с помощью формулы данной сигнатуры в данной интерпретации) k-местного предиката.

Выберем k переменных $x_1, \ldots, x_k$. Рассмотрим произвольную формулу φ, все параметры которой содержатся в списке $x_1, \ldots, x_k$. Истинность этой формулы зависит только от значений переменных $x_1, \ldots, x_k$. Тем самым возникает отображение $M^k \to \mathbb{B} = \{\mathbf{И}, \mathbf{Л}\}$, то есть некоторый k-местный предикат на M. Говорят, что этот предикат *выражается* формулой φ. Все предикаты, которые можно получить таким способом, называются *выразимыми*. (Ясно, что конкретный выбор списка переменных роли не играет.) Соответствующие им подмножества множества M^k (области истинности выразимых предикатов) также называют выразимыми.

48. Докажите, что пересечение, объединение и разность двух выразимых множеств являются выразимыми. Докажите, что проекция k-мерного выразимого множества вдоль одной из «осей координат» является $(k-1)$-мерным выразимым множеством.

Пример. Сигнатура содержит одноместный функциональный символ S и двуместный предикатный символ равенства $(=)$. Рассмотрим интерпретацию этой сигнатуры. В качестве носителя выберем натуральный ряд $\mathbb{N}$. Символ S будет обозначать функцию прибавления единицы (можно считать S сокращением от слова successor — последователь). Знак равенства интерпретируется как совпадение элементов.

Легко проверить, что одноместный предикат «быть нулём» выразим в этой интерпретации, несмотря на то, что константы для нуля в сигнатуре не предусмотрено. В самом деле, он выражается формулой

$$\neg\exists y(x = S(y))$$

с единственным параметром x.

Ещё проще выразить в этой сигнатуре двуместный предикат «быть больше на 2», при этом даже не нужны кванторы: $y = S(S(x))$.

Любопытно, что уже в такой простой ситуации можно сформулировать содержательную задачу: выразить предикат $y = x + N$, где N — большое число (скажем, миллиард), с помощью существенно более короткой формулы, чем $y = S(S(\ldots(S(x))\ldots))$. Как ни удивительно, это вполне возможно, и соответствующую формулу вполне можно уместить на листе бумаги.

49. Докажите, что предикат $y = x + N$ можно выразить формулой указанной сигнатуры, длина которой есть $O(\log N)$. (Указание. Если мы научились выражать $y = x + n$, можно выразить $y = x + 2n$ с помощью формулы

$$\exists z\,((z = x + n) \wedge (y = z + n))$$

(в которой через $z = x + n$ и $y = z + n$ обозначены соответствующие формулы). Это само по себе ничего не даёт, так как длина формулы увеличилась вдвое, но можно использовать такой трюк:

$$\exists z\,\forall u\,\forall v(((u = x \wedge v = z) \vee (u = z \wedge v = y)) \to (v = u + n)).$$

Далее можно воспользоваться записью числа N в двоичной системе счисления.)

Можно доказать, что в этой сигнатуре кванторы почти не увеличивают набор выразимых предикатов: всякий выразимый предикат будет выражаться бескванторной формулой (возможно, гораздо более длинной), если добавить к сигнатуре константу 0. Мы вернёмся к этому вопросу в разделе 3.6.

Чтобы привыкнуть к понятию выразимости, рассмотрим ещё один пример. Пусть сигнатура содержит предикат равенства и трёхместный предикат C. Рассмотрим интерпретацию, в которой носителем является множество точек плоскости, равенство интерпретируется как совпадение точек, а $C(x, y, z)$ означает, что точки x и y равноудалены от точки z. Оказывается, что этого предиката достаточно, чтобы выразить более или менее все традиционные понятия элементарной геометрии.

Как, например, записать, что три различные точки A, B, C лежат на одной прямой? Вот как: «не существует другой точки C', которая находилась бы на тех же расстояниях от A и B, что и точка C».

50. Напишите соответствующую формулу указанной сигнатуры.

Теперь легко выразить такое свойство четырёх точек A, B, C, D: «точки A и B различны, точки C и D различны и прямые AB и CD параллельны». В самом деле, надо написать, что нет точки, которая бы одновременно лежала на одной прямой с A и B, а также на одной прямой с C и D.

После этого можно выразить свойство четырёх точек «быть вершинами параллелограмма». Это позволяет переносить отрезок параллельно себе. После этого несложно выразить такое свойство: «расстояние AB равно расстоянию CD».

51. Запишите соответствующую формулу.

Аналогичным образом можно двигаться и дальше.

52. Выразите свойство $|OA| \leqslant |OB|$ трёх точек O, A, B. (Указание. Напишите, что все прямые, проходящие через A, пересекаются с окружностью радиуса OB с центром в O.)

53. Запишите в виде формулы: (**а**) равенство треугольников; (**б**) равенство углов; (**в**) свойство угла быть прямым.

54. Рассмотрим естественную интерпретацию сигнатуры $(=, <)$ на множестве целых чисел. Как выразить предикат $y = x + 1$?

55. Рассмотрим множество действительных чисел как интерпретацию сигнатуры $(=, +, y = x^2)$. Как выразить трёхместный предикат $xy = z$?

56. Рассмотрим множество целых положительных чисел как интерпретацию сигнатуры, содержащей равенство и двуместный предикат «x делит y». Выразить свойства «равняться единице» и «быть простым числом».

57. Рассмотрим плоскость как интерпретацию сигнатуры, содержащей предикат равенства (совпадение точек) и двуместный предикат «находиться на расстоянии 1». Выразить двуместные предикаты «находиться на расстоянии 2» и «находиться на расстоянии не более 2».

3.4. Выразимость в арифметике

Рассмотрим сигнатуру, имеющую два двуместных функциональных символа — сложение и умножение (как обычно, мы будем писать $x + y$ вместо $+(x, y)$ и т. д.) и двуместный предикатный символ равенства. Рассмотрим интерпретацию этой сигнатуры, носителем которой является множество $\mathbb{N}$ натуральных чисел, а сложение, умножение и равенство интерпретируются стандартным образом.

Выразимые с помощью формул этой сигнатуры предикаты называются *арифметическими* и играют в математической логике важную роль. Соответствующие множества также называются *арифметическими*. О них подробно рассказано в другой нашей книжке [5]; оказывается, что почти всякое множество, которое можно описать словами, является арифметическим.

58. Докажите, что существует множество натуральных чисел, не являющееся арифметическим. (Указание: семейство всех подмножеств множества $\mathbb{N}$ несчётно, а арифметических множеств счётное число.)

Для начала мы установим арифметичность довольно простых предикатов.

- Предикат $x \leqslant y$ является арифметическим. В самом деле, его можно записать как $\exists z\,(x + z = y)$.

- Предикаты $x = 0$ и $x = 1$ являются арифметическими. В самом деле, $x = 0$ тогда и только тогда, когда $x \leqslant y$ для любого y (а также когда $x + x = x$). А $x = 1$ тогда и только тогда, когда x представляет собой наименьшее число, отличное от нуля. (Можно также воспользоваться тем, что $y \cdot 1 = y$ при любом y.)

- Вообще для любого фиксированного числа c предикат $x = c$ является арифметическим. (Например, можно написать сумму из большого числа единиц.)

- Полезно такое общее наблюдение: если мы уже установили, что какой-то предикат является арифметическим, то в дальнейшей его можно использовать в формулах, как если бы он входил в сигнатуру, поскольку его всегда можно заменить на выражающую его формулу.

- Предикат $x|y$ (число x является делителем числа y), очевидно, арифметичен (формула $\exists z\,(xz = y)$).

- Предикат «x — простое число» арифметичен. В самом деле, число просто, если оно отлично от 1 и любой его делитель равен 1 или самому числу. Это сразу же записывается в виде формулы.

- Операции частного и остатка арифметичны (в том смысле, что трёхместные предикаты «q есть частное при делении a на b» и «r есть остаток при делении a на b» арифметичны. Например, первый из них записывается формулой $\exists r\,((a = bq + r) \land (r < b))$ (как мы уже говорили, использование арифметического предиката $(r < b)$ не создаёт проблем).

- Этот список можно продолжать: для многих предикатов их определение по существу уже является нужной формулой. Например, свойства «быть наибольшим общим делителем», «быть наименьшим общим кратным», «быть взаимно простыми» все относятся к этой категории.

- Предикат «быть степенью двойки» является арифметическим (хотя это и не столь очевидно, как в предыдущих примерах). В самом деле, это свойство можно переформулировать так: любой делитель либо равен единице, либо чётен.

Последнее из наших рассуждений годится для степеней тройки и вообще для степеней любого простого числа. Однако уже для степеней четвёрки оно не проходит, и, пожалуй, мы подошли к границе, где без некоторого общего метода не обойтись.

Два наиболее известных способа доказывать арифметичность основаны на возможности «кодирования» конечных множеств и последовательностей. Один восходит к Гёделю (так называемая β-функция Гёделя), второй изложен в книге «Теория формальных систем» [24]. Её написал Р. Смаллиан, известный также как автор популярных сборников «логических задач» и анекдотов. (Один из таких сборников имеет парадоксальное название «Как же называется эта книга?» [23].)

В некоторых отношениях метод Гёделя предпочтительней, и мы рассказываем о нём в книжке о вычислимых функциях [5], но сейчас для разнообразия рассмотрим другой способ. Зафиксируем взаимно однозначное соответствие между натуральными числами и двоичными словами:

$$\begin{array}{cccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \ldots \\ \Lambda & 0 & 1 & 00 & 01 & 10 & 11 & 000 & 001 & \ldots \end{array}$$

Это соответствие задаётся так: чтобы получить слово, соответствующее числу n, надо записать $n+1$ в двоичной системе и удалить первую единицу. Например, нулю соответствует пустое слово Λ, числу 15 — слово 0000 и т. д. Теперь можно говорить об арифметичности предикатов, определённых на двоичных словах, имея в виду арифметичность соответствующих предикатов на $\mathbb{N}$.

- Предикат «слово x состоит из одних нулей» арифметичен. В самом деле, при переходе к числам ему соответствует предикат «$x + 1$ есть степень двойки», который (как мы видели) арифметичен.

- Предикат «слова x и y имеют одинаковую длину» арифметичен. В самом деле, это означает, что найдётся степень двойки c, для которой $c - 1 \leqslant x, y < 2c - 1$ (именно такой промежуток заполняют числа, которым соответствуют слова одной длины).

- Предикат «слово z является конкатенацией слов x и y» (проще говоря, z получается приписыванием y справа к слову x) арифметичен. В самом деле, его можно выразить так: найдётся слово y' из одних нулей, имеющее ту же длину, что и слово y, при этом $(z+1) = (x+1)(y'+1) + (y-y')$ (умножение на $y'+1$ соответствует дописыванию нулей, а добавление $y - y'$ заменяет нули на буквы слова y).

- Предикат «слово x является началом слова y» арифметичен. В самом деле, это означает, что существует слово t, при котором y есть конкатенация x и t.

- То же самое верно для предикатов «x есть конец слова y», «x есть подслово слова y» (последнее означает, что найдутся слова u и v, для которых y есть конкатенация u, x и v; конкатенация трёх слов выразима через конкатенацию двух).

- Существует арифметический трёхместный предикат $S(x,a,b)$ с такими свойствами: (**а**) для любых a и b множество $S_{ab} = \{x \mid S(x,a,b)\}$ конечно; (**б**) среди множеств S_{ab} при различных парах a,b встречаются все конечные множества. Например, в качестве такого предиката можно взять «axa есть подслово слова b» (здесь axa есть конкатенация трёх слов: a, x и снова a).

  В самом деле, ясно, что слово x не длиннее слова b, и потому множество S_{ab} всегда конечно. С другой стороны, пусть имеется некоторое конечное множество слов $x_1,\ldots,x_n$. Положим $a = 100\ldots001$, где число нулей больше длины любого из слов x_i, и $b = ax_1ax_2a\ldots ax_na$.

Последнее утверждение не упоминает явно о словах, и больше они нам не понадобятся: достаточно знать, что конечные множества натуральных чисел можно кодировать парами натуральных чисел в описанном смысле.

Теперь мы можем выразить, что число x является степенью числа 4, следующим образом: существует конечное множество U, которое содержит число x и обладает таким свойством: всякий элемент $u \in U$ либо равен 1, либо делится на 4 и $u/4$ также принадлежит U. Теперь надо везде заменить множество U на его код u_1, u_2, а утверждение $x \in U$ на $S(x, u_1, u_2)$, где S — построенный нами кодирующий предикат.

Немного сложнее выразить двуместный предикат $x = 4^k$. Здесь нам хотелось бы сказать так: существует последовательность $x_0, x_1, \ldots, x_k$, для которой $x_0 = 1$, каждый следующий член вчетверо больше предыдущего ($x_{i+1} = 4x_i$) и $x_k = x$. Как научиться говорить о последовательностях, если мы умеем говорить о множествах? Вспомним, что в терминах теории множеств последовательность есть функция, определённая на начальном отрезке натурального ряда, то есть конечное множество пар $\{\langle 0, x_0\rangle, \langle 1, x_1\rangle, \ldots, \langle k, x_k\rangle\}$. Пары можно кодировать числами. Например, можно считать кодом пары $\langle x, y\rangle$ число $c = (x+y)^2+x$, поскольку по нему арифметически восстанавливается $x + y$ (как наибольшее число, квадрат которого не превосходит c), а затем x и y. Теперь конечное множество пар можно заменить конечным множеством их кодов, которое в свою очередь можно закодировать парой чисел.

59. Проведите это рассуждение подробно.

60. Покажите, что двуместный предикат «x есть n-ое по порядку простое число» арифметичен.

3.5. Невыразимые предикаты: автоморфизмы

Мы видели, как можно доказать выразимость некоторых свойств. Сейчас мы покажем, каким образом можно доказывать невыразимость.

Начнём с такого примера. Пусть сигнатура содержит двуместный предикат равенства ($=$) и двуместную операцию сложения ($+$). Рассмотрим её интерпретацию, носителем которой являются целые числа, а равенство и сложение интерпретируются стандартным образом. Оказывается, что предикат $x > y$ не является выразимым.

Причина очевидна: с точки зрения сложения целые числа устроены симметрично, положительные ничем не отличаются от отрицательных. Если мы изменим знак у всех переменных, входящих в формулу, то её истинность не может измениться. Но при этом $x > y$ заменится на $x < y$, и потому это свойство не является выразимым.

Формально говоря, надо доказывать по индукции такое свойство: если формула φ указанной сигнатуры истинна при оценке π, то она истинна и при оценке π', в которой значения всех переменных меняют знак. (Подробно мы объясним это в общей ситуации дальше.)

Сформулируем общую схему, которой следует это рассуждение. Пусть имеется некоторая сигнатура σ и интерпретация этой сигнатуры, носителем которой является множество M. Взаимно однозначное отображение $\alpha\colon M \to M$ называется *автоморфизмом* интерпретации, если все функции и предикаты, входящие в интерпретацию, устойчивы относительно α. При этом k-местный предикат P называется *устойчивым* относительно α, если

$$P(\alpha(m_1), \ldots, \alpha(m_k)) \Leftrightarrow P(m_1, \ldots, m_k)$$

для любых элементов $m_1, \ldots, m_k \in M$. Аналогичным образом k-местная функция f называется *устойчивой* относительно α, если

$$f(\alpha(m_1), \ldots, \alpha(m_k)) = \alpha(f(m_1, \ldots, m_k)).$$

Это определение обобщает стандартное определение автоморфизма для групп, колец, полей и т. д.

Теорема 27. Предикат, выразимый в данной интерпретации, устойчив относительно её автоморфизмов.

$\lhd$ Проведём доказательство этого (достаточно очевидного) утверждения формально.

Пусть π — некоторая оценка, то есть отображение, ставящее в соответствие всем индивидным переменным некоторые элементы носителя. Через $\alpha \circ \pi$ обозначим оценку, которая получится, если к значению каждой переменной применить отображение α; другими словами, $\alpha \circ \pi(\xi) = \alpha(\pi(\xi))$ для любой переменной ξ.

Первый шаг состоит в том, чтобы индукцией по построению терма t доказать такое утверждение: значение терма t при оценке $\alpha \circ \pi$ получается применением α к значению терма t при оценке π:

$$[t](\alpha \circ \pi) = \alpha([t](\pi)).$$

Для переменных это очевидно, а шаг индукции использует устойчивость всех функций интерпретации относительно α.

Теперь индукцией по построению формулы φ легко доказать такое утверждение:

$$[\varphi](\alpha \circ \pi) = [\varphi](\pi).$$

Мы не будем выписывать эту проверку; скажем лишь, что взаимная однозначность α используется, когда мы разбираем случай кванторов. (В самом деле, если с одной стороны изоморфизма берётся какой-то объект, то взаимная однозначность позволяет взять соответствующий ему объект с другой стороны изоморфизма.) $\triangleright$

Теорема 27 позволяет доказать невыразимость какого-то предиката, предъявив автоморфизм интерпретации, относительно которого интересующий нас предикат неустойчив. Вот несколько примеров:

- $(\mathbb{Z}, =, <)$ Сигнатура содержит равенство и отношение порядка. Интерпретация: целые числа. Невыразимый предикат: $x = 0$. Автоморфизм: $x \mapsto x + 1$.

- $(\mathbb{Q}, =, <, +)$ Сигнатура содержит равенство, отношение порядка и операцию сложения. Интерпретация: рациональные числа. Невыразимый предикат: $x = 1$. Автоморфизм: $x \mapsto 2x$.

  Заметим, что сложение позволяет выразить предикат $x = 0$. Кроме того, отметим, что вместо рациональных чисел можно взять действительные (но не целые, так как в этом случае единица описывается как наименьшее число, большее нуля).

- $(\mathbb{R}, =, <, 0, 1)$ Сигнатура содержит равенство, порядок и константы 0 и 1. Интерпретация: действительные числа. Невыразимый предикат: $x = 1/2$. (Автоморфизм упорядоченного множества $\mathbb{R}$, сохраняющий 0 и 1, но не $1/2$, построить легко.)

- $(\mathbb{R}, =, +, 0, 1)$ Сигнатура содержит равенство, сложение, константы 0 и 1. Интерпретация: действительные числа. Одноместный предикат $x = \gamma$ выразим для рациональных γ и невыразим для иррациональных γ.

  В самом деле, выразимость для рациональных γ очевидна. Невыразимость для иррациональных γ следует из того, что для любых двух иррациональных γ_1 и γ_2 существует автоморфизм, переводящий γ_1 в γ_2. (В самом деле, рассмотрим $\mathbb{R}$ как бесконечномерное векторное пространство над $\mathbb{Q}$. Векторы $1, \gamma_1$ линейно независимы и потому их можно дополнить до базиса Гамеля (подробности смотри в книжке по теории множеств [6]). Сделаем то же самое с векторами $1, \gamma_2$. Получатся равномощные базисы, после чего мы берём $\mathbb{Q}$-линейный оператор, переводящий 1 в 1 и γ_1 в γ_2.)

- $(\mathbb{C}, =, +, \times, 0, 1)$ В сигнатуру входят предикат равенства, операции сложения и умножения, а также константы 0 и 1. Интерпретация: комплексные числа. Предикат $x = \gamma$, где γ — некоторое комплексное число, выразим для рациональных γ и невыразим для иррациональных γ.

  В самом деле, если γ иррационально, то оно может быть алгебраическим или трансцендентным. В первом случае рассмотрим многочлен из $\mathbb{Q}[x]$ минимальной степени, обращающийся в 0 в точке γ; по предположению он имеет степень больше 1 и потому имеет другой корень γ'. В алгебре доказывается (с использованием трансфинитной индукции или леммы Цорна, а также базисов трансцендентности), что существует автоморфизм $\mathbb{C}$ над $\mathbb{Q}$, переводящий γ в γ'.

В случае трансцендентного γ мы используем такой факт: для любых трансцендентных $\gamma_1, \gamma_2 \in \mathbb{C}$ существует автоморфизм поля $\mathbb{C}$ над $\mathbb{Q}$, который переводит γ_1 в γ_2.

Отметим, что для поля $\mathbb{R}$ вместо $\mathbb{C}$ такое рассуждение не проходит, так как это поле не имеет нетривиальных автоморфизмов. (Отношение порядка выразимо: положительные числа суть квадраты, поэтому любой автоморфизм сохраняет порядок. Поскольку автоморфизм оставляет на месте все рациональные числа, он должен быть тождественным.)

В этом случае предикат $x = \gamma$ выразим тогда и только тогда, когда γ — алгебраическое число. Это легко следует из теоремы Тарского – Зайденберга (раздел 3.8, с. 135).

61. Покажите, что предикат $y = x + 1$ невыразим в интерпретации $(\mathbb{Z}, =, f)$, где f — одноместная функция $x \mapsto (x + 2)$.

62. Покажите, что предикат $x = 2$ невыразим в множестве целых положительных чисел с предикатами равенства и «x делит y».

3.6. Невыразимые предикаты: элиминация кванторов

При всей простоте метод доказательства невыразимости с помощью автоморфизмов страдает очевидным недостатком: очень часто требуемого автоморфизма нет. Например, натуральные числа с операцией прибавления единицы вообще не допускают никакого нетривиального автоморфизма. (Тем не менее там выразимо очень немногое, как мы вскоре увидим.) Целые числа с операцией прибавления единицы допускают автоморфизмы (сдвиги), но эти автоморфизмы не позволяют доказать, что отношение порядка невыразимо (поскольку оно устойчиво относительно сдвигов).

Более прямой метод доказательства состоит в том, что мы предъявляем некоторый класс $\mathcal{E}$ предикатов, который содержит все выразимые предикаты и не содержит интересующего нас предиката. При этом мы доказываем, что $\mathcal{E}$ содержит все выразимые предикаты, таким способом: проверяем, что $\mathcal{E}$ содержит все предикаты, выразимые атомарными формулами, а также замкнут относительно логических операций (объединение, пересечение, дополнение) и операции проекции (соответствующей навешиванию квантора существования; квантор всеобщности выражается через квантор существования). Часто класс $\mathcal{E}$ совпадает с классом всех предикатов, выразимых бескванторными формулами (иногда надо расширить сигнатуру), и потому этот метод называют методом «элиминации кванторов». (Это краткое описание, возможно, станет яснее из приводимых далее примеров.)

Начнём с такого примера. Пусть сигнатура содержит равенство, одноместную функцию S (прибавление единицы) и константу 0. Носителем интерпретации будет множество $\mathbb{Z}$ целых чисел, символы сигнатуры интерпретируются естественным образом. В этой ситуации изоморфизмов не существует, так что предыдущий способ доказательства невыразимости здесь неприменим.

Тем не менее класс выразимых предикатов весьма ограничен: это предикаты, выразимые бескванторными формулами. Будем называть две формулы (рассматриваемой нами сигнатуры) эквивалентными (в данной интерпретации), если они выражают один и тот же предикат, то есть истинны при одних и тех же значениях переменных.

Теорема 28. Для всякой формулы рассматриваемой нами сигнатуры существует эквивалентная ей бескванторная формула.

◁ Будем доказывать индукцией по построению (или, если угодно, по длине) формулы φ существование эквивалентной ей в $(\mathbb{Z}, =, S, 0)$ бескванторной формулы. Для удобства (чтобы рассматривать один случай, а не два) будем считать, что наша формула может содержать только кванторы существования, но не всеобщности. Это законно, так как формулы $\forall\xi\,\psi$ и $\neg\exists\xi\,\neg\psi$ эквивалентны.

Случай, когда φ есть атомарная формула, очевиден — она и так бескванторная. Если φ является конъюнкцией, дизъюнкцией или импликацией двух частей, достаточно заменить каждую часть на эквивалентную бескванторную (что можно сделать по предположению индукции).

Единственный содержательный случай — когда формула φ начинается с квантора существования, то есть имеет вид $\exists x\tau$ (пусть под квантором стоит переменная x). Формула τ имеет (возможно) и другие параметры, скажем, $x_1, \ldots, x_n$. Чтобы подчеркнуть это, обычно вместо τ пишут $\tau(x, x_1, \ldots, x_n)$. Нам надо найти бескванторную формулу нашей сигнатуры, эквивалентную формуле

$$\exists x\,\tau(x, x_1, \ldots, x_n).$$

Формула $\tau(x, x_1, \ldots, x_n)$ представляет собой булеву комбинацию атомарных формул. Посмотрим на те атомарные формулы, которые содержат переменную x. Атомарная формула представляет собой равенство двух термов $S(S(\ldots(S(u))\ldots)) = S(S(\ldots(S(v))\ldots))$; здесь u и v — либо переменные, либо константа 0. Если переменная x входит и в левую, и в правую часть, то (в этой интерпретации) такая атомарная формула либо всегда истинна, либо всегда ложна, и её можно заменить на какую-нибудь тождественно истинную или тождественно ложную формулу, не содержащую x. После этого останутся атомарные формулы, которые можно записать как

$$\begin{aligned} &x = t_1,\\ &x = t_2,\\ &\dots\dots\\ &x = t_k. \end{aligned}$$

Здесь t_i — либо целая константа, либо выражение вида $x_j + c$, где x_j — какая-то другая переменная, а c — целое число. Мы позволили себе слегка отступить от канонов, разрешив прибавлять и вычитать целые константы вместо того, чтобы применять функцию S в левой и правой частях равенства. Ясно, что это не меняет класса выразимых формул, зато позволяет оставить x в левой части, а константу перенести в правую.

Теперь сравним формулу

$$\varphi = \exists x\, \tau(x, x_1, \dots, x_n)$$

с формулой

$$\tau(t_1, x_1, \dots, x_n) \vee \tau(t_2, x_1, \dots, x_n) \vee \dots \vee \tau(t_k, x_1, \dots, x_n),$$

которую мы будет обозначать φ'. Формула φ' представляет собой дизъюнкцию формул, полученных в результате подстановки различных t_i вместо x в бескванторную формулу $\tau(x, x_1, \dots, x_n)$. (После подстановки можно вернуться к обычному виду записи формулы, заменив прибавление констант на нужное количество применений функции S с той или другой стороны равенства.)

Очевидно, что если для каких-то значений переменных $x_1, \dots, x_n$ формула φ' истинна, то для этих значений $x_1, \dots, x_n$ истинна и формула φ. В самом деле, если истинен i-й член дизъюнкции, то в формуле φ в качестве x можно взять значение выражения t_i.

Верно ли обратное? Не обязательно. Вполне возможно, что тот x, который существует и делает формулу φ истинной, отличается от всех t_i. Но мы пропустили по существу только один случай — все такие x в некотором смысле одинаковы, так как они делают все атомарные формулы, содержащие x, ложными, поэтому всё равно, какой из таких x выбрать. Отметим также, что хотя бы один такой x найдётся, поскольку $\mathbb{Z}$ бесконечно, а выражений t_i лишь конечное число.

Обозначим через φ'' формулу, которая получится из τ заменой всех атомарных формул, содержащих x, на тождественно ложные формулы. Сказанное выше объясняет, почему формула φ эквивалентна дизъюнкции $\varphi' \vee \varphi''$. Мы достигли цели — нашли бескванторную формулу, эквивалентную формуле φ. $\triangleright$

Легко понять, что отношение порядка $x > y$ не выражается бескванторной формулой нашей сигнатуры, поскольку такая формула может включать лишь атомарные формулы вида $x = y + c$ и для неё случай, когда y сильно больше x, неотличим от случая, когда y сильно меньше x. Тем самым мы доказали (чего нельзя было сделать методом автоморфизмов), что отношение $x > y$ невыразимо (в данной интерпретации данной сигнатуры).

Немного более сложное рассуждение понадобится, если добавить к сигнатуре отношение порядка.

Теорема 29. Всякая формула в $(\mathbb{Z}, =, <, S)$ (где S — функция прибавления единицы) эквивалентна некоторой бескванторной формуле. (Как говорят, $(\mathbb{Z}, =, <, S)$ *допускает элиминацию кванторов.*)

$\triangleleft$ Полностью утверждение теоремы звучит так: для всякой формулы сигнатуры, содержащей равенство, порядок и символ S, найдётся бескванторная формула той же сигнатуры, которая эквивалентна ей в интерпретации, где носителем является $\mathbb{Z}$, а символы сигнатуры интерпретируются естественным образом. (В дальнейшем мы будем опускать такие пояснения.)

Доказательство следует прежней схеме. Правда, теперь атомарных формул больше — помимо формул $x = t_i$ у нас будут формулы $x < t_i$. Поэтому нельзя рассчитывать на то, что все значения x, не встречающиеся среди $\{t_1, \ldots, t_k\}$, ведут себя одинаково, и наш приём с выделением случая, когда все равенства ложны, более не проходит.

Как же быть? Для данных значений $x_1, \ldots, x_n$ числа $t_1, \ldots, t_k$ делят числовую ось (точнее, множество $\mathbb{Z}$ целых чисел) на промежутки, и для выяснения истинности формулы φ нам надо попробовать (помимо всех t_i) хотя бы по одному числу из каждого промежутка. Это будет гарантировано, если мы напишем дизъюнкцию, в которую, помимо всех формул $\tau(t_i, x_1, \ldots, x_n)$, войдут также формулы $\tau(t_i + 1, x_1, \ldots, x_n)$ и $\tau(t_i - 1, x_1, \ldots, x_n)$. Это позволяет нам обойтись без формулы φ'' и благополучно завершить доказательство. $\triangleright$

63. Проверьте, что добавление константы 0 к этой сигнатуре не препятствует элиминации кванторов.

Что будет, если мы из этой сигнатуры удалим функцию S? Легко понять, что класс выразимых множеств не изменится, так как $y = S(x)$ можно выразить как «y является наименьшим элементом, бóльшим x». Однако при этом мы использовали кванторы, так что для $(\mathbb{Z}, =, <)$ элиминация кванторов невозможна.

64. Убедитесь, что в самом деле формула $y = S(x)$ не эквивалентна никакой бескванторной формуле этой сигнатуры.

Часто такой переход приходится выполнять в обратном направлении: у нас есть некоторая ситуация, в которой элиминация кванторов не проходит. Мы обходим эту трудность, добавив некоторые выразимые предикаты и функции в нашу сигнатуру, после чего элиминация кванторов удаётся. В этом случае мы получаем описание всех выразимых предикатов (предикат выразим, если он записывается бескванторной формулой расширенной сигнатуры). Мы встретимся с такой ситуацией дальше, говоря об арифметике Пресбургера (раздел 3.7).

В некоторых случаях рассуждение упрощается, если использовать приведение бескванторной формулы к дизъюнктивной нормальной форме. Вот один из таких примеров.

Теорема 30. Всякая формула в $(\mathbb{Q}, =, <)$ эквивалентна некоторой бескванторной формуле.

$\lhd$ Как всегда, достаточно рассмотреть случай формулы вида

$$\exists x\, \tau(x, x_1, \ldots, x_n),$$

где $\tau(x, x_1, \ldots, x_n)$ — бескванторная формула. Формулу τ можно считать формулой в дизъюнктивной нормальной форме (теорема 4, с. 19). Напомним, это означает, что τ представляет собой дизъюнкцию конъюнкций, а каждая конъюнкция соединяет несколько литералов (атомарных формул или их отрицаний).

В данном случае можно избавится от отрицаний, заменив $\neg(x = y)$ на $((x < y) \vee (x > y))$, а $\neg(x < y)$ — на $((x = y) \vee (x > y))$. После этого надо воспользоваться дистрибутивностью и вновь придти к дизъюнктивной нормальной форме — с большим числом членов, но уже без отрицаний.

Теперь надо воспользоваться тем, что квантор существования (который есть «бесконечная дизъюнкция») можно переставлять с дизъюнкцией. Точнее говоря, мы пользуемся тем, что формулы

$$\exists x\, (\tau_1 \vee \tau_2)$$

и

$$\exists x\, \tau_1 \vee \exists x\, \tau_2$$

эквивалентны. (Белый или чёрный единорог существует тогда и только тогда, когда существует белый единорог или существует чёрный единорог.) Это обстоятельство позволяет заменить формулу

$$\exists x\, (\tau_1 \vee \tau_2 \vee \ldots \vee \tau_n)$$

на

$$\exists x\, \tau_1 \vee \exists x\, \tau_2 \vee \ldots \vee \exists x\, \tau_n$$

и дальше разбираться с каждой из формул поодиночке.

Итак, нам осталось преобразовать к бескванторному виду формулу

$$\exists x\,(\rho_1 \wedge \rho_2 \wedge \ldots \wedge \rho_k),$$

где каждая из формул ρ_i соединяет какие-то две переменные знаком $=$ или $<$ (напомним, от отрицаний мы уже избавились).

Некоторые из формул ρ_i не содержат переменной x. Тогда их можно вынести за квантор: если x не является параметром формулы α, то формулы

$$\exists x\,(\alpha \wedge \beta) \quad \text{и} \quad \alpha \wedge \exists x\,\beta$$

эквивалентны (если α истинно для некоторых значений параметров, то в обеих формулах его можно опустить; если α ложно, то обе формулы ложны при этих значениях параметров).

Вынеся такие формулы, можно считать, что под квантором остались лишь формулы вида $x < x_i$, $x = x_i$ и $x > x_i$, сравнивающие переменную x с какими-то другими переменными. Если там есть хоть одно равенство, то квантор существования вырождается — его можно удалить вместе с переменной x, заменив её на ту переменную, которой она равна. Например, формулу $\exists x\,((x = y) \wedge \wedge A(x))$ можно заменить на $A(y)$.

Итак, остался случай, когда переменная x встречается лишь в неравенствах. Другими словами, нас спрашивают, найдётся ли значение x, большее каких-то переменных и меньшее каких-то других. Если все ограничения на x одного знака (только снизу или только сверху), то такое значение x существует при любых значениях других переменных (поскольку в множестве $\mathbb{Q}$ нет ни наибольшего, ни наименьшего элементов). Что делать, если есть ограничения разных знаков? Пусть наша формула, например, имеет вид

$$\exists x\,((x > a) \wedge (x > b) \wedge (x < c) \wedge (x < d)).$$

Как записать условия на a, b, c, d, при которых это верно, не используя кванторов? Надо написать такую формулу:

$$(a < c) \wedge (a < d) \wedge (b < c) \wedge (b < d).$$

Мы хотим написать, что наибольшая из нижних границ меньше наименьшей из верхних, но поскольку заранее неизвестно, какая будет наибольшей и какая наименьшей, мы пишем, что любая нижняя граница меньше любой верхней. Поскольку множество $\mathbb{Q}$ является плотным (между любыми двумя элементами найдётся третий), то эта формула равносильна исходной.

Так, постепенно сводя дело ко всё более простым случаям, мы завершили рассуждение. $\triangleright$

Заметим, что в этом доказательстве из свойств рациональных чисел мы использовали лишь отсутствие наибольшего и наименьшего элемента и плотность. Поэтому все наши преобразования остаются эквивалентными для любого упорядоченного множества с такими свойствами, а не только для $\mathbb{Q}$. Применив эти преобразования к замкнутой формуле (формуле без параметров), мы получим или тождественно истинную формулу, или тождественно ложную (только надо добавить в язык константы для истины и лжи, чтобы не использовать фиктивных переменных, когда надо написать тождественно истинное или тождественно ложное выражение). Отсюда мы заключаем, что во всех плотных упорядоченных множествах без первого и последнего элемента справедливы одни и те же формулы нашей сигнатуры. Как говорят, все такие множества *элементарно эквивалентны* с точки зрения нашей сигнатуры, см. раздел 3.9. (Другое доказательство этого факта можно получить, используя теорему Левенгейма – Сколема о счётной подмодели и теорему об изоморфизме счётных плотных линейно упорядоченных множеств без первого и последнего элементов, см. раздел 3.11.)

В частности, мы доказали, что для рациональных и действительных чисел истинны одни и те же формулы сигнатуры $(=, <)$.

Ещё одним побочным продуктом нашего рассуждения (как и других рассуждений об элиминации кванторов) является способ выяснить, будет ли данная замкнутая формула истинной или ложной в рассматриваемой интерпретации. Для этого надо привести её к бескванторному виду и посмотреть, получится ли **И** или **Л**. Другими словами, элиминация кванторов устанавливает *разрешимость* элементарной теории рациональных чисел с отношениями равенства и порядка.

Элиминация кванторов остаётся возможной (и рассуждение даже немного упрощается), если рациональные (или действительные) числа рассматривать не только с равенством и порядком, но и со сложением и рациональными константами. В этом случае можно воспользоваться приведённой ранее схемой с конечным представительным набором термов. В самом деле, пусть x — переменная, которую (вместе с квантором существования по ней) мы хотим элиминировать. Все атомарные формулы, её содержащие, можно «разрешить» относительно x, получив некоторое количество формул вида $x = t_i$, $x > t_i$ и $x < t_i$, где t_i — линейные комбинации остальных переменных с рациональными коэффициентами. (Разрешение рациональных коэффициентов вместо целых ничего не меняет, так как можно привести всё к общему знаменателю и получить целые коэффициенты, затем перенести отрицательные коэффициенты в другую часть, а положительные заменить многократным сложением.)

Затем в качестве представительного набора надо взять набор, состоящий, во-первых, из всех t_i, во-вторых, из всех средних арифметических $(t_i + t_j)/2$, и, наконец, из выражений $t_i - 1$ и $t_i + 1$. Ясно, что как бы ни расположились точки t_i на числовой оси, этот набор захватит как минимум по одной точке из каждого промежутка (средние арифметические нужны для интервалов, а прибавление и вычитание единицы — для лучей по краям).

65. Провести это рассуждение подробно.

Возможность элиминации кванторов в только что рассмотренной ситуации ($\mathbb{Q}, =, <, +$, рациональные константы) имеет интересное геометрическое применение.

Теорема 31. Пусть единичный квадрат разрезан на несколько меньших квадратов. Тогда все они имеют рациональные стороны.

$\triangleleft$ Пусть дано такое разрезание с n меньшими квадратами. Напишем формулу с $3n$ параметрами (n из которых соответствуют размерам меньших квадратов, а $2n$ — координатам их левых верхних углов), которая говорит, что эти параметры действительно задают разрезание квадрата (квадраты содержатся внутри единичного, не имеют общих точек и всякая точка единичного квадрата покрывается хотя бы одним из меньших квадратов). Навесив кванторы существования по переменным, задающим координаты, получим формулу $F(x_1, \ldots, x_n)$ с параметрами $x_1, \ldots, x_n$, которая истинна, когда из квадратов размеров $x_1, \ldots, x_n$ можно составить единичный квадрат.

Элиминация кванторов позволяет считать, что формула F бескванторная, то есть представляет собой логическую комбинацию равенств и неравенств вида $c_1x_1 + \ldots + c_nx_n + c_0 = 0$ и $c_1x_1 + \ldots + c_nx_n + c_0 > 0$ с различными рациональными коэффициентами. Посмотрим на все выражения, стоящие в левой части таких равенств и неравенств. Подставим в них числа $\overline{x}_1, \ldots, \overline{x}_n$, соответствующие данному нам разрезанию. При этом получится истинная формула $F(\overline{x}_1, \ldots, \overline{x}_n)$, в которой некоторые из левых частей равенств и неравенств будут равны нулю, а другие нет. Временно забудем про те, которые не равны нулю, а равные нулю будем воспринимать как левые части уравнений с неизвестными $x_1, \ldots, x_n$ (с нулём в правой части) независимо от того, входили ли они в F как левые части уравнений или неравенств. Получится система уравнений, для которой числа $\overline{x}_1, \ldots, \overline{x}_n$ будут решениями. Если эти числа являются единственными её решениями, то они рациональны (например, потому, что правила Крамера для решения системы уравнений содержат отношения определителей с рациональными элементами). Покажем, что другого быть не может.

В самом деле, если решение не единственно, то есть целая прямая, проходящая через точку $\overline{x} = \langle \overline{x}_1, \ldots, \overline{x}_n \rangle$ и лежащая в множестве решений системы. Все точки прямой, достаточно близкие к $\overline{x}$, неотличимы от $\overline{x}$ с точки зрения формулы F и потому делают формулу F истинной. В самом деле, левые части, равные нулю в $\overline{x}$, равны нулю на всей прямой, а левые части, отличные от нуля в точке $\overline{x}$, сохраняют знак в некоторой окрестности этой точки. Пусть $\langle h_1, \ldots, h_n \rangle$ — направляющий вектор этой прямой. Тогда при всех достаточно малых значениях t из квадратов размеров

$$\overline{x}_1 + th_1, \overline{x}_2 + th_2, \ldots, \overline{x}_n + th_n$$

можно составить единичный квадрат. Но это невозможно. Чтобы убедиться в этом, достаточно оставить логику и вернуться к геометрии: площади этих квадратов в сумме должны равняться 1, но площадь каждого есть многочлен второй степени по t, и коэффициент при t^2 положителен, поэтому сумма таких многочленов не может тождественно равняться единице ни на каком интервале. $\triangleright$

Насколько существенна в этом рассуждении ссылка на возможность элиминации кванторов? В принципе можно было бы рассуждать так. Пусть дано разрезание квадрата. Посмотрим на конфигурацию, образуемую меньшими квадратами, и напишем равенства и неравенства на размеры частей, которые гарантируют, что в этой конфигурации нет щелей и перекрытий. (Далее продолжаем рассуждение как раньше.) Конечно, возникает вопрос: почему мы уверены, что такую систему уравнений и неравенств можно написать? Глядя на конкретную конфигурацию, это сделать легко, но как провести это рассуждение строго для общего случая, не вполне понятно.

Изложенные методы позволяют провести элиминацию кванторов и описать выразимые множества во многих ситуациях; несколько простых примеров такого рода предлагаются в качестве задач. Два более сложных примера (арифметика Пресбургера и теория сложения и умножения действительных чисел) разбираются в двух следующих разделах.

66. Описать выразимые предикаты, проведя элиминацию кванторов (и расширив сигнатуру, если нужно) для (**а**) $(M, =)$, где M — произвольное бесконечное множество; (**б**) $(\mathbb{Q}, =, +)$; (**в**) $(\mathbb{Q}, =, S)$, где S — операция прибавления единицы; (**г**) $(\mathbb{N}, =, S)$, где S — операция прибавления единицы; (**д**) $(\mathbb{N}, =, S, P)$, где S — операция прибавления единицы, а P — одноместный предикат «быть степенью двойки».

3.7. Арифметика Пресбургера

В этом разделе мы описываем выразимые множества в $(\mathbb{Z}, =, <, +, 0, 1)$. Отметим сразу же, что с такой сигнатурой элиминация кванторов невозможна. В самом деле, формула $\exists y\,(x = y + y)$, истинная для чётных x, не эквивалентна никакой бескванторной формуле. Поэтому нам нужно, прежде чем проводить элиминацию кванторов, расширить сигнатуру. Приведённый пример формулы подсказывает, какое расширение нам необходимо. Рассмотрим счётное семейство двуместных предикатных символов $\equiv_2, \equiv_3, \equiv_4, \ldots$ Символ $\equiv_c$ будет интерпретироваться как равенство по модулю c. Другими словами, формула $x \equiv_c y$ будет истинна в нашей интерпретации, если x сравнимо с y по модулю c (остатки по модулю c равны; $x - y$ кратно c).

Важно иметь в виду, что индекс c в $x \equiv_c y$ не является переменной: у нас не трёхместный предикат, а счётное семейство двуместных предикатов.

Такое расширение не меняет класса выразимых предикатов, поскольку, например, $x \equiv_3 y$ можно выразить как $\exists z\,(x = y+z+z+z)$. Зато после этого всякая формула эквивалентна бескванторной, как показывает следующая теорема (называемая теоремой об элиминации кванторов *в арифметике Пресбургера*).

Теорема 32. В $\langle \mathbb{Z}, =, <, +, 0, 1, \equiv_2, \equiv_3, \ldots \rangle$ выполнима элиминация кванторов.

$\lhd$ Мы будем применять метод, опробованный в предыдущем разделе: выбор представительного множества термов (после некоторых преобразований формулы).

Напомним, как это делается. Мы хотим доказать, что всякая формула эквивалентна бескванторной. Рассуждая по индукции, мы должны лишь проверить, что всякая формула вида

$$\exists x\, \tau(x, x_1, \ldots, x_n),$$

где $\tau(x, x_1, \ldots, x_n)$ обозначает бескванторную формулу, все переменные которой содержатся среди $x, x_1, \ldots, x_n$, эквивалентна некоторой бескванторной формуле (с теми же переменными, не считая x).

Посмотрим, какие атомарные формулы, содержащие переменную x, входят в τ. Перенося члены в одну сторону, эти атомарные формулы можно записать в одном из трёх видов: $L(x, x_1, \ldots, x_n) = 0$, $L(x, x_1, \ldots, x_n) > 0$ или $L(x, x_1, \ldots, x_n) \equiv_c 0$, где $L(x, x_1, \ldots, x_n)$ представляет собой линейную комбинацию переменных $x, x_1, \ldots, x_n$ с целыми коэффициентами и целочисленным свободным членом. (В отличие от ситуации в $\mathbb{Q}$, здесь нельзя делить на коэффициент при x.) Перенося x в левую часть, а всё остальное — в правую, получаем соотношение одного из четырёх видов:

$$\begin{aligned}
&kx = l(x_1, \ldots, x_n);\\
&kx < l(x_1, \ldots, x_n);\\
&kx > l(x_1, \ldots, x_n);\\
&kx \equiv_c l(x_1, \ldots, x_n),
\end{aligned}$$

где k — положительное целое число (разное для разных атомарных формул), а l — линейная комбинация переменных $x_1, \ldots, x_n$ с целыми коэффициентами и свободным членом.

Как мы говорили, коэффициенты в левой части (а также, разумеется, правые части) у разных атомарных формул разные. Однако мы можем их унифицировать, перейдя к общему кратному. В самом деле, неравенства и равенства можно умножать на число, сравнения — тоже, если модуль сравнения (индекс c в $\equiv_c$) умножить на то же самое число. Поэтому можно считать, что наша формула имеет вид $\exists x\, \tau(kx, x_1, \ldots, x_n)$, понимая под этим, что x появляется только в левых частях и везде с коэффициентом k. Такую формулу можно переписать как

$$\exists y\, (\tau(y, x_1, \ldots, x_n) \wedge (y \equiv_k 0)).$$

Таким образом, без ограничения общности можно считать, что $k = 1$, поскольку новая формула имеет тот же самый вид

$$\exists y\, \tau(y, x_1, \ldots, x_n),$$

что и исходная, но уже безо всякого коэффициента при y (и с модифицированной формулой τ). Пусть $l_1, \ldots, l_k$ — выражения, стоящие в правых частях равенств, неравенств и сравнений с левой частью y.

Мы хотим, как и в предыдущем разделе, указать представительный набор значений $Y_1, \ldots, Y_N$. Каждое из Y_i представляет собой линейную комбинацию переменных $x_1, \ldots, x_n$ с целыми коэффициентами и свободным членом. «Представительность» означает, что если для каких-то $x_1, \ldots, x_n$ найдётся y, для которого $\tau(y, x_1, \ldots, x_n)$, то такой y можно найти и среди значений $Y_1, \ldots, Y_N$ (при тех же $x_1, \ldots, x_n$).

Чтобы указать представительный набор, разделим все атомарные формулы в τ, содержащие y, на два типа — сравнения по модулю и остальные (равенства и неравенства). Посмотрим, по каким модулям проводятся сравнения. Пусть D — общее кратное всех этих модулей. В этом случае изменение значения переменной y на величину, кратную D, не влияет на результаты сравнений. Теперь возьмём все выражения, встречающиеся в правых частях равенств или неравенств, и будем прибавлять к ним всевозможные целые числа из отрезка от $-D$ до D. Это и будет представительный набор. Другими словами, в представительный набор входят все выражения $l + c$, где l — одна из правых частей равенств или неравенств, содержащих y в левой части, а c — целое число, не превосходящее D по абсолютной величине.

Покажем, что полученный набор действительно будет представительным. Пусть при данных $x_1, \ldots, x_n$ найдётся некоторое y, для которого $\tau(y, x_1, \ldots, x_n)$. Посмотрим, какие значения принимают правые части равенств и неравенств при данных $x_1, \ldots, x_n$. Если значение y попало в объединение D-окрестностей этих значений, то доказывать нечего. Если же нет, начнём смещать y, двигаясь шагами размера D в направлении какой-то точки из этого объединения. Миновать мы её не можем (ширина окрестности равна $2D$, а размер шага равен D), поэтому в какой-то момент мы впервые попадём в это объединение. Обозначим эту точку (первую попавшую в объединение) через y'. Тогда y' при подстановке в τ даёт те же самые результаты, что и y. В самом деле, для сравнений это гарантировано, потому что сдвиг кратен модулю сравнений. Но это верно и для равенств и неравенств, поскольку на предыдущем шаге мы были вне D-окрестности всех правых частей и потому не могли перейти с одной стороны на другую.

Таким образом, среди представительного набора есть значение (а именно, y'), удовлетворяющее формуле τ, что и требовалось доказать. $\triangleright$

Итак, мы получили ответ на интересующий нас вопрос: выразимые в арифметике Пресбургера предикаты — это предикаты, выразимые бескванторными формулами, содержащими целые константы, сложение, равенство, отношение порядка и сравнения по любым фиксированным модулям.

3.8. Теорема Тарского – Зайденберга

В этом разделе мы покажем, что в элементарной теории действительных чисел со сложением и умножением выполнима элиминация кванторов. Более точно, рассмотрим сигнатуру, содержащую предикаты $=$ и $<$, константы 0 и 1, а также операции сложения и умножения. Рассмотрим интерпретацию этой сигнатуры, носителем которой является множество действительных чисел, а предикаты и операции понимаются естественным образом. Тогда для каждой формулы существует эквивалентная (выражающая тот же предикат) бескванторная формула. Это утверждение называют *теоремой Тарского – Зайденберга*.

Прежде чем доказывать эту теорему, сделаем несколько комментариев:

- Свойство $x < y$ можно выразить как «существует ненулевое z, для которого $x + z^2 = y$». Таким образом, класс выразимых предикатов не изменится, если мы удалим символ $<$ из сигнатуры. (Но предикатов, выразимых бескванторными формулами, станет меньше: свойство $x > 0$, как легко понять, не эквивалентно никакой бескванторной формуле, содержащей константы, сложение, умножение и равенство.)

- Бескванторную формулу нашей сигнатуры можно привести к дизъюнктивной нормальной форме, после чего она превратится в совокупность систем уравнений вида $P = 0$ и неравенств вида $P > 0$. В самом деле, в конъюнкциях могут ещё быть отрицания, то есть отношения $\ne$ и $\geqslant$, но можно разбить $P \ne 0$ на $(P < 0) \vee (P > 0)$, а $P \geqslant 0$ на $(P = 0) \vee (P > 0)$, после чего воспользоваться дистрибутивностью.

- Подмножества $\mathbb{R}^n$, задаваемые уравнениями вида $P = 0$ и неравенствами вида $P > 0$ (где P — произвольный многочлен от нескольких переменных с целыми коэффициентами), а также множества, получаемые из них любым числом операций объединения и пересечения, называют *полуалгебраическими*. Предыдущее замечание показывает, что всякая бескванторная формула задаёт полуалгебраическое множество. (Полуалгебраические множества являются обобщениями *алгебраических* множеств, задаваемых системами полиномиальных уравнений.)

- Из теоремы Тарского – Зайденберга вытекает, что проекция полуалгебраического множества $A \subset \mathbb{R}^n$ вдоль одной из осей является полуалгебраическим подмножеством пространства $\mathbb{R}^{n-1}$. В самом деле, переход к проекции приводит к добавлению квантора существования, который можно затем элиминировать. (Утверждение о полуалгебраичности проекции полуалгебраического множества по существу равносильно теореме Тарского – Зайденберга, так как элиминация квантора существования является единственным нетривиальным шагом в доказательстве этой теоремы.)

- Пример: равенство $x^2 + px + q = 0$ задаёт полуалгебраическое (и даже алгебраическое) множество троек $\langle x, p, q\rangle$. Какова будет его проекция вдоль оси x на плоскость p, q? Как учат в школе, это будет множество $p^2 - 4q \geqslant 0$, которое оказывается полуалгебраическим в полном согласии с теоремой Тарского – Зайденберга. Про аналогичные критерии разрешимости уравнений большей степени в школе не учат, но теорема Тарского – Зайденберга гарантирует их существование.

- Как и во всех предыдущих случаях элиминации кванторов, преобразование формулы в бескванторную формулу эффективно (выполняется некоторым алгоритмом). В частности, этот алгоритм можно применить к замкнутой формуле (формуле без параметров). Тогда получится бескванторная формула без параметров (формально говоря, там могут быть параметры, от значений которых ничего не зависит, но их можно заменить, скажем, нулями).

Истинность такой формулы можно алгоритмически проверить. Тем самым можно алгоритмически проверить истинность любого утверждения о действительных числах, выраженного формулой нашей сигнатуры. Как говорят, элементарная теория действительных чисел со сложением и умножением *разрешима*.

- Большинство утверждений школьного курса геометрии с помощью метода координат можно записать как утверждения о действительных числах в нашей сигнатуре. (Исключение, впрочем, составляют утверждения, где речь идёт не о треугольниках и четырёхугольниках, а о n-угольниках без указания конкретного n). Записав теоремы в виде замкнутых формул нашей сигнатуры, можно алгоритмически проверить их истинность. Тем самым мы получаем общий метод доказательства большинства теорем школьной геометрии (впрочем, он имеет лишь теоретическое значение, так как алгоритм работает необозримо долго на сколько-нибудь сложных формулах).

Теорема 33 (Тарского – Зайденберга). Для всякой формулы сигнатуры $(=, <, 0, 1, +, \times)$ существует бескванторная формула, задающая тот же предикат на множестве действительных чисел.

$\lhd$ (Это доказательство предложено Ан. А. Мучником.) Как обычно, достаточно рассматривать формулу с единственным квантором существования, то есть формулу φ вида

$$\exists x\, B(x, x_1, \ldots, x_n),$$

где $B(x, x_1, \ldots, x_n)$ — бескванторная формула, включающая в себя только переменные из числа $x, x_1, \ldots, x_n$. Надо доказать, что найдётся эквивалентная формуле φ бескванторная формула $B'(x_1, \ldots, x_n)$.

Посмотрим на атомарные формулы, входящие в формулу B. Перенося все переменные в одну часть, можно считать, что каждая атомарная формула имеет вид $P(x, x_1, \ldots, x_n) = 0$ или $P(x, x_1, \ldots, x_n) > 0$, где P — некоторый многочлен с целыми коэффициентами от переменных $x, x_1, \ldots, x_n$. Кольцо многочленов с целыми коэффициентами от переменных $x, x_1, \ldots, x_n$ обозначается через $\mathbb{Z}[x, x_1, \ldots, x_n]$. Группировка членов по степеням переменной x даёт многочлен от x, коэффициенты которого представляют собой многочлены от $x_1, \ldots, x_n$. Символически это записывается так:

$$\mathbb{Z}[x, x_1, \ldots, x_n] = (\mathbb{Z}[x_1, \ldots, x_n])[x]$$

(многочлены от $n + 1$ переменных можно рассматривать как многочлены от одной переменной, коэффициенты которых лежат в кольце многочленов от n переменных).

При фиксации значений переменных $x_1, \ldots, x_n$ входящие в B многочлены превращаются в многочлены от одной переменной x с числовыми коэффициентами. Формула φ выражает тогда какое-то свойство этих многочленов и может быть истинной или ложной. Нам надо доказать, что те $\langle x_1, \ldots, x_n \rangle$, при которых она истинна, образуют полуалгебраическое множество.

Для этого введём понятие *диаграммы* семейства многочленов. Пусть $Q_1(x), \ldots, Q_k(x)$ — многочлены от x с действительными коэффициентами. Диаграммой набора $Q_1, \ldots, Q_k$ будет таблица, которая строится так. Возьмём все корни всех многочленов Q_i (не считая нулевых многочленов) и расположим их в порядке возрастания. Получим некоторый набор чисел $\alpha_1 < \alpha_2 < \ldots < \alpha_m$. Эти числа разбивают числовую ось на $m + 1$ промежутков (два луча и $m - 1$ интервалов), на каждом из которых знаки всех Q_i постоянны. Составим таблицу, в которой будет k строк (по одной для каждого из многочленов) и $2m + 1$ столбцов, соответствующих m корням и $m + 1$ промежуткам (столбцы идут в порядке возрастания, так что корни чередуются с промежутками). В каждой ячейке таблицы запишем один из трёх символов $+$, $-$ или 0 в зависимости от того, является ли многочлен положительным, отрицательным или нулевым на соответствующем промежутке (или в соответствующем корне).

Пример. Выпишем диаграмму для системы многочленов x^2-1, x, 0. Корнями здесь будут числа -1, 0, 1, так что столбцы соответствуют четырём промежуткам и трём разделяющим их корням.

		$\langle -1\rangle$		$\langle 0\rangle$		$\langle 1\rangle$	
x^2-1	$+$	0	$-$	$-$	$-$	0	$+$
x	$-$	$-$	$-$	0	$+$	$+$	$+$
0	0	0	0	0	0	0	0

Отметим, что значения корней не являются частью диаграммы, так что, например, система многочленов x^2-4, $2x-1$, 0 имеет точно такую же диаграмму.

Если ни один из многочленов не имеет корней, то они сохраняют знак на всей прямой, и диаграмма состоит из единственного столбца, в котором записаны все эти знаки.

Теперь рассмотрим набор многочленов $Q_1, \ldots, Q_k \in \mathbb{Z}[x, x_1, \ldots, x_n]$. При фиксированных значениях переменных $x_1, \ldots, x_n$ мы получаем набор многочленов от одной переменной с действительными коэффициентами и можем построить его диаграмму. Эта диаграмма будет зависеть от выбора значений $x_1, \ldots, x_n$. Число строк в диаграмме равно k, а ширина её зависит от числа различных корней и может меняться, однако во всех случаях не превосходит $2N+1$, где N — сумма степеней всех многочленов (рассматриваются степени по x, то есть степени соответствующих многочленов от x с коэффициентами в $\mathbb{Z}[x_1, \ldots, x_n]$).

Таким образом, число возможных диаграмм конечно, и пространство $\mathbb{R}^n$ возможных значений переменных $x_1, \ldots, x_n$ разбивается на конечное число частей: каждая часть соответствует одному из возможных значений диаграммы.

Для доказательства теоремы Тарского – Зайденберга достаточно доказать, что эти части будут полуалгебраическими множествами. В самом деле, если в качестве многочленов $Q_1, \ldots, Q_k$ взять многочлены, входящие в формулу $B(x, x_1, \ldots, x_n)$, то область истинности формулы

$$\varphi = \exists x\, B(x, x_1, \ldots, x_n)$$

будет объединением нескольких частей соответствующего разбиения. В самом деле, если мы двигаем точку $\langle x_1, \ldots, x_n \rangle$ в пределах одной части разбиения, то диаграмма не меняется, значит, и истинность формулы φ не меняется (по диаграмме можно определить истинность формулы, перепробовав значения x, соответствующие всем столбцам).

Итак, нам осталось доказать, что для любого набора многочленов $Q_1, \ldots, Q_k \in \mathbb{Z}[x, x_1, \ldots, x_n]$ части пространства $\mathbb{R}^n$, соответствующие различным значениям диаграммы, являются полуалгебраическими множествами. Начнём с такого очевидного наблюдения: если это верно для какого-то набора $Q_1, \ldots, Q_k$, то это останется верным и для любого меньшего набора. В самом деле, диаграмму меньшего семейства многочленов можно получить из диаграммы большего семейства: выкидывая многочлен, надо выбросить соответствующую строку, а также столбцы, которые соответствовали корням этого многочлена (если они не были корнями других многочленов). При выбрасывании столбца два окружающих его столбца сливаются в один.

Поэтому мы имеем право для удобства расширить данный нам набор многочленов и доказывать полуалгебраичность частей для расширенного набора. Расширение будет состоять в замыкании относительно некоторых операций, которые мы сейчас опишем.

Напомним ещё раз, что мы рассматриваем семейство многочленов из $\mathbb{Z}[x, x_1, \ldots, x_n]$, которые разложены по степеням x, то есть записаны как многочлены от x с коэффициентами в $\mathbb{Z}[x_1, \ldots, x_k]$. Рассмотрим следующие операции:

- отбрасывание старшего члена (с наибольшей степенью переменной x); эта операция понижает степень (по x) на единицу;
- взятие старшего коэффициента (коэффициента при наибольшей степени переменной x); эта операция понижает степень (по x) до нуля;
- дифференцирование по x; эта операция понижает степень (по x) на единицу;
- взятие модифицированного остатка при делении одного многочлена на другой.

Говоря о «модифицированном остатке», мы имеем в виду следующее. При делении «уголком» многочлена A на многочлен B с остатком нам неоднократно приходится делить на старший коэффициент многочлена B. Поэтому в общем случае коэффициенты частного и остатка представляют собой дроби, в знаменателях которых стоят некоторые степени старшего коэффициента многочлена B.

Тем самым при вычислении остатка от деления A на B мы выходим за пределы кольца $\mathbb{Z}[x, x_1, \ldots, x_n]$. Этого не случится, если старший коэффициент многочлена B равен единице. Но в общем случае мы должны принять какие-то меры, если хотим оставаться в указанном кольце. Меры эти состоят в следующем: прежде чем делить A на B, мы *умножаем A на старший коэффициент многочлена B в достаточно большой степени*. Если вспомнить процедуру деления уголком, легко сообразить, что достаточно взять степень $a - b + 1$, где a и b — степени многочленов A и B (по переменной x). Например, при $a = b$ требуется всего один шаг деления, и достаточно умножить A на старший коэффициент многочлена B в первой степени.

Итак, операция модифицированного остатка применима к любым двум многочленам $A, B \in (\mathbb{Z}[x_1, \ldots, x_n])[x]$ степеней a и b (по x) и даёт третий многочлен этого кольца, который есть остаток от деления $A\beta^{a-b+1}$ на B

(здесь β — старший коэффициент многочлена B). Заметим, что степень этого многочлена меньше степени многочлена B. Мы будем предполагать, что $a \geqslant b$ (иначе остаток совпадает с A и деление не даёт ничего нового). Таким образом, результат этой операции имеет меньшую степень, чем оба операнда.

Заметим, что определение модифицированного остатка имеет смысл для многочленов с коэффициентами из произвольного кольца (не только $\mathbb{Z}[x_1, \ldots, x_n]$).

Лемма 1. Для всякого конечного множества F многочленов из $(\mathbb{Z}[x_1, \ldots, x_n])[x]$ существует его конечное расширение, замкнутое относительно указанных четырёх операций.

Это утверждение верно для любого кольца коэффициентов и почти очевидно следует из того, что степень результата операции меньше степени (любого) операнда. Более формально рассуждать надо так. Рассмотрим выражения, составленные из элементов F с помощью четырёх указанных операций. Глубина такого выражения не превосходит максимальной степени многочленов из F, поскольку каждая операция уменьшает степень. Поэтому таких выражений конечное число, и их множество очевидным образом замкнуто относительно указанных операций. Лемма 1 доказана.

Доказанная лемма позволяет без ограничения общности считать, что данное нам конечное множество многочленов замкнуто относительно четырёх указанных выше операций.

Лемма 2. Пусть F — конечное множество многочленов из $(\mathbb{Z}[x_1, \ldots, x_n])[x]$, замкнутое относительно перечисленных операций. Пусть F_0 — его часть, состоящая только из многочленов степени 0 по x (они представляют собой многочлены из $\mathbb{Z}[x_1, \ldots, x_n]$). Тогда диаграмма множества F при данных $x_1, \ldots, x_n$ полностью определяется диаграммой множества F_0 при тех же $x_1, \ldots, x_n$.

Заметим, что диаграмма множества F_0 имеет всего один столбец, указывающий, какие из многочленов положительны, какие отрицательны и какие равны нулю при данных $x_1, \ldots, x_n$. Поэтому различным вариантам диаграммы для множества F_0 соответствуют полуалгебраические подмножества в $\mathbb{R}^n$, и из леммы 2 следует, что те же самые множества составят искомое разбиение для полной системы F. Таким образом, нам осталось лишь доказать лемму 2.

Будем добавлять в множество F_0 многочлены по одному, в порядке возрастания (неубывания) их степеней, пока не получим всё множество F. Достаточно показать, что на каждом шаге диаграмма расширенного множества (с новым многочленом) может быть однозначно восстановлена по диаграмме предыдущего множества. Мы сейчас опишем, как это делается.

Пусть добавляется многочлен $P \in (\mathbb{Z}[x_1, \ldots, x_n])[x]$, при этом многочлены всех меньших степеней из F уже есть в диаграмме. В силу замкнутости F старший коэффициент многочлена P содержится в F и, имея меньшую (нулевую) степень, уже представлен в диаграмме. (Соответствующая строка состоит из одинаковых знаков, так как он не зависит от x.) Если там стоят нули, то (при данных $x_1, \ldots, x_n$) старший коэффициент равен нулю, и многочлен P совпадает с многочленом, получающимся при отбрасывании старшего члена. Этот многочлен тоже есть в F и в диаграмме, так что надо лишь продублировать соответствующую строку.

Итак, достаточно рассмотреть случай, когда старший коэффициент многочлена P (при данных $x_1, \ldots, x_n$) не равен нулю. Пополнение диаграммы включает в себя два шага: сначала мы должны определить знаки многочлена P в точках (корнях), уже входящих в диаграмму. Затем надо пополнить диаграмму корнями многочлена P (при этом число столбцов в ней увеличится).

Как найти знак многочлена P в одной из старых точек? По определению диаграммы в этой точке (обозначим её α) один из старых многочленов равен нулю. Пусть Q — такой многочлен. Можно считать, что старший коэффициент Q (как многочлена от x) отличен от нуля при данных $x_1, \ldots, x_n$. Если это не так, заменим Q на многочлен, получающийся отбрасыванием старшего члена. Мы знаем, что множество F замкнуто относительно четырёх операций и что все многочлены из F, имеющие меньшую степень, уже входят в диаграмму. Поэтому вся необходимая информация для отбора подходящего Q у нас есть.

Кроме того, по тем же причинам нам известен знак старшего коэффициента многочлена Q. Применим операцию модифицированного деления с остатком к P и Q:

$$\beta^s P = (\text{частное}) \cdot Q + R$$

(здесь β — старший коэффициент многочлена Q). Подставим в это равенство число α. При этом Q обратится в нуль, так как α является корнем Q по построению. Многочлен R входит в диаграмму в силу наших предположений, так что его знак в точке α нам известен, как и знак β. Тем самым можно найти знак $P(\alpha)$.

Итак, мы определили знак нового многочлена в старых корнях. Покажем, что этого достаточно, чтобы предсказать, на каких участках диаграммы появятся новые корни (многочлена P). При этом нам пригодится (пока что не использованная) операция дифференцирования.

Если в двух соседних старых корнях α_1, α_2 многочлен P имеет один и тот же знак (скажем, положителен), то между ними нет нового корня. В самом деле, если бы на интервале (α_1, α_2) многочлен P обращался в нуль, то минимум многочлена P на $[\alpha_1, \alpha_2]$ достигался бы в некоторой внутренней точке, в которой производная P' равнялась бы нулю. Но производная P' входит в множество F и представлена в диаграмме, так что тогда α_1 и α_2 не были бы соседними корнями диаграммы.

Если в одной из точек α_1 и α_2 многочлен P обращается в нуль, то на интервале (α_1, α_2) он корней иметь не может (по теореме Ролля такой корень повлёк бы за собой корень производной).

Наконец, если $P(\alpha_1)$ и $P(\alpha_2)$ имеют разные знаки, то по теореме о промежуточном значении многочлен P имеет на интервале (α_1, α_2) хотя бы один корень. При этом по уже понятным нам причинам (теорема Ролля) двух корней он иметь не может. Это позволяет вставить столбец для этого корня в диаграмму. При этом соответствующий интервал диаграммы разобьётся на два, которые будут отличаться лишь в строке для многочлена P.

Осталось провести аналогичное рассуждение для лучей, стоящих с края диаграммы. Поведение многочлена P на бесконечности определяется его старшим коэффициентом (который, напомним, не равен нулю — сейчас мы впервые используем это предположение). Поэтому если P стремится, скажем, к $+\infty$ при $x \to +\infty$, а значение P в самом правом корне было отрицательным, то на этом луче появляется новый корень (только один по теореме Ролля). Если же значение P в са́мом правом корне равно нулю или имеет тот же знак, что и старший коэффициент, то мы повторяем рассуждение из предыдущего абзаца и убеждаемся, что корней P на правом луче нет. Аналогично определяется и поведение P слева от са́мого левого корня.

На этом доказательство леммы 2, а с ней и теоремы Тарского – Зайденбрега, завершается. $\triangleright$

67. Докажите, что множество троек $\langle p, q, r\rangle$, при которых многочлен $x^3 + px^2 + q + r$ имеет ровно два положительных корня, является полуалгебраическим.

Подобного рода задачи рассматривались в алгебре ещё в прошлом веке (число перемен знака, правило Штурма и др.).

68. Докажите, что предикат $x = \alpha$, где α — некоторое действительное число, выразим тогда и только тогда, когда α является алгебраическим (мы отмечали это на с. 109).

Разобравшись с действительными числами, можно перейти к комплексным. На самом деле (как часто бывает) здесь ситуация проще.

На комплексных числах нет естественного отношения порядка, поэтому рассмотрим сигнатуру $(=, 0, 1, +, \times)$.

Будем, как всегда, считать две формулы эквивалентными, если они истинны при одних и тех же значениях параметров (в естественной интерпретации с носителем $\mathbb{C}$).

Теорема 34 (элиминация кванторов в поле комплексных чисел). Всякая формула этой сигнатуры эквивалентна бескванторной.

$\triangleleft$ Эта теорема имеет много разных доказательств, но после доказательства теоремы Тарского – Зайденберга нам проще всего модифицировать его.

Теперь в диаграммах будут стоять не знаки $-, 0, +$, а только знаки 0 и $\neq 0$ (поскольку порядка на $\mathbb{C}$ нет). По той же причине мы не можем упорядочить корни, так что диаграмма будет состоять из неупорядоченных столбцов, соответствующих корням, и одного столбца, соответствующего дополнению к множеству корней (в котором будут стоять знаки $\neq 0$ для всех многочленов, кроме нулевых). Говоря о неупорядоченных столбцах, мы имеем в виду, что не различаем диаграммы, отличающиеся лишь порядком столбцов.

Основной шаг в доказательстве теоремы Тарского – Зайденберга (и единственный, использовавший свойства порядка на действительных числах) состоял в пополнении диаграммы новым многочленом. Что будет с ним теперь?

Как и раньше, мы можем определить, в каких старых корнях новый многочлен равен нулю. Более того, мы можем определить кратность этих нулей, так как знаем всё необходимое про его производные (которые уже включены в диаграмму). Поэтому основная теорема алгебры говорит нам, сколько будет новых корней (заметим, что все новые корни имеют кратность 1, так как иначе они были бы корнями производной и не были бы новыми). Поскольку порядка на корнях нет, больше никакой информации нам и не нужно. $\triangleright$

69. Провести доказательство элиминации кванторов в поле $\mathbb{C}$, не использующее диаграмм (это можно сделать, начав с приведения бескванторной формулы к дизъюнктивной нормальной форме, а затем применяя разные соображения из алгебры о наибольшем общем делителе многочленов). Для теоремы Тарского – Зайденберга это несколько сложнее; рассуждение такого рода приведено в книжке Энгелера [32].

70. Докажите, что множество тех четвёрок комплексных чисел $\langle p, q, r, s\rangle$, при которых многочлены $z^2 + pz + q = 0$ и $z^2 + rz + s = 0$ имеют общий корень, задаётся бескванторной формулой. Найти эту формулу.

Задача 70 хорошо знакома алгебраистам. Ответ в ней можно записать в виде $R(p, q, r, s) = 0$, где R — многочлен, называемый *результантом* и равный определителю матрицы

$$\begin{vmatrix} 1 & p & q & 0 \\ 0 & 1 & p & q \\ 1 & r & s & 0 \\ 0 & 1 & r & s \end{vmatrix}$$

71. Докажите, что множество всех пар комплексных чисел $\langle p, q\rangle$, при которых многочлен $z^3 + pz + q$ имеет хотя бы один кратный корень, задаётся бескванторной формулой. Найти эту формулу. Как выглядит аналогичная формула для многочлена $z^2 + pz + q$?

(Ответ к задаче 71 тоже хорошо известен в алгебре; соответствующий многочлен называется *дискриминантом.*)

72. Обобщить утверждение предыдущей задачи на многочлены произвольной степени со старшим коэффициентом 1 и найти выражение дискриминанта в виде определителя.

3.9. Элементарная эквивалентность

Пока что мы в основном использовали технику элиминации кванторов для какой-то одной интерпретации (формула заменялась на бескванторную, которая эквивалентна исходной в данной интерпретации). Однако, как упоминалось на с. 117, этот метод позволяет сравнивать различные интерпретации. Мы приведём несколько примеров такого рода.

Начнём с определения. Пусть фиксирована некоторая сигнатура σ. Две интерпретации этой сигнатуры называются *элементарно эквивалентными*, если в них истинны одни и те же замкнутые формулы этой сигнатуры.

Легко доказать, что изоморфные интерпретации будут элементарно эквивалентны — надо только дать формальное определение изоморфизма для двух интерпретаций данной сигнатуры.

Пусть M_1 и M_2 — две интерпретации сигнатуры σ. Биекция (взаимно однозначное отображение) $\alpha\colon M_1 \to$ $\to M_2$ называется *изоморфизмом* этих интерпретаций, если она сохраняет все функции и предикаты сигнатуры. Это означает, что если P_1 и P_2 — два k-местных предиката в M_1 и M_2, соответствующих одному предикатному символу сигнатуры, то

$$P_1(a_1,\ldots,a_k) \Leftrightarrow P_2(\alpha(a_1),\ldots,\alpha(a_k))$$

для всех $a_1,\ldots,a_k \in M_1$. Аналогичное условие для функций: если k-местные функции f_1 и f_2 соответствуют одному функциональному символу, то

$$\alpha(f_1(a_1,\ldots,a_k)) = f_2(\alpha(a_1),\ldots,\alpha(a_k))$$

для всех $a_1,\ldots,a_k \in M_1$.

Две интерпретации называются *изоморфными*, если между ними существует изоморфизм.

Легко понять, что это определение обобщает обычные определения изоморфизма для групп, колец, упорядоченных множеств и т. д.

73. Докажите, что тождественное отображение есть изоморфизм. Докажите, что отображение, обратное изоморфизму, есть изоморфизм. Докажите, что композиция двух изоморфизмов есть изоморфизм. (Отсюда следует, что отношение изоморфности есть отношение эквивалентности на интерпретациях данной сигнатуры.)

Теперь можно сформулировать и доказать обещанное утверждение:

Теорема 35. Изоморфные интерпретации элементарно эквивалентны.

$\lhd$ Естественно доказывать это утверждение по индукции. Для этого его надо обобщить на произвольные формулы (не только замкнутые). Вот это обобщение: пусть $\alpha\colon M_1 \to M_2$ — изоморфизм, а F — произвольная формула нашей сигнатуры. Тогда она истинна в M_1 при оценке π тогда и только тогда, когда она истинна в M_2 при оценке $\alpha \circ \pi$.

Обычно истинность формулы F в интерпретации M обозначают как $M \vDash F$. Если формула имеет параметры $x_1, \ldots, x_n$, её часто обозначают $F(x_1, \ldots, x_n)$; при этом запись $M \vDash F(m_1, \ldots, m_n)$ (где $m_i \in M$) означает, что формула F истинна при оценке, которая ставит в соответствие параметру x_i значение m_i. После всех этих приготовлений доказываемое по индукции утверждение можно записать так:

$$M_1 \vDash F(a_1, \ldots, a_n) \Leftrightarrow M_2 \vDash F(\alpha(a_1), \ldots, \alpha(a_n))$$

для любой формулы $F(x_1, \ldots, x_n)$ и для любых элементов $a_1, \ldots, a_n \in M_1$.

После такого обобщения доказательство по индукции становится очевидным. $\triangleright$

74. В каком месте индуктивного рассуждения существенно, что α — взаимно однозначное соответствие? (Ответ: сюръективность α используется, когда мы рассматриваем формулу, начинающуюся с квантора существования, и из её истинности в M_2 выводим истинность в M_1. Инъективность α не используется, но она автоматически следует из определения изоморфизма, если сигнатура содержит равенство и интерпретации нормальны, то есть равенство интерпретируется как совпадение элементов.)

75. Рассуждение, использованное при доказательстве теоремы 35, нам по существу уже встречалось. Где?

Изоморфные интерпретации — это по существу одна и та же интерпретация, только её элементы названы по-разному. Интересны скорее примеры, когда интерпретации не изоморфны, но тем не менее элементарно эквивалентны. Один такой пример мы уже коротко обсуждали раньше, сформулируем его более подробно.

Теорема 36. Естественные интерпретации сигнатуры $(=, <, +, 0, 1)$ в множестве рациональных и действительных чисел элементарно эквивалентны.

$\lhd$ Для начала заметим, что эти интерпретации не изоморфны (поскольку мощности различны). Однако формулы этой сигнатуры допускают, как мы видели на с. 118, элиминацию кванторов. При этом получающаяся формула будет эквивалентна исходной в обеих интерпретациях. Начав с замкнутой формулы, мы получим бескванторную формулу без переменных (или с фиктивными переменными, от значений которых ничего не зависит, тогда вместо них можно подставить, скажем, нули). Эта формула будет содержать только рациональные константы и потому будет одинаково истинной в $\mathbb{R}$ и в $\mathbb{Q}$. $\rhd$

Заметим, что при уменьшении сигнатуры элементарная эквивалентность сохраняется (по очевидным причинам), так что из теоремы 36 очевидно следует, что $\mathbb{R}$ и $\mathbb{Q}$ элементарно эквивалентны как упорядоченные множества (этот факт мы отмечали на с. 117).

В этом примере элементарно эквивалентные, но не изоморфные структуры имеют различную мощность. В следующем примере это уже не так.

Теорема 37. Упорядоченные множества $\mathbb{Z}$ и $\mathbb{Z}+\mathbb{Z}$ (второе состоит из двух копий множества $\mathbb{Z}$, причём все элементы первой копии считаются меньшими всех элементов второй копии) элементарно эквивалентны как интерпретации сигнатуры $(=,<)$.

$\lhd$ Здесь также можно применить элиминацию кванторов, только надо добавить одноместные функции взятия последующего и предыдущего элементов. После этого надо заметить, что стандартная процедура элиминации кванторов (см. доказательство теоремы 29) состоит из преобразований, сохраняющих эквивалентность в обеих интерпретациях. $\rhd$

76. Можно ли построить счётную интерпретацию сигнатуры $(=,<)$, в которой равенство интерпретируется как совпадение элементов (такие интерпретации называют *нормальными*), элементарно эквивалентную множеству $\mathbb{Q}$, но не изоморфную ему? Тот же вопрос для множества неотрицательных рациональных чисел. Почему существенна нормальность интерпретации?

77. Существует ли упорядоченное множество, элементарно эквивалентное упорядоченному множеству $\mathbb{R}$, но имеющее бо́льшую мощность?

78. Существуют ли два несчётных неизоморфных элементарно эквивалентных упорядоченных множества одинаковой мощности?

79. Будут ли упорядоченные множества $\mathbb{Z}$ и $\mathbb{Z} \times \mathbb{Z}$ (пары целых чисел; сравниваются сначала вторые компоненты пар, а при их равенстве — первые) изоморфны? элементарно эквивалентны?

80. Будет ли упорядоченное множество $\mathbb{N}+\mathbb{N}$ элементарно эквивалентно $\mathbb{N}$? Будет ли $\mathbb{N}+\mathbb{Z}$ элементарно эквивалентно $\mathbb{N}$?

Рассуждение, использованное при доказательстве теоремы Тарского – Зайденберга, также можно приспособить для доказательства элементарной эквивалентности. Сейчас мы рассмотрим более простой случай алгебраически замкнутых полей, соответствующий элиминации кванторов в $\mathbb{C}$; к вещественному случаю мы вернёмся на с. 226.

Поле называется *алгебраически замкнутым*, если всякий многочлен, отличный от константы, имеет в нём хотя бы один корень. (Отсюда легко следует, что любой многочлен разлагается на линейные множители.) *Характеристикой* поля называют минимальное число слагаемых в сумме вида $1 + 1 + \ldots + 1$, при котором она обращается в нуль. Если никакая сумма такого вида не равна нулю, то поле называют полем *характеристики* 0.

В алгебраически замкнутых полях характеристики 0 справедливы все обычные свойства многочленов с комплексными коэффициентами. В частности, корень является кратным тогда и только тогда, когда он будет корнем производной, сумма корней с учётом кратности равна степени многочлена и т. д. Это позволяет заметить, что все преобразования, которые выполнялись при элиминации кванторов, являются эквивалентными в произвольных алгебраически замкнутых полях характеристики 0. Тем самым мы получаем такую теорему:

Теорема 38 (о полноте теории алгебраически замкнутых полей характеристики нуль). Любые два алгебраически замкнутых поля характеристики 0 элементарно эквивалентны.

(Название этой теоремы станет понятным, когда мы будем говорить о полных теориях.)

81. Покажите, что любые два алгебраически замкнутых поля одной и той же конечной характеристики элементарно эквивалентны.

Теорему 38 можно несколько усилить. Для этого нам понадобится понятие «элементарного расширения».

Пусть фиксирована сигнатура σ и две интерпретации этой сигнатуры с носителями M_1 и M_2. Пусть при этом $M_1 \subset M_2$ и интерпретации предикатных и функциональных символов в M_1 и M_2 согласованы, то есть на аргументах из M_1 символы интерпретируются одинаково. (Заметим, что отсюда следует замкнутость M_1 относительно сигнатурных операций.) В этом случае M_1 иногда называют *подструктурой* в M_2, а M_2 — *расширением* M_1.

Например, если мы рассматриваем группы как интерпретации сигнатуры $(=, \times, 1, \text{обращение})$, то подструктуры — это подгруппы.

82. Почему здесь важно, что операция обращения включена в сигнатуру?

Интерпретацию M_2 называют *элементарным расширением* её подструктуры M_1, если выполнено такое свойство: для всякой (не обязательно замкнутой формулы) F и для всякой оценки π со значениями в M_1 формула F истинна в M_1 на этой оценке тогда и только тогда, когда она истинна в M_2 на той же оценке.

В частности, если формула замкнута (не содержит параметров), то её истинность не зависит от оценки и мы получаем, что M_1 и M_2 элементарно эквивалентны.

83. Пусть сигнатура содержит константы для всех элементов интерпретации M_1, которая является подструктурой интерпретации M_2. Покажите, что если интерпретации M_1 и M_2 элементарно эквивалентны, то M_2 является элементарным расширением M_1.

Нам понадобится такой пример: пусть имеется поле k_1 и его расширение k_2. Мы будем рассматривать поля k_1 и k_2 как две интерпретации сигнатуры $(=, +, \times, 0, 1)$. Пусть имеется некоторая система полиномиальных уравнений с несколькими переменными с коэффициентами из k_1. Тогда утверждение о том, что она имеет решение, записывается в виде формулы (содержащей кванторы существования по переменным и конъюнкцию уравнений; коэффициенты многочленов являются параметрами этой формулы). Поэтому если k_2 является элементарным расширением k_1, то всякая система уравнений с коэффициентами в k_1, имеющая решение в k_2, имеет решение и в k_1.

Теорема 39. Пусть k_1 — подполе поля k_2, причём оба они алгебраически замкнуты и имеют характеристику 0. Тогда k_2 (как интерпретация указанной сигнатуры) является элементарным расширением интерпретации k_1.

$\triangleleft$ В самом деле, элиминация кванторов преобразует любую формулу (с параметрами или без) в эквивалентную ей бескванторную, причём эквивалентность имеет место в обоих полях. А для бескванторной формулы её истинность при оценке со значениями в k_1 никак не может зависеть от того, внутри какого поля эта истинность вычисляется. $\triangleright$

Эту теорему называют теоремой о модельной полноте теории алгебраически замкнутых полей характеристики нуль. Из неё с учётом замечания перед её формулировкой вытекает такой хорошо известный алгебраистам факт:

Теорема 40 (Гильберта о нулях). Всякая система полиномиальных уравнений с коэффициентами в алгебраически замкнутом поле характеристики нуль, имеющая решение в некотором расширении этого поля, имеет решение и в самом поле.

$\triangleleft$ В самом деле, расширение можно ещё расширить до алгебраически замкнутого, при этом решение не пропадёт, а затем воспользоваться теоремой 39. $\triangleright$

84. Другой вариант теоремы Гильберта о нулях формулируется так: пусть дана система уравнений

$$\begin{cases} P_1(x_1,\ldots,x_n)=0,\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ P_k(x_1,\ldots,x_n)=0,\end{cases}$$

где все P_i — многочлены с комплексными коэффициентами, причём эта система не имеет решения в $\mathbb{C}$. Тогда можно найти такие многочлены $Q_i(x_1,\ldots,x_n)$, что

$$P_1(x_1,\ldots,x_n)Q_1(x_1,\ldots,x_n)+\ldots+P_k(x_1,\ldots,x_n)Q_k(x_1,\ldots,x_n)$$

тождественно равно единице.

Выведите это утверждение из доказанного нами варианта теоремы Гильберта о нулях. (Указание: рассмотрим в кольце $\mathbb{C}[x_1,\ldots,x_n]$ идеал, порождённый многочленами $P_1,\ldots,P_k$; если он содержит единицу, то всё доказано, если нет, то расширим его до максимального идеала I; тогда факторкольцо $\mathbb{C}[x_1,\ldots,x_n]/I$ будет полем, расширяющим $\mathbb{C}$, и в этом поле классы многочленов $x_1,\ldots,x_n$ составляют решение нашей системы.)

3.10. Игра Эренфойхта

Вернёмся от алгебры к логике и сформулируем общий критерий элементарной эквивалентности двух интерпретаций некоторой сигнатуры. Будем считать, что наша сигнатура содержит только предикатные символы. (Это ограничение не очень существенно, так как функцию $f(x_1,\ldots,x_n)$ можно заменить предикатом $f(x_1,\ldots,x_n)=$ $=y$, имеющим на один аргумент больше.) Кроме того, будем считать, что сигнатура конечна (в некоторый момент наших рассуждений это будет существенно).

Критерий будет сформулирован в терминах некоторой игры, называемой *игрой Эренфойхта*. В ней участвуют два игрока, называемые Новатором (**Н**) и Консерватором (**К**). Игра определяется выбранной парой интерпретаций; как мы докажем, интерпретации элементарно эквивалентны тогда и только тогда, когда **К** имеет выигрышную стратегию в этой игре.

В начале игры Новатор объявляет натуральное число k. Далее они ходят по очереди, начиная с **Н**; каждый из игроков делает k ходов, после чего определяется победитель.

На i-м ходу **Н** выбирает элемент в одной из интерпретаций (в любой из двух, причём выбор может зависеть от номера хода) и помечает его числом i. В ответ **К** выбирает некоторый элемент из другой интерпретации и также помечает его числом i. После k ходов игра заканчивается. При этом в каждой интерпретации k элементов оказываются помеченными числами от 1 до k (при этом уже не важно, кто из игроков их пометил). Обозначим эти элементы $a_1, a_2, \ldots, a_k$ (для первой интерпретации; элемент a_i имеет пометку i) и $b_1, b_2, \ldots, b_k$ (для второй). Элементы a_i и b_i (с одним и тем же i) будем называть *соответствующими* друг другу. Посмотрим, найдётся ли предикат сигнатуры, который различает помеченные элементы первой и второй интерпретации (то есть истинен на некотором наборе помеченных элементов в одной интерпретации, но ложен на соответствующих элементах другой). Если такой предикат найдётся, то выигрывает Новатор, в противном случае — Консерватор.

Прежде чем доказывать, что эта игра даёт критерий элементарной эквивалентности, рассмотрим несколько простых примеров.

- Среди элементов $a_1, \ldots, a_k$ и $b_1, \ldots, b_k$ могут быть одинаковые. Если в нашей сигнатуре есть предикат равенства и в обеих интерпретациях он интерпретируется как совпадение элементов, то Консерватор обязан повторять ходы, если их повторил Новатор (скажем, если $a_i = a_j$, а $b_i \neq b_j$, то Новатор выигрывает, поскольку предикат равенства истинен в одной интерпретации, но ложен на соответствующих элементах другой).

- Если интерпретации изоморфны, то у Консерватора есть очевидный способ выиграть: изоморфизм заранее группирует все элементы в пары соответствующих. (Это согласуется с тем, что изоморфные интерпретации элементарно эквивалентны.)

- Рассмотрим сигнатуру упорядоченных множеств (предикаты $=$ и $<$) и её естественные интерпретации в $\mathbb{N}$ и $\mathbb{Z}$. Они не являются элементарно эквивалентными, поскольку среди натуральных чисел есть наименьшее, а среди целых — нет. Покажем, что в игре Эренфойхта для данных интерпретаций выигрывает Новатор.

  Н объявляет, что игра будет проведена в два хода и на первом ходу помечает число 0 из интерпретации $\mathbb{N}$. В ответ **К** вынужден пометить некоторое число m из $\mathbb{Z}$. На втором ходу **Н** помечает в $\mathbb{Z}$ некоторое число, меньшее m (например, $m-1$). Теперь **К** проигрывает при любом ответном ходе, поскольку пометить число, меньшее нуля, он не может.

- Для той же сигнатуры рассмотрим интерпретации в $\mathbb{Z}$ и $\mathbb{Q}$. Эти интерпретации не элементарно эквивалентны, поскольку порядок на рациональных числах плотен, а на целых — нет. Покажем, что в игре Эренфойхта снова выигрывает Новатор.

  Игра будет проходить в три хода. На первых двух ходах **Н** помечает числа 0 и 1 из $\mathbb{Z}$. **К** должен пометить некоторые элементы b_1 и b_2 из $\mathbb{Q}$. При этом должно быть $b_1 < b_2$ (иначе **Н** заведомо выиграет). Тогда на третьем ходу **Н** помечает любое рациональное число, лежащее строго между b_1 и b_2. Так как между 0 и 1 нет натуральных чисел, **К** не может соблюсти требования игры и проигрывает при любом ходе.

- Рассмотрим теперь упорядоченные множества $\mathbb{Z}$ и $\mathbb{Z} + \mathbb{Z}$. Как мы видели (с. 140), они элементарно эквивалентны, и потому должна существовать выигрышная стратегия для Консерватора. Как же он должен играть? Кажется разумным поддерживать одинаковые расстояния между соответствующими элементами в $\mathbb{Z}$ и $\mathbb{Z}+\mathbb{Z}$. Проблема в том, что в $\mathbb{Z}+\mathbb{Z}$ некоторые расстояния бесконечны (между элементами разных слагаемых). Что же делать Консерватору, если Новатор пометил два таких элемента?

К счастью для **К**, он знает заранее, сколько ходов осталось до конца игры. Ясно, что если игра скоро кончится, то **Н** не удастся отличить бесконечное расстояние от достаточно большого. Более точно, если до конца игры остаётся s ходов, то **К** может считать все расстояния, большие или равные 2^s, бесконечно большими. В конце (при $s = 0$) это означает, что все ненулевые расстояния отождествляются (что правильно, так как в конце важен лишь порядок). Таким образом, **К** стремится поддерживать такой «инвариант» (как сказали бы программисты): соответствующие элементы в A и в B идут в одном и том же порядке, и расстояния между соответствующими парами соседей одинаковы (при этом все бесконечно большие расстояния считаются одинаковыми). Ясно, что такая стратегия гарантирует ему выигрыш; надо лишь проверить, что поддержать инвариант можно.

При очередном ходе **Н** возможны несколько случаев. **Н** мог разбить «конечный» (меньший 2^s, где s — число оставшихся ходов) промежуток на две части. В этом случае соответствующий промежуток в другом множестве также «конечен» и имеет ту же длину, так что **К** должен лишь выбрать элемент на том же расстоянии от концов. Пусть **Н** разбил «бесконечный» (длины 2^s или больше) промежуток на две части. Тогда хотя бы одна из частей будет иметь длину 2^{s-1} или больше, то есть на следующем шаге будет считаться «бесконечной». Если обе части «бесконечны» (с точки зрения следующего шага), то **К** должен разбить «бесконечный» (длины 2^s или более) промежуток другого множества на две «бесконечные» (длины 2^{s-1} или более) части; это, очевидно, возможно. Если одна часть «бесконечна», а другая «конечна», то надо отложить то же «конечное» расстояние в другом множестве. Наконец, обе части не могут быть «конечными» (если каждая меньше 2^{s-1}, то в сумме будет меньше 2^s).

Наконец, новый элемент мог быть больше (или меньше) всех уже отмеченных элементов интерпретации; в этом случае **K** должен отметить элемент другой интерпретации, находящийся на том же расстоянии от наибольшего (наименьшего) отмеченного элемента (или на «бесконечном» расстоянии, если такова была ситуация с выбранным **Н** элементом).

85. Кто выигрывает в игре Эренфойхта для упорядоченных множеств (**а**) $\mathbb{Z}$ и $\mathbb{R}$; (**б**) $\mathbb{R}$ и $\mathbb{Q}$; (**в**) $\mathbb{N}$ и $\mathbb{N}+\mathbb{Z}$? Как он должен играть?

Приведённые примеры делают правдоподобной связь между наличием формулы, различающей интерпретации, и выигрышной стратегии для **Н**. При этом число ходов, которое понадобится Новатору, соответствует *кванторной глубине* различающей интерпретации формулы. Кванторная глубина формулы определяется так:

- Глубина атомарных формул равна нулю.
- Глубина формул $\varphi \vee \psi$ и $\varphi \wedge \psi$ равна максимуму глубин формул φ и ψ.
- Глубина формулы $\neg\varphi$ равна глубине формулы φ.
- Глубина формул $\exists\xi\,\varphi$ и $\forall\xi\,\varphi$ на единицу больше глубины формулы φ.

Другими словами, глубина формулы — это наибольшая «глубина вложенности» кванторов (максимальная длина цепочки вложенных кванторов).

Рассмотрим позицию, которая складывается в игре после k ходов **Н** и **К** (перед очередным ходом **Н**) и за l ходов до конца игры (таким образом, общая длина игры есть $k+l$). В этот момент в каждой из интерпретаций совместными усилиями **Н** и **К** выбрано по k элементов. Пусть это будут элементы $a_1,\ldots,a_k$ в одной интерпретации (назовём её A) и $b_1,\ldots,b_k$ в другой (B).

Лемма. Если существует формула глубины l с параметрами $x_1,\ldots,x_k$, отличающая $a_1,\ldots,a_k$ от $b_1,\ldots,b_k$, то в указанной позиции **Н** имеет выигрышную стратегию; в противном случае её имеет **К**.

Поясним смысл условия леммы. Пусть φ — формула глубины l, все параметры которой содержатся в списке $x_1,\ldots,x_k$. Тогда имеет смысл ставить вопрос об её истинности в интерпретации A при значениях параметров $a_1,\ldots,a_k$, а также в интерпретации B при значениях параметров $b_1,\ldots,b_k$. Если окажется, что в одном случае формула φ истинна, а в другом ложна, то мы говорим, что φ отличает $a_1,\ldots,a_k$ от $b_1,\ldots,b_k$.

Пусть такая формула φ существует. Она представляет собой логическую (бескванторную) комбинацию некоторых формул вида вида $\forall\xi\,\psi$ и $\exists\xi\psi$, где ψ — формула глубины $l-1$. Хотя бы одна из формул, входящих в эту комбинацию, должна также отличать $a_1,\ldots,a_k$ от $b_1,\ldots,b_k$. Переходя к отрицанию, можно считать, что эта формула начинается с квантора существования. Пусть формула φ, имеющая вид

$$\exists x_{k+1}\psi(x_1,\ldots,x_k,x_{k+1}),$$

истинна для $a_1,\ldots,a_k$ и ложна для $b_1,\ldots,b_k$. Тогда найдётся такое a_{k+1}, для которого в A истинно

$$\psi(a_1,\ldots,a_k,a_{k+1}).$$

Это a_{k+1} и будет выигрывающим ходом Новатора; при любом ответном ходе b_{k+1} Консерватора формула

$$\psi(b_1,\ldots,b_k,b_{k+1})$$

будет ложной. Таким образом, некоторая формула глубины $l-1$ отличает $a_1, \ldots, a_k, a_{k+1}$ от $b_1, \ldots, b_k, b_{k+1}$ и потому, рассуждая по индукции, мы можем считать, что в оставшейся $(l-1)$-ходовой игре **Н** имеет выигрышную стратегию. (В конце концов мы придём к ситуации, когда некоторая бескванторная формула отличает $k+l$ элементов в A от соответствующих элементов в B, то есть **Н** выиграет.)

Обратное рассуждение (если наборы не отличимы никакой формулой глубины l, то **К** имеет выигрышную стратегию в оставшейся l-ходовой игре) аналогично, но чуть более сложно. Здесь важно, что по существу есть лишь конечное число различных формул глубины k.

Точнее говоря, будем называть две формулы (с параметрами) эквивалентными, если они одновременно истинны или ложны в любой интерпретации на любой оценке. Поскольку сигнатура конечна, существует лишь конечное число атомарных формул, все параметры которых содержатся среди $u_1, \ldots, u_s$. Существует лишь конечное число булевых функций с данным набором аргументов, поэтому существует лишь конечное число неэквивалентных бескванторных формул, все параметры которых содержатся среди $u_1, \ldots, u_s$. Отсюда следует, что существует лишь конечное число неэквивалентных формул вида

$$\exists u_s\, \psi(u_1, \ldots, u_s),$$

и потому лишь конечное число неэквивалентных формул глубины 1, параметры которых содержатся среди $u_1, \ldots, u_{s-1}$. (Здесь мы снова используем утверждение о конечности числа булевых функций с данным конечным списком аргументов, а также возможность переименовывать переменную под квантором, благодаря которой мы можем считать, что эта переменная есть u_s.) Продолжая эти рассуждения, мы заключаем, что для любого l и для любого набора переменных $u_1, \ldots, u_n$ существует лишь конечное число неэквивалентных формул глубины l, все параметры которых содержатся среди $u_1, \ldots, u_n$. (Здесь мы существенно используем конечность сигнатуры.)

Теперь можно закончить рассуждения про игру Эренфойхта. Пусть элементы $a_1, \ldots, a_k$ нельзя отличить от элементов $b_1, \ldots, b_k$ с помощью формул глубины l. Опишем выигрышную стратегию для **К**. Пусть **Н** выбрал произвольный элемент в одной из интерпретаций, скажем, a_{k+1}. Рассмотрим все формулы глубины $l - 1$ с $k + 1$ параметрами (с точностью до эквивалентности их конечное число); некоторые из них будут истинны на $a_1, \ldots, a_{k+1}$, а некоторые ложны. Тогда формула, утверждающая существование a_{k+1} с ровно такими свойствами (после квантора существования идёт конъюнкция всех истинных формул и отрицаний всех ложных) будет формулой глубины l, истинной на $a_1, \ldots, a_k$. По предположению эта формула должна быть истинной и на $b_1, \ldots, b_k$, и потому существует b_{k+1} с теми же свойствами, что и a_{k+1}. Этот элемент b_{k+1} и должен пометить **К**. Теперь предположение индукции позволяет заключить, что в возникшей позиции (где до конца игры $l - 1$ ходов) у **К** есть выигрышная стратегия.

Лемма доказана. Её частным случаем является обещанный критерий элементарной эквивалентности:

Теорема 41. Интерпретации A и B элементарно эквивалентны тогда и только тогда, когда в соответствующей игре Эренфойхта выигрывает Консерватор.

86. Покажите, что условие конечности сигнатуры существенно (без него из элементарной эквивалентности не следует существование выигрышной стратегии для **К**).

Заметим, что в некоторых случаях (например, для $\mathbb{Z}$ и $\mathbb{Z} + \mathbb{Z}$) игра Эренфойхта даёт нам новый способ доказательства элементарной эквивалентности.

3.11. Понижение мощности

В этом разделе мы опишем приём, позволяющей в интерпретации большой мощности выделять часть, которая будет элементарно эквивалентна исходной (и, более того, исходная будет её элементарным расширением в смысле определения на с. 142). Например, во всяком бесконечном упорядоченном множестве этот приём позволит найти счётное подмножество, элементарно эквивалентное исходному как интерпретация сигнатуры $(=,<)$.

С помощью этой конструкции (составляющей содержание теоремы Левенгейма – Сколема об элементарной подмодели) легко дать обещанное на с. 117 другое доказательство того, что любые два плотно упорядоченных множества без первого и последнего элемента элементарно эквивалентны. В самом деле, выберем в них счётные части, элементарно эквивалентные целым множествам. Эти части будут плотными и не будут иметь первого и последнего элементов, так как эти свойства записываются формулами. Как известно (см., например, [6]), любые два счётных плотных упорядоченных множества без первого и последнего элемента изоморфны, и потому (теорема 35, с. 138) элементарно эквивалентны. Следовательно, и исходные множества будут элементарно эквивалентны.

Прежде всего уточним слова «часть интерпретации». Если сигнатура состоит только из предикатных символов, то проблем нет: взяв произвольное непустое подмножество X произвольной интерпретации, мы можем ограничить предикаты на X и получить новую интерпретацию. Если в сигнатуре есть функциональные символы, мы должны ещё потребовать, чтобы X было замкнуто относительно соответствующих функций (значения функций на элементах подмножества X должны лежать в X). Возникающая при этом интерпретация с носителем X называется *подструктурой* исходной.

Теорема 42 (Левенгейма – Сколема об элементарной подмодели). Пусть имеется конечная или счётная сигнатура σ и некоторая бесконечная интерпретация M этой сигнатуры. Тогда можно указать счётное подмножество подмножество $M' \subset M$, которое будет подструктурой M (замкнуто относительно сигнатурных функций) и для которого M будет элементарным расширением M'.

$\lhd$ Начнём с первого требования теоремы: M' должно быть подструктурой. Само по себе его выполнить легко, как говорит следующая лемма.

Лемма 1. Пусть $A \subset M$ — произвольное конечное или счётное множество. Тогда существует конечное или счётное множество $B \subset M$, содержащее A, которое является подструктурой (замкнуто относительно сигнатурных функций в M).

Утверждение леммы почти очевидно: надо добавить к A результаты применения всех функций к его элементам, потом результаты применения всех функций к добавленным элементам и так счётное число раз. (Другими словами, надо добавить значения всех термов сигнатуры на оценках, при которых индивидные переменные принимают значения в A.) Ясно, что получится конечное или счётное множество, так как на каждом шаге расширения добавляется счётное множество новых элементов и шагов счётное число. (Можно заметить также, что термов счётное число.) Лемма 1 доказана.

Замкнутость подмножества A множества M относительно сигнатурных функций позволяет рассматривать интерпретацию с носителем A и с индуцированными из M функциями и предикатами. Однако она, конечно, не обязана быть элементарно эквивалентной M, как показывает множество очевидных примеров. (Если, скажем, в сигнатуре нет функций, а одни предикаты, то любое подмножество будет замкнуто.)

Поэтому нам необходимо ещё одно свойство замкнутости. Пусть A — некоторое подмножество M (напомним, что мы рассматриваем интерпретацию сигнатуры σ с носителем M). Множество A назовём *экзистенциально замкнутым*, если для всякой формулы $\varphi(x, x_1, \ldots, x_n)$ сигнатуры σ и для любых элементов $a_1, \ldots, a_n \in A$ выполнено такое утверждение: если существует $m \in M$, для которого (в M) истинно $\varphi(m, a_1, \ldots, a_n)$, то элемент m с таким свойством можно выбрать и внутри A.

(Более формально следовало бы сказать, что для всякой формулы φ, параметры которой содержатся среди

$x, x_1, \ldots, x_n$, и для любых элементов $a_1, \ldots, a_n \in A$ выполнено такое утверждение: если существует $m \in M$, для которого φ истинна в интерпретации M на оценке $(x \mapsto m, x_1 \mapsto a_1, \ldots, x_n \mapsto a_n)$, то существует и элемент $m \in A$ с тем же свойством.)

Обратите внимание, что в этом определении (в отличие от формулировки теоремы) не идёт речь об истинности какой бы то ни было формулы в A — только об истинности в M. В нём говорится примерно вот что: если вообще (во всём M) найдётся элемент, связанный неким формульным отношением с элементами $a_1, \ldots, a_n \in A$, то такой элемент найдётся и внутри самого A.

Лемма 2. Пусть $A \subset M$ — произвольное конечное или счётное множество. Тогда существует конечное или счётное множество $B \subset M$, содержащее A, являющееся экзистенциально замкнутым.

Доказательство леммы 2 аналогично доказательству предыдущей леммы: формул φ счётное число и конечных наборов элементов из A тоже счётное число. Поэтому можно посмотреть, в каких случаях элемент m из определения экзистенциальной замкнутости существует, и добавить один из таких элементов (здесь используется аксиома выбора). Один раз так сделать недостаточно, так как добавленные элементы также могут использоваться в качестве $a_1, \ldots, a_n$ в определении, поэтому такую процедуру надо повторить счётное число раз и взять объединение полученных множеств. Оно уже будет экзистенциально замкнуто (любой набор получается на конечном шаге и на следующем шаге он обслуживается, если нужно). Лемма 2 доказана.

На самом деле утверждения лемм 1 и 2 могут быть соединены.

Лемма 3. Пусть $A \subset M$ — произвольное конечное или счётное множество. Тогда существует конечное или счётное множество $B \subset M$, содержащее A, замкнутое относительно сигнатурных функций и экзистенциально замкнутое.

В самом деле, чтобы получить такое множество B, достаточно чередовать шаги замыкания относительно сигнатурных функций и экзистенциального замыкания, а потом взять объединение полученной последовательности множеств. Лемма 3 доказана.

Лемма 4. Пусть $M' \subset M$ замкнуто относительно сигнатурных функций и экзистенциально замкнуто. Тогда M является элементарным расширением M'.

Отсюда уже вытекает утверждение теоремы 42: применим лемму 3 к некоторому счётному подмножеству множества M, а затем воспользуемся леммой 4.

Доказательство леммы 4 также довольно просто. Напомним определение элементарного расширения: требуется, чтобы

$$M' \vDash \varphi(a_1, \ldots, a_n) \quad \Leftrightarrow \quad M \vDash \varphi(a_1, \ldots, a_n)$$

для любой формулы $\varphi(x_1, \ldots, x_n)$ и для любых элементов $a_1, \ldots, a_n \in M'$.

(Формально следовало бы сказать: для любой формулы с параметрами и любой оценки, при которой все параметры принимают значения в M', истинность этой формулы в M' на этой оценке равносильна истинности той же формулы в M на той же оценке.)

Будем доказывать это индукцией по построению формулы φ. Для атомарных формул это очевидно: значения термов не зависят от того, проводим ли мы вычисления в M или M', а предикаты на M' индуцированы из M.

Если формула φ есть конъюнкция, дизъюнкция, импликация или отрицание, то её истинность как в M, так и в M' определяется истинностью её частей (и можно сослаться на предположение индукции).

Единственный нетривиальный случай — если формула φ начинается с квантора. Мы можем сократить себе работу и рассматривать только квантор существования, так как $\forall\xi$ можно заменить на $\neg\exists\xi\neg$. Итак, пусть $\varphi(x_1, \ldots, x_n)$ имеет вид

$$\exists x\, \psi(x, x_1, \ldots, x_n).$$

Если $M' \vDash \varphi(a_1, \ldots, a_n)$ для некоторых $a_1, \ldots, a_n \in M'$, то по определению истинности найдётся элемент $m \in M'$, для которого $M' \vDash \psi(m, a_1, \ldots, a_n)$. Тогда по предположению индукции (формула ψ короче формулы φ) можно перейти к большей интерпретации и заключить, что $M \vDash \psi(m, a_1, \ldots, a_n)$, и потому по определению истинности $M \vDash \varphi(a_1, \ldots, a_n)$. Обратное рассуждение просто так не проходит, поскольку существующий элемент m существует в M, а не в M', и предположение индукции применить нельзя. Однако ровно для этого у нас есть требование экзистенциальной замкнутости, которое позволяет заменить элемент m на другой элемент из M' и завершить доказательство. $\triangleright$

Вот пример применения теоремы Левенгейма – Сколема в алгебре: существует алгебраически замкнутое счётное подполе поля $\mathbb{C}$ комплексных чисел. (В самом деле, требование алгебраической замкнутости можно записать в виде счётной последовательности формул — по одной для каждой степени многочлена. Аксиомы поля также можно записать в виде формул. Значит, счётная элементарная подмодель поля $\mathbb{C}$ будет также алгебраически замкнутым полем.)

Впрочем, алгебраистов такое применение скорее насмешит — они и так знают, что алгебраические элементы поля $\mathbb{C}$ (корни многочленов с целыми коэффициентами) образуют счётное алгебраически замкнутое поле.

Любопытный парадокс связан с попытками применить теорему Левенгейма – Сколема в теории множеств. Представим себе интерпретацию языка теории множеств (предикаты $=$ и $\in$), носителем которой является множество всех множеств. Такого множества, строго говоря, не бывает, но если про это забыть и применить теорему Левенгейма – Сколема об элементарной подмодели, то можно оставить лишь счётное число множеств так, чтобы истинность утверждений теории множеств не изменилась. Но среди этих утверждений есть и утверждение о существовании несчётного множества — как же так? Это рассуждение содержит столько пробелов, что указать один из них совсем нетрудно. Тем не менее оно может быть переведено в аксиоматическую теорию множеств и даёт интересные (хотя уже не парадоксальные) результаты.

Два дополнительных замечания усиливают теорему Левенгейма – Сколема. Во-первых, легко видеть, что для всякого конечного или счётного подмножества $A \subset M$ найдётся счётная элементарная подструктура $M' \subset M$, содержащая все элементы A. (В самом деле, процесс замыкания, использованный при доказательстве, можно начинать с множества A.)

Во-вторых, можно отказаться от требования счётности сигнатуры и сказать так: для всякого подмножества $A \subset M$ найдётся элементарная подструктура $M' \subset M$, содержащая A, мощность которой не превосходит максимума из $\aleph_0$, мощности множества A и мощности сигнатуры. В самом деле, и конструкция замыкания относительно сигнатурных операций, и конструкция экзистенциального замыкания, и счётное объединение возрастающей цепи не выводят мощность за пределы указанного максимума, поскольку и формулы, и термы являются конечными последовательностями символов сигнатуры и счётного числа других символов (см. подробнее в [6]); то же самое можно сказать о числе возможных наборов значений параметров.

Мы научились уменьшать мощность структуры, не меняя множества истинных в ней формул. Можно, напротив, увеличивать мощность (соответствующее утверждение иногда называют теоремой Левенгейма – Сколема об элементарном расширении). Но эта конструкция использует теорему компактности для языков первого порядка, которая в свою очередь вытекает из теоремы Гёделя о полноте. Поэтому мы отложим обсуждение этого утверждения до следующей главы.

4. Исчисление предикатов

4.1. Общезначимые формулы

Исчисление высказываний (глава 2) позволяло выводить все тавтологии из некоторого набора базисных тавтологий (названных аксиомами) с помощью некоторых правил вывода (на самом деле единственного правила modus ponens). Сейчас мы хотим решить аналогичную задачу для формул первого порядка. Соответствующее исчисление называется *исчислением предикатов*.

Пусть фиксирована некоторая сигнатура σ. Формула φ этой сигнатуры (возможно, с параметрами) называется *общезначимой*, если она истинна в любой интерпретации сигнатуры σ на любой оценке.

Общезначимые формулы в логике предикатов играют ту же роль, что тавтологии в логике высказываний. Между ними есть и формальная связь: если взять любую тавтологию и вместо входящих в неё пропозициональных переменных подставить произвольные формулы сигнатуры σ, получится общезначимая формула. В самом деле, пусть есть некоторая интерпретация сигнатуры σ и некоторая оценка (то есть фиксированы значения индивидных переменных). Тогда каждая из подставленных формул станет истинной или ложной, а значение всей формулы определяется с помощью таблиц истинности для логических связок, то есть по тем же правилам, что в логике высказываний.

Конечно, бывают и другие общезначимые формулы, не являющиеся частным случаями пропозициональных тавтологий. Например, формула

$$\forall x\, A(x) \to \exists y A(y)$$

общезначима (здесь существенно, что носитель любой интерпретации непуст). Другие примеры общезначимых формул:

$$\exists y\,\forall x\,B(x,y)\to\forall x\,\exists y\,B(x,y),$$
$$\neg\forall x\,\neg\varphi\to\exists x\,\varphi$$

(во втором случае φ — произвольная формула).

87. Будет ли общезначима формула (**а**) $\forall x\,\exists y\,B(x,y)\to\to\exists y\,\forall x\,B(x,y)$? (**б**) $\neg\forall x\,\exists y\,B(x,y)\to\exists x\,\forall y\,\neg B(x,y)$?

Многие вопросы можно сформулировать как вопросы об общезначимости некоторых формул. Например, можно записать свойства рефлексивности, транзитивности и антисимметричности в виде формул R, T и A сигнатуры $(=,<)$ и затем написать формулу

$$R\wedge T\wedge A\to\exists x\,\forall y\,((y<x)\vee(y=x)).$$

Общезначимость этой формулы означала бы, что любое линейно упорядоченное множество имеет наибольший элемент, так что она не общезначима.

88. Напишите формулы R,T,A и проверьте, что приведённая нами формула не общезначима, хотя истинна во всех конечных интерпретациях.

89. Известно, что формула истинна во всех конечных и счётных интерпретациях. Можно ли из этого заключить, что она общезначима? (Указание: воспользуйтесь теоремой Левенгейма – Сколема об элементарной подмодели.)

Две формулы φ и ψ (с параметрами или без) называются *эквивалентными*, если в любой интерпретации и на любой оценке, на которой истинна одна из них, истинна и другая. Это определение равносильно такому: формула $\varphi\leftrightarrow\psi$ общезначима. Здесь, напомним, $\varphi\leftrightarrow\psi$ есть сокращение для $((\varphi\to\psi)\wedge(\psi\to\varphi))$.

Общезначимость любой формулы φ очевидно равносильна общезначимости её *замыкания* — формулы, которая получится, если слева к φ приписать кванторы всеобщности по всем параметрам.

Двойственное к общезначимости понятие — выполнимость. Формула называется *выполнимой*, если она истинна в некоторой интерпретации на некоторой оценке.

Очевидно, формула φ общезначима тогда и только тогда, когда формула $\neg\varphi$ не является выполнимой.

90. Закончите утверждение: выполнимость формулы с параметрами равносильна выполнимости замкнутой формулы, которая получится, если...

Чтобы проверить, является ли формула тавтологией, достаточно подставить в неё все возможные наборы значений переменных. Хотя этот процесс может быть на практике невыполним (наборов слишком много), теоретически мы имеем простой алгоритм проверки, является ли формула тавтологией. Для общезначимых формул в общем случае такого алгоритма не существует (теорема Чёрча; её доказательство можно прочесть в [5]); он есть только для очень ограниченных классов формул. Например, если сигнатура содержит только нульместные предикатные символы, то задача по существу сводится к проверке тавтологичности (в этом случае кванторы фиктивны). Чуть более сложен случай с одноместными предикатами.

91. Пусть сигнатура σ содержит только одноместные предикаты. Докажите, что всякая выполнимая формула этой сигнатуры, содержащая n различных предикатов, выполнима в некоторой конечной интерпретации, содержащей не более 2^n элементов. Как использовать этот факт для алгоритмической проверки выполнимости формул такой сигнатуры?

4.2. Аксиомы и правила вывода

Возвратимся к нашей задаче: какие аксиомы и правила вывода нам нужны, чтобы получить все общезначимые формулы некоторой сигнатуры σ? Естественно использовать все схемы аксиом (1) – (11) исчисления высказываний (раздел 2.1), но только вместо букв A, B и C теперь можно подставлять произвольные формулы сигнатуры σ. Теорема о полноте исчисления высказываний гарантирует, что после этого мы сможем вывести любой частный случай любой пропозициональной тавтологии (то есть любую формулу, которая получается из пропозициональной тавтологии заменой пропозициональных переменных на формулы сигнатуры σ). В самом деле, возьмём вывод этой тавтологии в исчислении высказываний (которое, как мы знаем, полно) и выполним соответствующую замену во всех формулах этого вывода.

Почти столь же просто понять, что ничего другого такие аксиомы не дадут: если пользоваться лишь схемами аксиом (1) – (11), разрешая брать в них в качестве A, B, C произвольные формулы сигнатуры σ, а в качестве правила вывода использовать modus ponens, то все выводимые формулы будут частными случаями пропозициональных тавтологий. В самом деле, если какая-то подформула начинается с квантора, то в выводе она может встречаться только как единое целое, то есть такая подформула ведёт себя как пропозициональная переменная.

92. Проведите это рассуждение аккуратно.

Это наблюдение скорее тривиально, чем удивительно — если среди наших аксиом и правил вывода нет ничего о смысле кванторов, то формулы, начинающиеся с кванторов, будут вести себя как неделимые блоки. Таким образом, нам нужны аксиомы и правила вывода, отражающие интуитивный смысл кванторов.

Вспомним, как выглядели аксиомы исчисления высказываний. У нас было два типа аксиом для конъюнкции и дизъюнкции: одни говорили, что из них следует (например, из $A \wedge B$ следовало B), а другие — как их можно доказать (например, аксиома $(A \to (B \to (A \wedge B)))$ говорила, что для доказательства $(A \wedge B)$ надо доказать A и B). Кванторы всеобщности и существования в некотором смысле аналогичны конъюнкции и дизъюнкции, и аксиомы для них тоже будут похожими. Например, среди аксиом будет формула

$$\forall x\, A(x) \to A(t),$$

где A — одноместный предикатный символ нашей сигнатуры, а t — константа, переменная или вообще любой терм. (Если A верно для всех x, то оно должно быть верно и для нашего конкретного t. Можно сказать и так: из «бесконечной конъюнкции» всех $A(x)$ вытекает один из её членов.)

Конечно, такую аксиому надо иметь не только для одноместного предикатного символа A, но для любой формулы φ, любой переменной ξ и любого терма t. Естественно сказать, что если φ — любая формула, а t — любой терм, то формула

$$\forall\xi\,\varphi \to \varphi(t/\xi),$$

где $\varphi(t/\xi)$ обозначает результат подстановки t вместо всех вхождений переменной ξ в формулу φ, является аксиомой. (Запись $\varphi(t/\xi)$ можно читать как «фи от тэ вместо кси».)

К сожалению, всё не так просто. Например, если формула φ имеет вид

$$A(x) \wedge \exists x\, B(x,x),$$

то подстановка терма $f(y)$ вместо x даст абсурдное выражение

$$A(f(y)) \wedge \exists f(y)\, B(f(y), f(y)),$$

вообще не являющееся формулой. А если подставить $f(y)$ только внутри A и B, то получится выражение

$$A(f(y)) \wedge \exists x\, B(f(y), f(y)),$$

которое хотя и будет формулой, но имеет совсем не тот смысл, который нам нужен.

Конечно, в данном случае по смыслу ясно, что подставлять $f(y)$ надо лишь вместо самого первого вхождения переменной x. Но если мы хотим определить формальную систему аксиом и правил вывода, то надо дать формальные определения.

Для каждого квантора в формуле рассмотрим его *область действия* — начинающуюся с него подформулу. *Свободным вхождением* индивидной переменной в формулу называется вхождение, не попадающее в область действия одноимённого квантора. Легко понять, что это определение можно переформулировать индуктивно:

- любое вхождение переменной в терм свободно;

- свободные вхождения переменной в формулу φ являются её свободными вхождениями в формулу $\neg\varphi$;

- свободные вхождения любой переменной в одну из формул φ и ψ являются свободными вхождениями в $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$ и $(\varphi \to \psi)$;

- переменная ξ не имеет свободных вхождений в формулы $\forall\xi\, \varphi$ и $\exists\xi\, \varphi$; свободные вхождения остальных переменных в φ являются свободными вхождениями в эти две формулы.

Сравнивая это определение с индуктивным определением параметров формулы в разделе 3.2, мы видим, что параметры — это переменные, имеющие свободные вхождения в формулу.

Вхождения переменной, не являющиеся свободными (в том числе стоящие рядом с квантором) называют *связанными.* Например, переменная x имеет одно свободное и три связанных вхождения в формулу $A(x) \wedge \exists x\, B(x,x)$.

Теперь можно внести поправку в сказанное выше и считать, что аксиомами являются формулы

$$\forall\xi\, \varphi \to \varphi(t/\xi),$$

где $\varphi(t/\xi)$ есть результат подстановки t вместо всех *свободных* вхождений переменной ξ. Однако такой оговорки недостаточно, как показывает следующий пример.

Подставляя $f(y)$ вместо x в формулу $\forall z\, B(x,z)$, мы получаем (в полном согласии с нашей интуицией) формулу $\forall z\, B(f(y),z)$. Теперь рассмотрим формулу $\forall y\, B(x,y)$, которая отличается от $\forall z\, B(x,z)$ лишь именем связанной переменной и должна иметь тот же смысл. Переменная x в ней по-прежнему свободна, но подстановка $f(y)$ вместо x даёт формулу $\forall y\, B(f(y),y))$, в которой $f(y)$ неожиданно для себя попадает в область действия квантора по y. Такое явление иногда называют *коллизией переменных*; при этом подстановка даёт формулу, имеющую совсем не тот смысл, какой мы хотели.

93. Приведите пример формулы вида $\forall\xi\, \varphi \to \varphi(t/\xi)$, в которой происходит коллизия переменных и которая не является общезначимой. (Ответ: $\forall x\, \exists y\, A(x,y) \to \exists y A(y,y)$.)

Поэтому нам придётся принять ещё одну меру предосторожности и формально определить понятие *корректной* подстановки терма вместо переменной. Мы будем говорить, что подстановка терма t вместо переменной ξ корректна, если в процессе текстуальной замены всех свободных вхождений переменной ξ на терм t никакая переменная из t не попадает в область действия одноимённого квантора.

Педантичный читатель мог бы попросить доказать, что результат такой подстановки будет формулой. Это проще всего сделать так: дать индуктивное определение корректной подстановки, равносильное исходному.

Сначала определим индуктивно результат подстановки терма t вместо переменной ξ в терм u; этот результат будем обозначать $u(t/\xi)$:

- $\xi(t/\xi)$ есть t; для любой переменной η, отличной от ξ, мы полагаем $\eta(t/\xi)$ равным η.
- если f есть k-местный функциональный символ, а $t_1, \ldots, t_k$ — термы, то
$$f(t_1, \ldots, t_k)(t/\xi) = f(t_1(t/\xi), \ldots, t_k(t/\xi)).$$

Теперь индуктивное определение продолжается для формул:

- для атомарных формул: если R есть k-местный предикатный символ, а $t_1, \ldots, t_k$ — термы, то
$$R(t_1, \ldots, t_k)(t/\xi) = R(t_1(t/\xi), \ldots, t_k(t/\xi))$$
и подстановка является корректной;

- подстановка терма t вместо переменной ξ в формулу $\neg\varphi$ корректна, если она корректна для формулы φ, при этом

  $$[\neg\varphi](t/\xi) = \neg[\varphi(t/\xi)]$$

  (квадратные скобки указывают порядок действий, не являясь частью формулы);

- подстановка терма t вместо переменной ξ в формулу $(\varphi \wedge \psi)$ корректна, если она корректна для обеих формул φ и ψ, при этом

  $$(\varphi \wedge \psi)(t/\xi) = (\varphi(t/\xi) \wedge \psi(t/\xi));$$

  аналогично для формул $(\varphi \vee \psi)$ и $(\varphi \to \psi)$.

- наконец, подстановка t вместо ξ в формулу $\forall\eta\,\varphi$ корректна в двух случаях:

  (1) если ξ не является параметром формулы $\forall\eta\,\varphi$ (это возможно, когда ξ не является параметром φ или когда ξ совпадает с η); при этом подстановка ничего не меняет в формуле;

  (2) переменная ξ является параметром формулы $\forall\eta\,\varphi$, но переменная η не входит в терм t и подстановка $\varphi(t/\xi)$ корректна; при этом

  $$[\forall\eta\,\varphi](t/\xi) = \forall\eta\,[\varphi(t/\xi)].$$

  Аналогично определяется корректная подстановка в формулу $\exists\xi\varphi$.

Главная часть в этом определении — последний его пункт, который, во-первых, говорит, что вместо связанных вхождений переменных ничего подставлять не надо, а во-вторых, требует, чтобы при корректной подстановке переменные из терма t не подпадали под действие одноимённых кванторов.

После всех этих приготовлений мы можем сформулировать две оставшиеся схемы аксиом исчисления предикатов: формула

(12) $\forall\xi\,\varphi \to \varphi(t/\xi)$

и двойственная ей формула

(13) $\varphi(t/\xi) \to \exists\xi\,\varphi$

будут аксиомами исчисления предикатов, если указанные в них подстановки корректны.

Два частных случая, когда подстановка заведомо корректна: во-первых, можно безопасно подставлять константу (или любой терм без параметров), во-вторых, подстановка переменной вместо себя всегда корректна (и ничего не меняет в формуле).

Отсюда следует, что формулы $\forall\xi\,\varphi \to \varphi$ и $\varphi \to \exists\xi\,\varphi$ будут аксиомами исчисления предикатов (для любой формулы φ и переменной ξ).

Нужны ли нам ещё какие-нибудь аксиомы и правила вывода? Конечно, нужны, поскольку уже сформулированные аксиомы не полностью отражают смысл кванторов. (Например, они вполне согласуются с таким пониманием этого смысла: формула $\forall\xi\,\varphi$ всегда ложна, а формула $\exists\xi\,\varphi$ всегда истинна.) Поэтому мы введём в наше исчисление два правила вывода, называемые *правилами Бернайса*, и на этом определение исчисления предикатов будет завершено.

Если переменная ξ не является параметром формулы ψ, то правила Бернайса разрешают такие переходы:

$$\frac{\psi \to \varphi}{\psi \to \forall\xi\,\varphi} \qquad\qquad \frac{\varphi \to \psi}{\exists\xi\,\varphi \to \psi}$$

Мы говорим, что стоящая снизу от черты (в каждом из правил) формула получается по соответствующему правилу из верхней. Соответственно дополняется и определение вывода как последовательности формул, в которой каждая формула либо является аксиомой, либо получается из предыдущих по одному из правил вывода (раньше было только правило MP, теперь добавились два новых правила).

Поясним интуитивный смысл этих правил. Первое говорит, что если из ψ следует φ, причём в φ есть параметр ξ, которого нет в ψ, то это означает, что формула φ истинна при всех значениях параметра ξ, если только формула ψ истинна.

Используя первое правило Бернайса, легко установить допустимость *правила обобщения*

$$\frac{\varphi}{\forall\xi\,\varphi} \qquad \text{(Gen)}$$

(если в исчислении предикатов выводима формула сверху от черты, то выводима и формула снизу). В самом деле, возьмём какую-нибудь выводимую формулу ψ без параметров (например, аксиому, в которой вместо A, B и C подставлены замкнутые формулы). Раз выводима формула φ, то выводима и формула $\psi \to \varphi$ (поскольку $\varphi \to (\psi \to \varphi)$ является тавтологией и даже аксиомой). Теперь по правилу Бернайса выводим $\psi \to \forall\xi\,\varphi$ и применяем правило MP к этой формуле и к формуле ψ.

Правило (Gen) (от Generalization — обобщение) кодифицирует стандартную практику рассуждений: мы доказываем какое-то утверждение φ со свободной переменной ξ, после чего заключаем, что мы доказали $\forall\xi\,\varphi$, так как ξ было произвольным.

Второе правило Бернайса также вполне естественно: желая доказать ψ в предположении $\exists\xi\,\varphi$, мы говорим: пусть такое ξ существует, возьмём его и докажем ψ (то есть докажем $\varphi \to \psi$ со свободной переменной ξ).

94. Покажите, что класс выводимых в исчислении предикатов формул не изменится, если мы вместо правил Бернайса добавим туда правило обобщения и две аксиомы

$$\forall\xi\,(\psi \to \varphi) \to (\psi \to \forall\xi\,\varphi)$$

и

$$\forall\xi\,(\varphi \to \psi) \to (\exists\xi\,\varphi \to \psi)$$

(в которых требуется, чтобы переменная ξ не была параметром формулы ψ).

Как и в случае исчисления высказываний, перед нами стоят две задачи: надо доказать корректность исчисления предикатов (всякая выводимая формула общезначима) и его полноту (всякая общезначимая формула выводима). Этим мы и займёмся в следующих разделах.

4.3. Корректность исчисления предикатов

Теорема 43. Всякая выводимая в исчислении предикатов формула является общезначимой.

$\triangleleft$ Для исчисления высказываний проверка корректности была тривиальной — надо было по таблице проверить, что все аксиомы (1)–(11) являются тавтологиями. С этими аксиомами и сейчас нет проблем. Но в двух следующих аксиомах есть ограничение на корректность подстановки, без которого они могут не быть общезначимыми. Естественно, это ограничение должно быть использовано и в доказательстве корректности, и это потребует довольно скучных рассуждений — тем более скучных, что сам факт кажется ясным и так. Тем не менее такие рассуждения надо уметь проводить, так что мы ничего пропускать не будем.

Итак, пусть фиксирована сигнатура σ, а также некоторая интерпретация этой сигнатуры. Всюду далее, говоря о термах и формулах, мы имеем в виду термы и формулы этой сигнатуры, а говоря об их значениях, имеем в виду значения в этой интерпретации.

Лемма 1. Пусть u и t — термы, а ξ — переменная. Тогда

$$[u(t/\xi)](\pi) = [u](\pi + (\xi \mapsto [t](\pi)))$$

для произвольной оценки π.

Напомним обозначения: в левой части мы подставляем t вместо ξ в терм u, и берём значение получившегося терма на оценке π. В правой части стоит значение терма u на оценке, которая получится из π, если значение переменной ξ изменить и считать равным значению терма t на оценке π.

В сущности, это утверждение совершенно тривиально: оно говорит, например, что значение $\sin(\cos(x))$ при $x = 2$ равно значению $\sin(y)$ при $y = \cos(2)$. Но раз уж мы взялись всё доказывать формально, докажем его индукцией по построению терма u. Если терм u есть переменная, отличная от ξ, то ни подстановка, ни изменение оценки не сказываются на значении терма u. Для случая $u = \xi$ получаем $[t](\pi)$ слева и справа. Если терм получается из других термов применением функционального символа, то подстановка выполняется отдельно в каждом из этих термов, так что искомое равенство также сохраняется. Лемма 1 доказана.

Аналогичное утверждение для формул таково:

Лемма 2. Пусть φ — формула, t — терм, а ξ — переменная, причём подстановка t вместо ξ в формулу φ корректна. Тогда

$$[\varphi(t/\xi)](\pi) = [\varphi](\pi + (\xi \mapsto [t](\pi)))$$

для произвольной оценки π.

Поясним смысл этой леммы на примере. Пусть ξ является единственным параметром формулы φ, а c — константа. Тогда формула $\varphi(c/\xi)$ замкнута; лемма утверждает, что её истинность равносильна истинности φ на оценке, при которой значение переменной ξ есть элемент интерпретации, соответствующий константе c.

Доказательство леммы проведём индукцией по построению формулы φ. Для атомарных формул это утверждение является прямым следствием леммы 1. Кроме того, из определения истинностного значения формулы и из определения подстановки ясно, что если утверждение леммы 2 верно для двух формул φ_1 и φ_2, то оно верно для их любой их логической комбинации (конъюнкции, дизъюнкции и импликации); аналогично для отрицания.

Единственный нетривиальный случай — формула, начинающаяся с квантора. Здесь наши определения вступают в игру. Пусть φ имеет вид $\forall\eta\,\psi$. Есть два принципиально разных случая: либо ξ является параметром формулы φ (т. е. формулы $\forall\eta\,\psi$), либо нет. Во втором случае $\varphi(t/\xi)$ совпадает с φ, а изменение значения переменной ξ в оценке π не влияет на значение формулы φ, так что всё сходится. Осталось разобрать случай, когда ξ является параметром формулы $\forall\eta\,\psi$ (отсюда следует, что ξ не совпадает с η). По определению корректной подстановки, в этом случае переменная η не входит в терм t и подстановка $\psi(t/\xi)$ корректна. Тогда

$$\begin{aligned}[(\forall\eta\,\psi)(t/\xi)](\pi) = [\forall\eta\,(\psi(t/\xi))](\pi) =&\\ = \wedge_m[\psi(t/\xi)](\pi + (\eta \mapsto m)) =&\\ = \wedge_m[\psi](\pi + (\eta \mapsto m) + (\xi \mapsto [t](\pi + (\eta \mapsto m)))).&\end{aligned}$$

Мы воспользовались определением подстановки, определением истинности ($\wedge_m$ означает конъюнкцию по всем элементам из носителя интерпретации) и предположением индукции для формулы ψ. Теперь надо заметить, что переменная η не входит в t по предположению корректности, и потому значение терма t не изменится, если заменить $\pi + (\eta \mapsto m)$ на π. Далее, ξ и η различны, поэтому два изменения в π можно переставить местами. Используя эти соображения, можно продолжить цепочку равенств:

$$\begin{aligned}&= \wedge_m[\psi](\pi + (\xi \mapsto [t](\pi)) + (\eta \mapsto m)) =\\ &= [\forall\eta\,\psi](\pi + (\xi \mapsto [t](\pi))) =\\ &= [\varphi](\pi + (\xi \mapsto [t](\pi))),\end{aligned}$$

что и требовалось. Случай формулы вида $\exists\xi\,\psi$ разбирается аналогично, надо только $\wedge_m$ заменить на $\vee_m$. Лемма 2 доказана.

Теперь уже ясно, почему формула

$$\forall\xi\,\varphi \to \varphi(t/\xi)$$

будет истинна на любой оценке π (если подстановка корректна). В самом деле, если левая часть импликации истинна на π, то φ будет истинна на любой оценке π', которая отличается от π лишь значением переменной ξ. В частности, φ будет истинна и на оценке $\pi + (\xi \mapsto [t](\pi))$, что по только что доказанной лемме 2 означает, что правая часть импликации истинна на π.

Общезначимость формулы

$$\varphi(t/\xi) \to \exists\xi\,\varphi$$

доказывается аналогично.

Нам осталось проверить, что правила вывода сохраняют общезначимость. Для правила MP это очевидно (как и в случае исчисления высказываний). Проверим это для правил Бернайса. Это совсем несложно, так как здесь нет речи ни о каких корректных подстановках.

Пусть, например, формула $\psi \to \varphi$ общезначима и переменная ξ не является параметром формулы ψ. Проверим, что формула $\psi \to \forall\xi\,\varphi$ общезначима, то есть истинна на любой оценке π (в любой интерпретации). В самом деле, пусть ψ истинна на оценке π. Тогда она истинна и на любой оценке π', отличающейся от π только значением переменной ξ (значение переменной ξ не влияет на истинность ψ, так как ξ не является параметром). Значит, и формула φ истинна на любой такой оценке π'. А это в точности означает, что $\forall\xi\,\varphi$ истинна на оценке π, что и требовалось.

Для второго правила Бернайса рассуждение симметрично. Пусть формула $\varphi \to \psi$ общезначима и переменная ξ не является параметром формулы ψ. Покажем, что формула $\exists\xi\,\varphi \to \psi$ общезначима. В самом деле, пусть её левая часть истинна на некоторой оценке π. По определению истинности формулы, начинающейся с квантора существования, это означает, что найдётся оценка π', которая отличается от π только на переменной ξ, для которой $[\varphi](\pi')$ истинно. Тогда и $[\psi](\pi')$ истинно. Но переменная ξ не является параметром формулы ψ, так что $[\psi](\pi') = [\psi](\pi)$. Следовательно, формула ψ истинна на оценке π, что и требовалось доказать. $\triangleright$

4.4. Выводы в исчислении предикатов

Примеры выводимых формул

Прежде чем доказывать теорему Гёделя о полноте исчисления предикатов, мы должны приобрести некоторый опыт построения выводов в этом исчислении.

- Прежде всего отметим, что возможность сослаться на теорему о полноте исчисления высказываний и считать выводимым любой частный случай пропозициональной тавтологии сильно облегчает жизнь. Например, пусть мы вывели две формулы φ и ψ и хотим теперь вывести формулу $(\varphi\wedge\psi)$. Это просто: заметим, что формула $(\varphi \to (\psi \to (\varphi \wedge \psi)))$ является частным случаем пропозициональной тавтологии (а на самом деле и аксиомой) и дважды применяем правило MP.

- Другой пример такого же рода: если формула $\varphi \to \psi$ выводима, то выводима и формула $\neg\psi \to \neg\varphi$, поскольку импликация

$$(\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$$

  является частным случаем пропозициональной тавтологии.

- Ещё один пример: если выводимы формулы $\varphi \to \psi$ и $\psi \to \tau$, то выводима и формула $\varphi \to \tau$, поскольку формула

$$(\varphi \to \psi) \to ((\psi \to \tau) \to (\varphi \to \tau))$$

  является частным случаем пропозициональной тавтологии.

- Для произвольной формулы φ выведем формулу

$$\forall x\, \varphi \to \exists x\, \varphi.$$

В самом деле, подстановка переменной вместо себя всегда допустима, поэтому формулы $\forall x\,\varphi \to \varphi$ и $\varphi \to \exists x\,\varphi$ являются аксиомами. Остаётся воспользоваться предыдущим замечанием.

- Для произвольной формулы φ выведем формулу

$$\exists y\,\forall x\,\varphi \to \forall x\,\exists y\,\varphi.$$

Формулы $\forall x\,\varphi \to \varphi$ и $\varphi \to \exists y\,\varphi$ являются аксиомами. С их помощью выводим формулу $\forall x\,\varphi \to \exists y\,\varphi$. Теперь заметим, что левая часть импликации не имеет параметра x, а правая часть не имеет параметра y, так что можно применить два правила Бернайса (в любом порядке) и добавить справа квантор $\forall x$, а слева — квантор $\exists y$.

- Предположим, что формула $\varphi \to \psi$ выводима, а ξ — произвольная переменная. Покажем, что в этом случае выводима формула $\forall\xi\,\varphi \to \forall\xi\,\psi$. В самом деле, формула $\forall\xi\,\varphi \to \varphi$ является аксиомой. Далее выводим (с помощью пропозициональных тавтологий и правила MP) формулу $\forall\xi\,\varphi \to \psi$; остаётся воспользоваться правилом Бернайса (левая часть не имеет параметра ξ).

- Аналогичным образом из выводимости формулы $\varphi \to \psi$ следует выводимость формулы $\exists\xi\,\varphi \to \exists\xi\,\psi$, только надо начать с аксиомы $\psi \to \exists\xi\,\psi$, затем получить $\varphi \to \exists\xi\,\psi$, а потом применить правило Бернайса.

- Таким образом, если формулы φ и ψ доказуемо эквивалентны (это значит, что импликации $\varphi \to \psi$ и $\psi \to \varphi$ выводимы), то формулы $\forall\xi\,\varphi$ и $\forall\xi\,\psi$ также доказуемо эквивалентны. (Аналогичное утверждение верно и для формул $\exists\xi\,\varphi$ и $\exists\xi\,\psi$.)

Теперь несложно доказать и и более общий факт: замена подформулы на доказуемо эквивалентную даёт доказуемо эквивалентную формулу (см. с. 192).

- Выведем формулу $\forall x\, A(x) \to \forall y\, A(y)$ (здесь A — одноместный предикатный символ). Это несложно: начнём с аксиомы $\forall x\, A(x) \to A(y)$, в ней левая часть не имеет параметра y и потому по правилу Бернайса из неё получается искомая формула. Этот пример показывает, что связанные переменные можно переименовывать, не меняя смысла формулы (подробнее об этом мы скажем в разделе 4.6.)

- Выведем формулы, связывающие кванторы всеобщности и существования:

$$\forall\xi\, \varphi \leftrightarrow \neg\exists\xi\, \neg\varphi;$$
$$\exists\xi\, \varphi \leftrightarrow \neg\forall\xi\, \neg\varphi.$$

  Напомним, что $\alpha \leftrightarrow \beta$ мы считаем сокращением для $(\alpha \to \beta)\wedge(\beta \to \alpha)$, так что нам надо вывести четыре формулы.

  Начнём с формулы $\exists\xi\, \varphi \to \neg\forall\xi\, \neg\varphi$. Имея в виду правило Бернайса, достаточно вывести формулу $\varphi \to \neg\forall\xi\, \neg\varphi$. Тавтология $(B \to \neg A) \to (A \to \neg B)$ позволяет вместо этого выводить формулу $\forall\xi\, \neg\varphi \to \neg\varphi$, которая является аксиомой.

  В только что выведенной формуле $\exists\xi\, \varphi \to \neg\forall\xi\, \neg\varphi$ можно в качестве φ взять любую формулу, в том числе начинающуюся с отрицания. Подставив $\neg\varphi$ вместо φ, получим

$$\exists\xi\, \neg\varphi \to \neg\forall\xi\, \neg\neg\varphi,$$

  где $\neg\neg\varphi$ доказуемо эквивалентна φ и потому может быть заменена на φ. После этого правило контрапозиции (если из A следует $\neg B$, то из B следует $\neg A$) даёт

$$\forall\xi\, \varphi \to \neg\exists\xi\, \neg\varphi.$$

  Выведем третью формулу: $\neg\exists\xi\, \neg\varphi \to \forall\xi\, \varphi$. По правилу Бернайса достаточно вывести $\neg\exists\xi\, \neg\varphi \to \varphi$, что после контрапозиции превращается в аксиому $\neg\varphi \to \exists\xi\,\neg\varphi$.

Четвёртая формула получится, если заменить в третьей φ на $\neg\varphi$ и применить контрапозицию.

Выводимость из посылок

В исчислении высказываний важную роль играло понятие выводимости из посылок и связанная с ним лемма о дедукции (с. 51). Для исчисления предикатов ситуация немного меняется. Если разрешить использовать посылки наравне с аксиомами безо всяких ограничений, то утверждение, аналогичное лемме о дедукции, будет неверным. Например, из формулы $A(x)$ можно вывести формулу $\forall x\,A(x)$ (как мы видели на с. 167 при обсуждении правила обобщения). Но импликация $A(x) \to \forall x\,A(x)$ не является выводимой (поскольку не общезначима).

Поэтому мы ограничимся случаем, когда все посылки являются замкнутыми формулами. Пусть Γ — произвольное множество замкнутых формул рассматриваемой нами сигнатуры σ. (Такие множества называют *теориями* в сигнатуре σ.) Говорят, что формула A *выводима из* Γ, если её можно вывести, используя наравне с аксиомами формулы из Γ. Как и для исчисления высказываний, мы пишем $\Gamma \vdash A$. Выводимые из Γ формулы называют также *теоремами* теории Γ.

Лемма о дедукции для исчисления предикатов. Пусть Γ — множество замкнутых формул, а A — замкнутая формула. Тогда $\Gamma \vdash (A \to B)$ тогда и только тогда, когда $\Gamma \cup \{A\} \vdash B$.

Доказательство проходит по той же схеме, что и для исчисления высказываний (с. 51): к формулам $C_1, \ldots, C_n$, образующим вывод $C_n = B$ из $\Gamma \cup \{A\}$, мы приписываем посылку A и дополняем полученную последовательность

$$(A \to C_1), \ldots, (A \to C_n)$$

до вывода из Γ. Отличие от пропозиционального случая в том, что в выводе могут встречаться правила Бернайса.

Например, от выводимости формулы

$$A \to (\psi \to \varphi)$$

надо перейти к выводимости формулы

$$A \to (\psi \to \forall\xi\,\varphi)$$

(в которой переменная ξ не является параметром формулы ψ). Это несложно сделать, если заметить, что в силу пропозициональных тавтологий можно перейти от $A \to (\psi \to \varphi)$ к $(A \wedge \psi) \to \varphi$, затем применить правило Бернайса (это законно, так как переменная ξ не является параметром формулы ψ, а формула A замкнута по предположению). Получится выводимая из Γ формула

$$(A \wedge \psi) \to \forall\xi\,\varphi,$$

и остаётся вернуть A из конъюнкции в посылку.

Сходным образом рассматривается и второе правило Бернайса. Если выводима формула $A \to (\varphi \to \psi)$, то в силу пропозициональных тавтологий выводима формула $\varphi \to (A \to \psi)$, к которой можно применить правило Бернайса и получить $\exists\xi\,\varphi \to (A \to \psi)$, после чего вернуть A назад с помощью пропозициональной тавтологии. Лемма о дедукции доказана.

Отметим теперь несколько полезных свойств выводимости из посылок.

- Если $\Gamma \vdash A$ и $\Gamma' \supset \Gamma$, то $\Gamma' \vdash A$. (Очевидно следует из определения.)
- Если $\Gamma \vdash A$, то существует конечное множество $\Gamma' \subset \Gamma$, для которого $\Gamma' \vdash A$. (Вывод конечен и потому может использовать лишь конечное число формул.)
- Если Γ конечно и равно $\{\gamma_1, \ldots, \gamma_n\}$, то $\Gamma \vdash A$ равносильно выводимости (без посылок) формулы

$$(\gamma_1 \wedge \ldots \wedge \gamma_n) \to A.$$

В самом деле, если $\{\gamma_1, \ldots, \gamma_n\} \vdash A$, то многократное применение леммы о дедукции даёт

$$\vdash \gamma_1 \to (\gamma_2 \to (\ldots(\gamma_n \to A)\ldots)),$$

и остаётся воспользоваться надлежащей пропозициональной тавтологией. (В обратную сторону рассуждение также проходит без труда.)

- Комбинируя три предыдущих замечания, приходим к такому эквивалентному определению выводимости из посылок: $\Gamma \vdash A$, если найдутся формулы $\gamma_1, \ldots, \gamma_n \in \Gamma$, для которых

$$\vdash \gamma_1 \to (\gamma_2 \to (\ldots(\gamma_n \to A)\ldots)).$$

  Это определение имеет смысл и для формул с параметрами, так что если уж определять выводимость из посылок с параметрами (чего обычно избегают), то именно так.

Понятие выводимости из посылок позволяет переформулировать теорему о корректности исчисления предикатов.

Говорят, что интерпретация M сигнатуры σ является *моделью* теории Γ, если все формулы из Γ истинны в M.

Теорема 44 (о корректности; переформулировка). Все теоремы теории Γ истинны в любой модели M теории Γ.

$\lhd$ Если формула A является теоремой теории Γ (т. е. $\Gamma \vdash A$), найдутся формулы $\gamma_1, \ldots, \gamma_n \in \Gamma$, для которых

$$\vdash \gamma_1 \to (\gamma_2 \to (\ldots(\gamma_n \to A)\ldots)).$$

По теореме о корректности (в уже известной нам форме) эта формула будет истинна во всех интерпретациях, в частности в M. Поскольку $\gamma_1, \ldots, \gamma_n$ истинны в M, то и формула A истинна в M (на любой оценке). $\rhd$

В следующих задачах — и только в них — знак $\vdash$ понимается в описанном выше смысле (в посылках допускаются параметры):

95. Пусть Γ — множество произвольных (не обязательно замкнутых) формул. **(а)** Пусть существует «вывод» некоторой формулы φ, в котором наравне с аксиомами используются формулы из Γ, при этом все применения правил Бернайса предшествуют появлению формул из Γ. Покажите, что $\Gamma \vdash \varphi$. Покажите, что верно и обратное утверждение. **(б)** Покажите, если в «выводе» формулы φ наравне с аксиомами используются формулы из Γ, но правила Бернайса не применяются по переменным, свободным в Γ, то $\Gamma \vdash \varphi$.

96. Покажите, что правила Бернайса можно переписать так:

$$\frac{\Gamma, A \vdash B}{\Gamma, A \vdash \forall\xi\, B} \qquad \frac{\Gamma, B \vdash A}{\Gamma, \exists\xi\ \vdash A},$$

где переменная ξ не является параметром формулы A, а также параметром формул из Γ. (В первом правиле мы для симметрии выделили формулу A, хотя она ничем не отличается от формул из Γ).

Переменные и константы

Отметим ещё несколько простых свойств выводимости, которые нам потребуются:

Лемма о свежих константах. Пусть выводима формула $\varphi(c/\xi)$, где φ — произвольная формула, ξ — переменная, c — константа, не входящая в формулу φ. Тогда выводима и формула φ.

Интуитивный смысл леммы: если мы доказали что-то про «свежую» константу c (не запятнавшую себя участием в формуле φ), то фактически мы доказали формулу φ для произвольных значений переменной.

Доказательство леммы. По условию существует вывод формулы $\varphi(c/\xi)$. Возьмём «свежую» переменную η, не встречающуюся в этом выводе, и всюду заменим в нём константу c на эту переменную. При этом вывод останется выводом, так как правила обращения с переменными и константами ничем не отличаются (кванторов по новой переменной в нём нет, так что корректные подстановки останутся корректными и применения правил Бернайса останутся допустимыми). Таким образом, выводима формула $\varphi(\eta/\xi)$.

По правилу обобщения выводима формула $\forall\eta\,\varphi(\eta/\xi)$. Осталось применить аксиому $\forall\eta\,\varphi(\eta/\xi) \to \varphi(\eta/\xi)(\xi/\eta)$; подстановка в правой части корректна и даёт формулу φ, так как сначала мы заменили свободные вхождения ξ на η, а затем обратно (так что в зону действия кванторов по ξ они попасть не могли). Лемма доказана.

97. Сформулируйте и докажите аналогичную лемму для нескольких констант.

Аналогичное рассуждение позволяет доказать и другое утверждение, которое нам потребуется:

Лемма о добавлении констант. Пусть формула φ некоторой сигнатуры σ выводима в исчислении предикатов расширенной сигнатуры σ', полученной из σ добавлением новых констант. Тогда φ выводима и в исчислении предикатов сигнатуры σ.

Доказательство. Пусть формула φ, не содержащая новых констант, имеет вывод, в котором новые константы встречаются. Как их оттуда удалить? Легко понять, что их можно заменить на свежие переменные, не входящие в вывод, и он останется выводом, но уже без новых констант. Лемма доказана.

На самом деле эта лемма верна для произвольного расширения сигнатуры (можно добавлять не только константы, но и функциональные символы любой валентности, а также предикатные символы). Чтобы удалить новые символы из вывода, поступаем так. Все термы вида $f(\ldots)$, где f — добавленный функциональный символ, мы заменяем на новую переменную (можно взять одну и ту же переменную для всех новых символов и всех их вхождений). Все атомарные формулы с новыми предикатными символами заменяем на какую-либо замкнутую формулу (одну и ту же; какая именно формула, роли не играет).

98. Проведите это рассуждение подробно.

Таким образом, мы можем говорить о выводимости формулы, не уточняя, в какой именно сигнатуре (содержащей все использованные в формуле предикатные и функциональные символы) мы ищем её вывод.

Если принять теорему о полноте, по которой выводимость равносильна общезначимости, независимость выводимости от сигнатуры становится очевидной: истинность формулы не зависит от интерпретации символов, которые в неё не входят. (Если интерпретировать отсутствующие в формуле символы как постоянные функции и предикаты, мы приходим к синтаксическому рассуждению, упомянутому выше.)

4.5. Полнота исчисления предикатов

В этом разделе мы докажем, что всякая общезначимая формула выводима в исчислении предикатов. Мы будем следовать схеме, использованной в разделе 2.2, и введём понятия непротиворечивой и полной теории.

Фиксируем некоторую сигнатуру σ. Пусть Γ — теория в сигнатуре σ, то есть произвольное множество замкнутых формул этой сигнатуры. Говорят, что теория Γ *противоречива*, если в ней выводится некоторая формула φ и её отрицание $\neg\varphi$. В этом случае из Γ выводится любая формула, так как имеется аксиома $\neg A \to (A \to B)$. Если теория Γ не является противоречивой, то она называется *непротиворечивой*.

99. Докажите, что теория противоречива тогда и только тогда, когда в ней выводится формула $\varphi \wedge \neg\varphi$ (здесь φ — произвольная формула сигнатуры).

Непосредственно из определения следует, что всякое подмножество непротиворечивого множества непротиворечиво. Кроме того, если бесконечное множество противоречиво, то некоторое его конечное подмножество тоже противоречиво (поскольку в выводе участвует лишь конечное число формул).

Синтаксическое понятие непротиворечивости мы будем сравнивать с семантическим понятием совместности. Пусть имеется некоторая интерпретация M сигнатуры σ. Напомним, что она называется *моделью* теории Γ, если все формулы из Γ истинны в M. Множество Γ

называется *совместным*, если оно имеет модель, то есть если все его формулы истинны в некоторой интерпретации.

Теорема 45 (о корректности; переформулировка). Любое совместное множество замкнутых формул непротиворечиво.

$\triangleleft$ Пусть все формулы из Γ истинны в некоторой интерпретации M. Может ли оказаться, что $\Gamma \vdash \varphi$ и $\Gamma \vdash \neg\varphi$ для некоторой замкнутой формулы φ? Легко понять, что нет. В самом деле, в этом случае теорема 44 (с. 177) показывает, что формулы φ и $\neg\varphi$ должны быть одновременно истинны в M, что, очевидно, невозможно. $\triangleright$

Для доказательства обратного утверждения (о совместности непротиворечивой теории) нам понадобится понятие полной теории.

Непротиворечивое множество Γ, состоящее из замкнутых формул сигнатуры σ, называется *полным* в этой сигнатуре, если для любой замкнутой формулы φ этой сигнатуры либо формула φ, либо её отрицание $\neg\varphi$ выводятся из Γ.

Другими словами, теория полна, если из любых двух формул φ и $\neg\varphi$ (соответствующей сигнатуры) ровно одна является теоремой этой теории.

Полное множество можно получить, взяв какую-либо интерпретацию и рассмотрев все замкутые формулы, истинные в этой интерпретации. (Впоследствии мы увидим, что любое полное множество может быть получено таким способом — это легко следует из теоремы 46.)

В определении полноты существенно, что мы ограничиваемся замкнутыми формулами той же сигнатуры. Например, если мы возьмём одноместный предикатный символ S, не входящий в Γ, то формулы из Γ про него ничего не утверждают, и потому, скажем, ни формула $\forall x\, S(x)$, ни её отрицание не выводимы из Γ. Замкнутость формулы φ тоже важна. Например, множество всех истинных в натуральном ряду формул сигнатуры $(=,<)$ полно, но ни формула $x = y$, ни формула $x \neq y$ из него не выводятся, иначе по правилу обобщения мы получили бы ложную в $\mathbb{N}$ формулу $\forall x \forall y\,(x = y)$ или $\forall x \forall y\,(x \neq y)$.

Полное множество подобно мировоззрению человека, достигшего предела умственного развития: на всё, что входит в круг его понятий (выражается формулой сигнатуры σ), он имеет точку зрения. Но это не относится ни к формулам большей сигнатуры (содержащим новые для него понятия), ни к формулам с параметрами (поскольку значения параметров не фиксированы).

Теперь мы готовы к доказательству основного результата этого раздела.

Теорема 46 (полнота исчисления предикатов, сильная форма). Любая непротиворечивая теория совместна.

$\triangleleft$ Напомним, как мы доказывали аналогичное утверждение для высказываний. Мы расширяли наше непротиворечивое множество Γ до полного множества Γ', а потом полагали пропозициональную переменную p истинной, если $\Gamma' \vdash p$. Здесь этого будет недостаточно, как мы увидим (например, непонятно, откуда брать носитель искомой модели). Но начало рассуждения будет таким же.

Лемма 1. Для всякого непротиворечивого множества Γ замкнутых формул сигнатуры σ существует полное непротиворечивое множество Γ' замкнутых формул той же сигнатуры, содержащее Γ.

Доказательство повторяет рассуждение раздела 2.2: рассматривая по очереди замкнутые формулы, мы добавляем либо их, либо их отрицания в множество Γ.

Это можно сделать без труда для конечной или счётной сигнатуры (тогда множество всех замкнутых формул этой сигнатуры счётно); для общего случая надо воспользоваться трансфинитной индукцией или леммой Цорна, как объяснялось в разделе 2.2. Лемма 1 доказана.

Как же нам теперь построить модель полного множества Γ? Прежде всего надо решить, что будет носителем этой модели. Заметим, что в сигнатуре могут быть некоторые константы (функциональные символы валентности 0). Им должны соответствовать некоторые элементы носителя. Кроме того, замкнутым термам (которые не содержат никаких переменных, только константы) также должны соответствовать элементы носителя. Попробуем взять в качестве носителя как раз множество T всех замкнутых термов нашей сигнатуры. При этом понятно, как надо определять сигнатурные функции на этом множестве: функция, соответствующая символу f валентности k, отображает замкнутые термы $t_1, \ldots, t_k$ в терм $f(t_1, \ldots, t_k)$. (Это определение никак не зависит от Γ.)

Предикаты на этом множестве определяем так: если A — предикатный символ, а $t_1, \ldots, t_n$ — замкнутые термы, то предикат, соответствующий символу A, истинен на термах $t_1, \ldots, t_n$, если формула $A(t_1, \ldots, t_n)$ выводима из Γ.

Тем самым интерпретация полностью описана, и мы хотели бы доказать, что все формулы из Γ в ней истинны. Мы будем доказывать по индукции такой факт: если $\Gamma \vdash \varphi$, то формула φ истинна в построенной интерпретации, а если $\Gamma \vdash \neg\varphi$, то формула φ ложна.

Однако без дополнительных предположений о множестве Γ этот план обречён на неудачу, поскольку замкнутых термов может быть совсем мало (или даже вовсе не быть), в то время как соответствующая теория не имеет конечных моделей. Если начать индуктивное рассуждение, то выяснится, что трудность возникает в случае, когда формула φ начинается с квантора. Например, может оказаться, что формула $\exists x\, A(x)$ выводима из множества Γ, в то время как ни для какого замкнутого терма t формула $A(t)$ не выводима из Γ. Тогда формула $\exists x\, A(x)$ будет ложной в описанной нами модели (хотя выводимой). Чтобы преодолеть эту трудность, мы наложим дополнительные требования на множество Γ.

Назовём теорию (множество замкнутых формул сигнатуры σ) *экзистенциально полной* в сигнатуре σ, если для всякой формулы $\exists\xi\,\varphi$ сигнатуры σ, выводимой из Γ, найдётся замкнутый терм t этой сигнатуры, для которого $\Gamma \vdash \varphi(t/\xi)$.

Если множество Γ полно и экзистенциально полно, то описанная выше конструкция с замкнутыми термами даёт его модель. Прежде чем проверять это, покажем, как расширить Γ до полного и экзистенциально полного множества. Ключевую роль здесь играет такая лемма:

Лемма 2. Пусть Γ — непротиворечивое множество замкнутых формул, из которого выводится замкнутая формула $\exists\xi\,\varphi$. Пусть c — константа, не встречающаяся ни в Γ, ни в φ. Тогда множество Γ останется непротиворечивым после добавления формулы $\varphi(c/\xi)$.

(Замечание. Здесь и далее, говоря о непротиворечивости и выводимости, мы не уточняем, в какой сигнатуре строятся выводы: все наши сигнатуры будут отличаться лишь набором констант, и лемма о добавлении констант на с. 179 даёт нам такое право.)

Доказательство леммы 2. Пусть Γ становится противоречивым после добавления формулы $\varphi(c/\xi)$. Отсюда следует (используем подходящую пропозициональную тавтологию), что отрицание этой формулы выводится из Γ, то есть выводима формула $\gamma \to \neg\varphi(c/\xi)$, где γ — конъюнкция конечного числа формул из Γ. По лемме о свежих константах (с. 178) выводима формула $\gamma \to \neg\varphi$ (напомним, что c не входит ни в φ, ни в γ). Контрапозиция даёт формулу $\varphi \to \neg\gamma$, а правило Бернайса — формулу $\exists\xi\,\varphi \to \neg\gamma$. По предположению формула $\exists\xi\,\varphi$ выводима из Γ, и множество Γ оказывается противоречивым. Лемма 2 доказана.

100. Докажите такое усиление леммы 2: при добавлении в Γ формулы $\varphi(c/\xi)$ (в предположениях леммы) множество выводимых из Γ формул исходной сигнатуры (без константы c) не меняется.

Лемма 3. Пусть Γ — непротиворечивое множество замкнутых формул сигнатуры σ. Тогда существует расширение сигнатуры σ новыми константами и непротиворечивое, полное и экзистенциально полное (в расширенной сигнатуре) множество Γ' замкнутых формул, содержащее Γ.

Доказательство. Пусть сигнатура конечна или счётна. Тогда формул вида $\exists\xi\,\varphi$, выводимых из Γ, не более чем счётное число. К каждой из них по очереди будем применять лемму 2, вводя новую константу. Согласно этой лемме, на каждом шаге множество Γ остаётся непротиворечивым, поэтому оно будет непротиворечивым и после добавления счётного числа формул (вывод противоречия затрагивает лишь конечное число формул).

Однако нельзя утверждать, что полученное множество будет экзистенциально полным в новой сигнатуре, поскольку про формулы вида $\exists\xi\,\varphi$ с добавленными константами мы ничего не знаем. Пополним это множество, применив лемму 1, и повторим рассуждение: для каждой выводимой формулы, начинающейся с квантора существования, введём новую константу и т. д.

Затем снова пополним его, снова добавим константы, снова пополним и так сделаем счётное число раз. Объединение всех полученных множеств будет непротиворечивым, полным и экзистенциально полным. В самом деле, оно непротиворечиво, так как противоречие должно выводиться из конечного числа формул (и поэтому должно появиться уже на конечном шаге). Оно полно: любая замкнутая формула φ содержит конечное число новых констант, поэтому на каком-то шаге пополнения она или её отрицание станут выводимыми. Наконец, построенное множество экзистенциально полно по той же причине: всякая формула содержит конечное число новых констант, потому на следующем шаге для неё предусмотрена своя константа.

Что меняется, если сигнатура несчётна? Тогда мы уже не можем рассматривать все экзистенциальные формулы по очереди, и надо обрабатывать их все сразу. При этом противоречие не появится: в самом деле, оно использовало бы лишь конечное число добавленных формул, а для конечного числа всё уже доказано.

После этого доказательство проходит как раньше (мы по-прежнему делаем счётное число чередующихся пополнений множества и расширений сигнатуры).

Лемма 3 доказана.

Последним шагом в доказательстве теоремы о полноте (всякое непротиворечивое множество замкнутых формул совместно) является такая лемма:

Лемма 4. Пусть Γ — полное и экзистенциально полное множество замкнутых формул некоторой сигнатуры σ. Тогда существует интерпретация M сигнатуры σ, в которой истинны все формулы из Γ.

Мы уже говорили, как надо строить такую интерпретацию. Повторим это более подробно. Рассмотрим все замкнутые термы сигнатуры σ, то есть термы, не содержащие переменных, а только функциональные символы и константы. (Такие термы существуют, поскольку теория Γ экзистенциально полна.) Это множество будет носителем интерпретации.

Как интерпретировать функциональные символы, понятно (это не зависит от множества Γ): если символ f имеет валентность n, то ему соответствует функция, которая отображает n замкнутых термов $t_1, \ldots, t_n$ в замкнутый терм $f(t_1, \ldots, t_n)$. Константы (функциональные символы валентности 0) интерпретируются сами собой.

Интерпретация предикатных символов такова. Пусть A — предикатный символ валентности n. Чтобы узнать, истинен ли соответствующий ему предикат на замкнутых термах $t_1, \ldots, t_n$, надо составить атомарную формулу $A(t_1, \ldots, t_n)$ и выяснить, что выводится из Γ — сама эта формула или её отрицание. (Здесь мы используем полноту.) В первом случае предикат будет истинным, во втором — ложным.

Индукцией по числу логических связок и кванторов в замкнутой формуле φ сигнатуры σ докажем такое утверждение:

$$\Gamma \vdash \varphi \Leftrightarrow \varphi \text{ истинна в } M.$$

Для атомарных формул это верно по построению интерпретации M.

Для пропозициональных связок рассуждение ничем не отличается от приведённого в разделе 2.2. Нам нужно проверить, что выводимость из Γ подчиняется тем же правилам, что и истинность:

$$\begin{gathered}\Gamma \vdash \neg A \Leftrightarrow \Gamma \nvdash A,\\ \Gamma \vdash A \wedge B \Leftrightarrow \Gamma \vdash A \text{ и } \Gamma \vdash B,\\ \Gamma \vdash A \vee B \Leftrightarrow \Gamma \vdash A \text{ или } \Gamma \vdash B,\\ \Gamma \vdash A \to B \Leftrightarrow \Gamma \nvdash A \text{ или } \Gamma \vdash B.\end{gathered}$$

Все эти свойства несложно доказать. Первое из них выражает полноту (и непротиворечивость — напомним, что по определению полная теория всегда непротиворечива) множества Γ. Остальные свойства легко проверить, если иметь в виду, что все частные случаи пропозициональных тавтологий выводимы.

Пусть теперь формула φ имеет вид $\exists\xi\,\psi$, где ψ — формула с единственным параметром ξ (или без параметров). Предположим, что она выводима из Γ. Тогда в силу экзистенциальной полноты найдётся константа c, для которой $\Gamma \vdash \psi(c/\xi)$. Формула $\psi(c/\xi)$ имеет меньшее число логических связок, поэтому к ней можно применить предположение индукции и заключить, что она истинна в M. Тогда формула ψ истинна на оценке $\xi \mapsto c$ (см. лемму 2 на с. 169 и замечание после неё), поэтому формула $\exists\xi\,\psi$ истинна в M.

Напротив, пусть формула $\exists\xi\,\psi$ истинна в M. Тогда (по определению истинности) найдётся элемент (замкнутый терм) t, для которого ψ истинна на оценке $\xi \mapsto t$ и потому формула $\psi(t/\xi)$ истинна в M. По предположению индукции формула $\psi(t/\xi)$ выводима из Γ. Осталось воспользоваться тем, что формула $\psi(t/\xi) \to \exists\xi\,\psi$ является аксиомой (напомним, подстановка замкнутого терма всегда корректна).

Наконец, рассмотрим случай, когда формула φ имеет вид $\forall\xi\,\psi$. Пусть она выводима из Γ. Формула $\forall\xi\,\psi \to$ $\to \psi(t/\xi)$ является аксиомой для любого замкнутого терма t. Поэтому и формула $\psi(t/\xi)$ выводима из Γ. В ней меньше логических связок, чем в φ, поэтому по предположению индукции она истинна в M. Значит, формула ψ истинна на любой оценке $\xi \mapsto t$, и потому формула $\forall\xi\,\psi$ истинна в M.

Если формула $\forall\xi\,\psi$ не выводима из Γ, то из Γ выводится её отрицание. Оно, как мы видели, доказуемо эквивалентно формуле $\exists\xi\,\neg\psi$. Поэтому в силу экзистенциальной полноты выводима формула $\neg\psi(c/\xi)$ для некоторой константы c. Эта формула истинна, поэтому ψ ложна при некотором значении переменной ξ, так что формула $\forall\xi\,\psi$ ложна в M.

Таким образом, мы доказали, что всякое непротиворечивое множество замкнутых формул имеет модель (расширив его до полного и экзистенциально полного, у которого есть модель из замкнутых термов). $\triangleright$

Анализ доказательства позволяет сделать такое наблюдение:

Теорема 47. Непротиворечивое множество замкнутых формул конечной или счётной сигнатуры имеет счётную модель.

$\triangleleft$ В самом деле, элементами построенной нами модели являются замкнутые термы, образованные из добавленных констант и функциональных символов сигнатуры. На каждом шаге добавляется счётное множество констант, поэтому всех констант счётное число, значит, и термов счётное число. $\triangleright$

Аналогичное рассуждение с использованием свойств операций с мощностями (о которых можно прочесть в [6]) устанавливает такой факт:

Теорема 48. Всякое непротиворечивое множество формул сигнатуры σ имеет модель мощности $\max(\aleph_0, |\sigma|)$ (где $\aleph_0$ обозначает счётную мощность, а $|\sigma|$ — мощность сигнатуры).

Кстати, при доказательстве теорем 47 и 48 можно было бы сослаться на теорему Левенгейма – Сколема об элементарной подмодели (построить модель произвольной мощности, а потом уменьшить, если надо).

Возвратимся теперь к исходной формулировке теоремы о полноте.

Теорема 49 (полнота исчисления предикатов, слабая форма). Всякая общезначимая формула выводима в исчислении предикатов.

$\lhd$ Пусть формула φ замкнута. Если она невыводима, то множество $\{\neg\varphi\}$ непротиворечиво и потому совместно. В его модели формула φ будет ложной, что противоречит предположению.

Что касается незамкнутых формул, то их общезначимость и выводимость равносильна общезначимости и выводимости их замыкания. $\rhd$

Как и в разделе 2.2, из теоремы о полноте можно вывести такое следствие:

Теорема 50 (компактность для исчисления предикатов). Пусть Γ — множество замкнутых формул некоторой сигнатуры, и любое его конечное подмножество имеет модель. Тогда и само множество Γ имеет модель.

$\lhd$ В самом деле, по теореме о полноте (и корректности, если быть точным) наличие модели (совместность) равносильно непротиворечивости. А по определению противоречивость затрагивает лишь конечное число формул из Γ. $\rhd$

101. Покажите, что теорема о полноте в сильной форме является следствием теоремы компактности и теоремы о полноте в слабой форме. (Указание: если множество Γ не имеет модели, то его конечная часть не имеет модели, поэтому формула $\langle\ldots\rangle$ общезначима, поэтому...)

Прямое доказательство теоремы компактности (без использования понятия выводимости) мы дадим в следующей главе (раздел 5.6).

Ещё один важный результат, вытекающий из теоремы о полноте — совпадение синтаксического понятия выводимости и семантического понятия следования. Пусть дана некоторая сигнатура σ. Рассмотрим множество Γ замкнутых формул этой сигнатуры (такие множества мы называем теориями в сигнатуре σ) и ещё одну замкнутую формулу φ. Говорят, что φ *семантически сле-*

дует из Γ, если φ истинна во всякой модели теории Γ, то есть во всякой интерпретации сигнатуры σ, где истинны все формулы из Γ. (Обозначение: $\Gamma \vDash \varphi$.)

Теорема 51.

$$\Gamma \vdash \varphi \Leftrightarrow \Gamma \vDash \varphi.$$

$\lhd$ Если $\Gamma \vdash \varphi$, то $\Gamma \vDash \varphi$ (как мы видели в теореме 44 на с. 177).

Напротив, пусть φ не выводима из Γ. Тогда теория $\Gamma \cup \{\neg\varphi\}$ непротиворечива и (в силу теоремы о полноте) имеет модель. Значит φ не следует из Γ. $\rhd$

102. Какими нужно взять φ и Γ в этой теореме, чтобы получить приведённые ранее формулировки теоремы о полноте? (Ответ. При $\varphi =\perp$ (тождественно ложная формула) получаем сильную форму теоремы о полноте, при $\Gamma = \varnothing$ — слабую.)

4.6. Переименование переменных

В этом разделе мы попытаемся аккуратно разобраться с простым вопросом о том, почему и как можно переименовывать связанные переменные, не меняя смысла формул. Мы уже видели, что формулы $\forall x\, A(x)$ и $\forall y\, A(y)$ доказуемо эквивалентны (с. 174), то есть их эквивалентность доказуема в исчислении предикатов. Сейчас мы хотим доказать общее утверждение об этом.

Корректная формулировка утверждения о переименовании переменных требует осторожности. Например, нельзя сказать, что формула $\forall\xi\,\varphi$ всегда эквивалентна $\forall\eta\,\varphi(\eta/\xi)$. Прежде всего, подстановка может быть некорректной, как в случае формул

$$\forall\xi\forall\eta\, B(\xi,\eta) \quad \text{и} \quad \forall\eta\forall\eta\, B(\eta,\eta)$$

(легко понять, что эти формулы не эквивалентны). Но даже если подстановка корректна, формулы могут не быть эквивалентными, как в случае формул

$$\forall\xi\, B(\xi,\eta) \quad \text{и} \quad \forall\eta\, B(\eta,\eta).$$

Как же сформулировать утверждение правильно?

Нагляднее всего, видимо, сделать так. Давайте заключим в рамку все связанные вхождения всех переменных (в том числе вхождения после кванторов). После этого соединим линиями переменную после квантора и все её связанные вхождения в зоне действия этого квантора. Свободные вхождения переменных остаются при этом без рамок. Получится что-то вроде

$$\forall \boxed{x}\ (\exists \boxed{z}\ B(\boxed{x}, \boxed{z}) \land C(\boxed{x})) \land D(x,y,z)$$

Если после этого стереть переменные внутри рамок, получится *схема* формулы, которая содержит всю существенную информацию о ней. Будем называть две формулы *подобными* (отличающимися лишь именами связанных переменных), если они имеют одну и ту же схему.

Теорема 52 (переименование связанных переменных). Подобные формулы доказуемо эквивалентны.

$\lhd$ Докажем две простые леммы:

Лемма 1. Если формула φ не содержит переменной η (ни связанно, ни свободно), то формулы

$$\forall\xi\,\varphi \quad \text{и} \quad \forall\eta\,\varphi(\eta/\xi)$$

доказуемо эквивалентны.

Доказательство. В самом деле, подстановка корректна, так как в φ нет кванторов по η. Поэтому выводима формула

$$\forall\xi\,\varphi \to \varphi(\eta/\xi).$$

Левая часть её не содержит переменной η, поэтому по правилу Бернайса можно вывести

$$\forall\xi\,\varphi \to \forall\eta\,\varphi(\eta/\xi).$$

В обратную сторону: подстановка ξ вместо η в формулу $\varphi(\eta/\xi)$ корректна (поскольку η была подставлена вместо свободных вхождений ξ, при обратной подстановке переменная ξ не попадёт в область действия кванторов по ней) и даёт формулу φ. Поэтому формула

$$\forall\eta\,\varphi(\eta/\xi) \to \varphi(\eta/\xi)(\xi/\eta)$$

или, что то же самое,

$$\forall\eta\,\varphi(\eta/\xi) \to \varphi$$

является аксиомой. Осталось применить правило Бернайса, заметив, что в левую часть переменная ξ свободно не входит (все свободные вхождения были заменены на η). Лемма 1 доказана.

Аналогичное утверждение для квантора существования доказывается точно так же.

Лемма 2. Замена подформулы на доказуемо эквивалентную даёт доказуемо эквивалентную формулу.

Доказательство. Как мы видели на с. 173, доказуемая эквивалентность сохраняется после навешивания квантора: если $\alpha \simeq \alpha'$, то $\forall\xi\,\alpha \simeq \forall\xi\,\alpha'$ и $\exists\xi\,\alpha \simeq \exists\xi\,\alpha'$ (символ $\simeq$ здесь обозначает доказуемую эквивалентность). Кроме того, из $\alpha \simeq \alpha'$ и $\beta \simeq \beta'$ следует, что $(\alpha \wedge \beta) \simeq (\alpha' \wedge \beta')$, $(\alpha \vee \beta) \simeq (\alpha' \vee \beta')$, $(\alpha \to \beta) \simeq (\alpha' \to \beta')$ и $\neg\alpha \simeq \neg\alpha'$. (В этом легко убедиться, написав подходящие пропозициональные тавтологии.)

Теперь утверждение леммы легко доказать индукцией (начав с заменённой подформулы и рассматривая всё более длинные части формулы). Лемма 2 доказана.

Леммы 1 и 2 позволяют нам заменять переменные внутри рамок схемы на новые (ранее не использованные) переменные, получая доказуемо эквивалентную и подобную исходной формулу. Такими заменами можно из двух подобных формул получить третью, используя для замены одни и те же переменные. При этом обе исходные формулы доказуемо эквивалентны третьей, а значит, и друг другу.

(Использование третьей формулы существенно: мы не можем преобразовать первую формулу сразу во вторую, так как при замене переменных в рамках может не выполняться условие леммы 1.) ▷

Аккуратное обращение со связанными и свободными переменными — традиционная головная боль авторов учебников по логике. Наиболее радикальный подход — вообще изгнать связанные переменные, заменив их квадратиками со связями между ними. Тогда при подстановке можно ни о чём не заботиться. Зато формулы перестают быть последовательностями символов, а становятся объектами со сложной структурой. (Этот подход использован в книге Бурбаки *Теория множеств* [3].)

Менее радикальный вариант состоит в том, чтобы разделить переменные на два типа — свободные и связанные. Так делается, например, в классической книге Гильберта и Бернайса *Основания математики* [8]. Тогда можно смело подставлять терм вместо свободной переменной, зато при навешивании квантора надо заменять свободную переменную на связанную.

Ещё один вариант — договориться, что при подстановке терма вместо свободной переменных автоматически происходит переименование связанных переменных, создающих коллизии.

Всё это, конечно, мелочи — но досадные, особенно если стремиться к краткости, ясности и наглядности. Следы мучительных раздумий на подобные темы видны в примечании на с. 101–102 книги Клини *Математическая логика* [16]: «Гильберт и Бернайс ⟨...⟩ и другие авторы используют для обозначения свободных и связанных переменных разные буквы ⟨...⟩ Мы следовали этому правилу в течение десятилетия ⟨...⟩ Сейчас же мы твёрдо убеждены, что использование единого списка переменных для свободных и замкнутых вхождений даёт небольшое, но чувствительное преимущество».

С этим связан и другой выбор: как определять истинность формул. Тут есть две возможности: можно определять истинность формулы на оценке (при данных значениях параметров), а можно говорить только о замкнутых формулах, вводя константы для всех элементов интерпретации. И тот, и другой способы имеют недостатки, а выбор нами первого подхода — результат не единодушия авторов, а волевого решения.

4.7. Предварённая нормальная форма

Говорят, что формула находится в *предварённой нормальной форме*, если все кванторы в ней вынесены налево, то есть если она имеет вид

$$Q_1\xi_1 \dots Q_k\xi_k\varphi,$$

где $Q_1, \dots, Q_k$ — кванторы всеобщности или существования, $\xi_1, \dots, \xi_k$ — переменные, а φ — бескванторная формула. Эта формула может иметь параметры (если формула φ имеет параметры, отличные от $\xi_1, \dots, \xi_k$).

Основной результат этого раздела гласит, что всякая формула (доказуемо) эквивалентна некоторой формуле в предварённой нормальной форме (*предварённой формуле*). Мы докажем его, одновременно построив некоторую классификацию формул (в каком-то смысле отражающую их «логическую сложность»). В качестве меры сложности можно было бы взять число кванторов в предварённой нормальной форме. Но правильнее учитывать число групп кванторов (считая одноимённые рядом стоящие кванторы за один).

Говорят, что предварённая формула является Σ_n-формулой, если её кванторная приставка содержит n групп кванторов, причём первыми стоят кванторы существования. Если первыми стоят кванторы всеобщности, говорят о классе Π_n. (Аналогичные обозначения используются в теории алгоритмов для классификации арифметических множеств, см. [5]).

Пример: формула $\forall x \exists y \exists z \forall u\, (A(x,u,z) \to B(z,u))$ принадлежит классу Π_3, формула $\exists u \forall v\, C(u,v)$ принадлежит классу Σ_2, а формула $\forall x\, (A(x) \to \exists y B(x,y))$ вообще не находится в предварённой нормальной форме.

103. Указать формулу в предварённой нормальной форме, доказуемо эквивалентную последней из перечисленных формул.

Нас интересует, что происходит с измеряемой таким образом «логической сложностью» формулы при логических операциях. Начнём с совсем простых наблюдений.

- Всякая формула из класса Σ_n или Π_n доказуемо эквивалентна формуле из класса Σ_{n+1}, а также формуле из класса Π_{n+1}. В самом деле, если формула ψ не имеет параметра η, то она будет доказуемо эквивалентна формулам $\exists\eta\,\psi$ и $\forall\eta\,\psi$ (одна импликация является аксиомой, другая получается из $\psi \to \to \psi$ по правилу Бернайса). Таким образом, можно добавить фиктивный квантор в начало кванторной приставки или в её конец; во втором случае надо сослаться на лемму 2 раздела 4.6 (с. 192).

- Отрицание любой формулы из класса Σ_n доказуемо эквивалентно некоторой формуле из класса Π_n и наоборот. В самом деле, мы видели, что $\neg\exists\xi\,\psi$ выводимо эквивалентно $\forall\xi\,\neg\psi$ и наоборот (с. 174), так что отрицание можно проносить внутрь, меняя по ходу дела кванторы на двойственные.

- Покажем, что конъюнкция двух формул из Π_1 доказуемо эквивалентна некоторой формуле из Π_1. Например, конъюнкция $\forall x\,A(x) \wedge \forall y\,B(y)$ доказуемо эквивалентна формуле $\forall x\forall y\,(A(x) \wedge B(y))$. В самом деле, используя аксиомы про квантор всеобщности, можно из $\forall x\,A(x)$ вывести $A(x)$, а из $\forall y\,B(y)$ вывести $B(y)$, поэтому из их конъюнкции выводится $A(x) \wedge B(y)$, после чего можно навесить два квантора всеобщности. В другую сторону: выводим формулу $\forall x\forall y\,(A(x) \wedge B(y)) \to A(x)$, затем применяем правило Бернайса и т. д.

104. Покажите, что можно сэкономить один квантор и использовать формулу $\forall x\,(A(x) \wedge B(x))$.

Общее рассуждение (для любых двух формул из класса Π_1) почти столь же просто, надо лишь переименовать связанные переменные, пользуясь теоремой 52 (с. 191).

- Аналогично можно доказать, что дизъюнкция двух формул из класса Σ_1 доказуемо эквивалентна некоторой формуле класса Σ_1. (Можно также перейти к двойственному классу Π_1, воспользовавшись уже известными свойствами отрицания.)

- Покажем теперь, что конъюнкция двух формул из класса Σ_1 доказуемо эквивалентна формуле класса Σ_1 и что дизъюнкция двух формул класса Π_1 доказуемо эквивалентна формуле класса Π_1. Для этого надо воспользоваться эквивалентностями вида

$$\exists x\, A(x) \wedge \exists y\, B(y) \leftrightarrow \exists x \exists y (A(x) \wedge B(y))$$

и

$$\forall x\, A(x) \vee \forall y\, B(y) \leftrightarrow \forall x \forall y (A(x) \vee B(y)).$$

Отметим кстати, что в них уже нельзя сэкономить квантор; например, формула $\exists x (A(x) \wedge B(x))$ не равносильна формуле $\exists x\, A(x) \wedge \exists x\, B(x)$. (В одном из выступлений времён начала перестройки М. С. Горбачёв сказал, что нужны «преданные делу социализма, но квалифицированные специалисты» — впрочем, в газетной публикации «но» было заменено на нейтральное «и». Так вот, их существование не вытекает из отдельного существования тех и других.)

Указанные эквивалентности, как легко видеть, общезначимы и потому выводимы. Это совсем просто понять для первой из них (чтобы найти пару объектов с заданными свойствами, надо найти отдельно первый и второй члены пары). Вторая эквивалентность немного сложнее — проще всего заметить, что она переходит в первую при добавлении отрицания. (Большая сложность отражает тот факт, что вторая эквивалентность, в отличие от первой, не является интуиционистски верной.)

- Теперь легко понять, что конъюнкция и дизъюнкция двух формул из класса Σ_n (или Π_n) доказуемо эквивалентны формулам из того же класса. В самом деле, с помощью указанных выше эквивалентностей можно слить кванторные приставки. Например, формула

$$\forall x \exists y\, A(x,y) \lor \forall u \exists v\, B(u,v)$$

доказуемо эквивалентна сначала формуле

$$\forall x \forall u\, (\exists y\, A(x,y) \lor \exists v\, B(u,v)),$$

а затем формуле

$$\forall x \forall u \exists y \exists v\, (A(x,y) \lor B(u,v)).$$

105. Как сэкономить один квантор в этом преобразовании?

Теперь всё готово для доказательства упомянутого в начале раздела результата.

Теорема 53 (о предварённой нормальной форме). Любая формула произвольной сигнатуры доказуемо эквивалентна некоторой формуле той же сигнатуры, имеющей предварённую нормальную форму.

$\triangleleft$ Индукция по построению формулы. Для атомарных формул это очевидно. Отрицание переводит формулу класса Σ_n в класс Π_n и наоборот. Конъюнкция и дизъюнкция: приведём каждую формулу к предварённой нормальной форме, затем добавим фиктивные кванторы так, чтобы они попали в один класс, а затем воспользуемся доказанным утверждением. Импликация сводится к дизъюнкции и отрицанию ($\varphi \to \psi$ доказуемо эквивалентно $\neg\varphi \lor \psi$). $\triangleright$

Отметим, что ни формулировка, ни доказательство этой теоремы не предполагают замкнутости формулы.

106. Привести к предварённой нормальной форме формулу $\forall x\, A(x) \to \forall x\, B(x)$.

107. Формулы φ и ψ принадлежат классу Σ_n. Найдём формулу в предварённой нормальной форме, выводимо эквивалентную формуле $\varphi \to \psi$. В каком классе она окажется? (Указание: возможны разные варианты.)

108. Применим описанный метод к общезначимой формуле $\exists x \forall y\, A(x,y) \to \forall y \exists x\, A(x,y)$. Какая предварённая формула получится? (Естественно, она будет общезначимой.)

4.8. Теорема Эрбрана

Естественно ожидать, что вопрос о выводимости (или общезначимости) формулы тем сложнее, чем сложнее сама формула. В этом разделе (а также в следующем) мы рассмотрим его для формул класса Σ_n и Π_n.

Начнём с самого простого случая — бескванторных формул. Пусть φ — бескванторная формула. Посмотрим, из каких атомарных формул она составлена, и заменим их на пропозициональные переменные (разные — на разные, одинаковые — на одинаковые). Получится формула логики высказываний, которую мы будем называть *прототипом* формулы φ. Имеет место следующее (почти очевидное) утверждение.

Теорема 54 (выводимость бескванторных формул). Бескванторная формула выводима (общезначима) тогда и только тогда, когда её прототип является тавтологией.

$\lhd$ Если прототип формулы φ является тавтологией, то формула φ является частным случаем пропозициональной тавтологии и потому выводима и общезначима.

Пусть прототип формулы φ не является тавтологией. Можно считать, что формула φ замкнута, поскольку свободные переменные с точки зрения общезначимости и выводимости ничем не отличаются от констант (мы уже отмечали это при доказательстве теоремы о полноте). Построим интерпретацию, где формула φ будет ложной. Носителем её будут замкнутые термы. Значения предикатов мы подберём так, чтобы атомарные формулы принимали те самые значения, которые делают прототип формулы φ ложным. Это возможно, так как значения разных атомарных формул можно выбирать независимо (это значения либо разных предикатов, либо одного и того же предиката, но на разных термах). $\triangleright$

Что можно сказать про общезначимость формул классов Π_1 и Σ_1? Для класса Π_1 всё просто: общезначимость формулы со свободными переменными равносильна общезначимости её замыкания (которое получается, если навесить кванторы всеобщности по всем переменным), поэтому формулы класса Π_1 по существу ничем не отличаются от бескванторных.

Вопрос для класса Σ_1 решается следующей теоремой:

Теорема 55 (Эрбрана). Формула $\exists\xi_1 \ldots \exists\xi_k\, \varphi$ (где формула φ — бескванторная) общезначима тогда и только тогда, когда найдётся конечный список подстановок

$$\begin{array}{c} \varphi(t_1/\xi_1, \ldots, t_k/\xi_k), \\ \varphi(u_1/\xi_1, \ldots, u_k/\xi_k), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \varphi(w_1/\xi_1, \ldots, w_k/\xi_k) \end{array}$$

(вместо переменных подставляются термы нашей сигнатуры), дизъюнкция которых общезначима.

Заметим, что дизъюнкция, о которой идёт речь в теореме, является бескванторной формулой. По теореме 54 она общезначима тогда и только тогда, когда является частным случае пропозициональной тавтологии.

Прежде чем доказывать эту теорему, приведём пример. Рассмотрим формулу

$$\exists x\, (A(c,x) \to A(x,d))$$

(в которой c и d — константы). Она общезначима; соответствующий набор состоит из подстановок c/x и d/x. В самом деле, формула

$$(A(c,c) \to A(c,d)) \vee (A(c,d) \to A(d,d))$$

истинна как при истинном $A(c,d)$, так и при ложном. Заметим, что в этом примере нам понадобились две подстановки.

$\lhd$ Доказательство теоремы Эрбрана. В одну сторону утверждение очевидно: если общезначима дизъюнкция подстановок, то общезначима формула с квантором. (Мы уже использовали это при элиминации кванторов в разделе 3.6 при доказательстве теоремы 28.)

Докажем обратное утверждение. Будем считать, что формула φ не содержит переменных, кроме $\xi_1,\ldots,\xi_k$ (как мы уже замечали, остальные переменные можно заменить константами). Рассмотрим (бесконечное) множество формул

$$\neg\varphi(t_1/\xi_1,\ldots,t_k/\xi_k)$$

для всевозможных наборов замкнутых термов $t_1,\ldots,t_k$. Если это множество противоречиво, всё доказано (тогда выводима дизъюнкция подстановок, отрицания которых используются при выводе противоречия). Если оно непротиворечиво, то существует интерпретация, в которой все эти формулы истинны. Мы не можем утверждать, что в этой интерпретации ложна формула

$$\exists\xi_1\ldots\exists\xi_k\,\varphi$$

(носитель интерпретации может содержать элементы, не являющиеся значениями замкнутых термов). Однако если мы выбросим лишние элементы и оставим только значения термов, то эта формула станет ложной, так что она не общезначима. $\rhd$

Заметим, что теорему Эрбрана можно сформулировать чисто синтаксически: если выводима Σ_1-формула $\exists\xi_1\ldots\exists\xi_k\varphi$, то можно найти конечное число подстановок, дизъюнкция которых выводима. Можно предложить и доказательство, не использующее понятия общезначимости. Такое доказательство приведено, например, в книге Клини [16] (для генценовского варианта исчисления предикатов) и в книге Шёнфилда [31] (для гильбертовского варианта). Синтаксическое доказательство (в отличие от нашего) конструктивно: по выводу Σ_1-формулы можно алгоритмически указать соответствующие термы.

Если сигнатура не содержит функциональных символов, то теорема Эрбрана позволяет алгоритмически проверить выводимость формул класса Σ_1, поскольку число возможных подстановок конечно. Это же можно сказать и про формулы класса Π_2, так как внешние кванторы всеобщности можно отбросить, не меняя выводимости.

Естественный вопрос: можно ли построить аналогичные алгоритмы для следующих классов? Отрицательный ответ даётся в следующем разделе.

4.9. Сколемовские функции

В этом разделе мы в разных формах используем ровно одну идею: утверждение

$$\forall x \exists y\, A(x, y)$$

равносильно существованию функции, которая по любому x даёт такой y, что $A(x, y)$. Это утверждение нельзя записать в виде эквивалентности

$$\forall x \exists y\, A(x, y) \Leftrightarrow \exists f \forall x\, A(x, f(x)),$$

поскольку в нашем языке нет квантора по функциям и $\exists f$ мы писать не имеем права. (Языки, содержащие кванторы по множествам и функциям, называются языками *второго порядка* и мы их не рассматриваем.)

Тем не менее это утверждение можно сформулировать и в наших терминах. Пусть, например, имеется формула φ с двумя параметрами x и y. Тогда замкнутая формула $\forall x \exists y\, \varphi$ выполнима тогда и только тогда, когда выполнима формула $\forall x \varphi(f(x)/y)$, где f — новый одноместный функциональный символ. (Аккуратный читатель поправит: надо ещё требовать, чтобы подстановка $f(x)$ вместо y была корректна. Мы уже знаем, что переменные можно переименовывать, поэтому будем легкомысленно считать, что все необходимые переименования уже сделаны.)

Аналогичное преобразование выполнимо и для произвольных предварённых формул. Например, формула

$$\forall x \forall y \exists z \forall u \exists v\, \varphi(x, y, z, u, v)$$

выполнима тогда и только тогда, когда выполнима формула

$$\forall x \forall y \forall u\, \varphi(x, y, f(x, y), u, g(x, y, u))$$

(здесь $\varphi(x, y, z, u, v)$ — формула, не имеющая параметров, кроме x, y, z, u, v, запись $\varphi(x, y, f(x, y), u, g(x, y, u))$ обозначает результат соответствующих подстановок, которые мы предполагаем корректными, а f и g — функциональные символы, не встречающиеся в формуле φ).

Сходное преобразование имеют в виду преподаватели математического анализа, которые иногда записывают определение предела ($\forall\varepsilon\exists\delta\ldots$) в несколько странной для логика форме $\forall\varepsilon\exists\delta = \delta(\varepsilon)\ldots$ — имеется в виду, что если для каждого ε найдётся δ, то это самое δ представляет собой функцию от ε.

Отметим, что это рассуждение использует аксиому выбора, когда из различных возможных (для данного ε) значений δ мы выбираем какое-то одно и объявляем его значением функции $\varepsilon(\delta)$.

109. Казалось бы, выбор v в приведённом выше примере зависит от x, y, z, u, так что следовало бы написать $\varphi(x, y, f(x, y), u, g(x, y, f(x, y), u))$ — но мы так не делаем. Почему это допустимо?

Используя описанное преобразование, мы приходим к такой теореме:

Теорема 56. Для всякой замкнутой формулы τ сигнатуры σ можно указать формулу τ' класса Π_1 сигнатуры σ с добавленными функциональными символами, которая выполнима или невыполнима одновременно с формулой τ. При этом преобразование $\tau \mapsto \tau'$ эффективно (выполняется некоторым алгоритмом).

$\triangleleft$ Приведя τ к предварённой нормальной форме, получим доказуемо эквивалентную формулу (выполнимую или невыполнимую одновременно с τ). После этого применяем описанное выше преобразование. $\triangleright$

Формула τ невыполнима тогда и только тогда, когда её отрицание общезначимо. Поэтому наши рассуждения показывают, что, скажем, формула $\neg\forall x\exists y\,\psi(x,y)$ общезначима одновременно с формулой $\neg\forall x\,\psi(x,f(x))$. Внося отрицание внутрь и заменяя $\neg\psi$ на φ, получаем такое утверждение: формулы

$$\exists x\forall y\,\varphi(x,y) \quad \text{и} \quad \exists x\,\varphi(x,f(x))$$

одновременно общезначимы. (Это утверждение чуть менее наглядно, чем двойственное ему утверждение о выполнимости.) В общем виде двойственное к теореме 56 утверждение выглядит так:

Теорема 57. Для всякой замкнутой формулы τ сигнатуры σ можно указать формулу τ' класса Σ_1 сигнатуры σ с добавленными функциональными символами, которая общезначима или необщезначима одновременно с формулой τ. При этом преобразование $\tau \mapsto \tau'$ эффективно (выполняется некоторым алгоритмом).

Заметим, что к формуле τ' можно применить теорему Эрбрана (с. 199): она общезначима тогда и только тогда, когда дизъюнкция нескольких подстановок является тавтологией.

Теорема о полноте позволяет заменить в этой формулировке общезначимость на выводимость: формулы τ и τ' одновременно выводимы. После этого естественно искать явный метод, который преобразует вывод формулы τ в вывод формулы τ' и обратно. Такой метод действительно существует, но для этого требуется более детальный анализ структуры выводов, при котором удобно пользоваться исчислениями генценовского типа.

Идея использования функций вместо групп кванторов $\forall\exists$ восходит к Эрбрану и Сколему. Такие функции иногда называют «эрбрановскими» или «сколемовскими», а их добавление — «сколемизацией». Есть также термин «сколемовская нормальная форма», но здесь добавляются не функциональные символы, а предикатные, и получается формула не класса Σ_1, как в теореме 57, а класса Σ_2.

Теорема 58 (о сколемовской нормальной форме). Для всякой замкнутой формулы τ сигнатуры σ можно указать формулу τ' класса Σ_2 сигнатуры σ с добавленными предикатными символами, которая общезначима или необщезначима одновременно с формулой τ. При этом преобразование $\tau \mapsto \tau'$ эффективно (выполняется некоторым алгоритмом).

$\lhd$ Как и раньше, нам будет удобнее говорить о выполнимости и доказывать, что для всякой формулы τ найдётся одновременно с ней выполнимая формула τ' из класса Π_2. Построение такой формулы мы объясним на примере. Пусть исходная формула имеет вид

$$\forall x \forall y \exists z \forall u \exists v\, \varphi(x, y, z, u, v).$$

Мы теперь не можем ввести функции f и g, как это делалось выше, на с. 202. Поэтому мы введём предикаты F и G, заменяющие графики этих функций, и напишем формулу

$$\begin{gathered}
\forall x \forall y \exists z\ F(x, y, z) \wedge \\
\forall x \forall y \forall u \exists v\ G(x, y, u, v) \wedge \\
\forall x \forall y \forall z \forall u \forall v\, (F(x, y, z) \wedge G(x, y, u, v) \to \varphi(x, y, z, u, v))
\end{gathered}$$

Если исходная формула выполнима, то новая тоже выполнима: достаточно взять в качестве F и G графики сколемовских функций. Напротив, если новая формула выполнима, то выполнима и старая (более того, из новой формулы следует старая): надо взять z и v согласно первым двум строкам и заметить, что согласно третьей строке они подойдут.

Такая конструкция применима к любой предварённой форме и даёт конъюнкцию Π_2-формул (последняя из которых будет даже и Π_1-формулой). А мы знаем (с. 197), что такая конъюнкция эквивалентна Π_2-формуле. $\rhd$

110. Дайте синтаксическое доказательство теоремы о сколемовской нормальной форме (показав, что из выводимости формулы следует выводимость её сколемовской нормальной формы и наоборот). (Указание: это проще, чем для формул с функциональными символами, и не требуется использовать генценовское исчисление.)

Утверждения этого раздела сводят вопрос о выводимости произвольной формулы исчисления предикатов к выводимости Σ_1-формулы (с функциональными символами). Если мы запрещаем функциональные символы, то вопрос о выводимости произвольной формулы сводится к выводимости Σ_2-формулы.

Известно (теорема Чёрча, доказательство можно прочесть в [5]), что вопрос о выводимости произвольных формул языка первого порядка неразрешим: не существует алгоритма, который бы по произвольной замкнутой формуле определял бы, выводима она или нет. Результаты этого раздела показывают, что уже для формул класса Σ_1 (с функциональными символами) или Σ_2 (без них) такого алгоритма не существует, поскольку из него можно было бы получить и общий алгоритм. (В предыдущем разделе мы видели, что для формул класса Σ_1 без функциональных символов такой алгоритм существует.)

5. Теории и модели

5.1. Аксиомы равенства

Пусть сигнатура σ включает в себя двуместный предикат равенства (записываемый традиционно $x = y$). Интерпретация этой сигнатуры называется нормальной, если предикат равенства интерпретируется как тождественное совпадение элементов носителя.

Возникает естественный вопрос. Пусть имеется некоторая теория T (множество замкнутых формул) в языке, сигнатура которого включает равенство. Мы знаем что теория имеет модель (интерпретацию, в которой все формулы из T истинны) тогда и только тогда, когда она непротиворечива. В каком случае она имеет нормальную модель (нормальную интерпретацию, в которой все формулы из T истинны)?

Чтобы ответить на этот вопрос, введём аксиомы равенства. Пусть σ — произвольная сигнатура. *Аксиомами равенства* в сигнатуре σ будут формулы

$$\forall x\,(x = x),$$
$$\forall x \forall y\,((x = y) \to (y = x)),$$
$$\forall x \forall y \forall z\,(((x = y) \land (y = z)) \to (x = z))$$

(называемые аксиомами рефлексивности, симметричности и транзитивности). Это ещё не всё. Для каждого функционального символа мы формулируем аксиому равенства, которая говорит, что его значение не меняется, если аргументы заменить на равные. Например, для двуместного функционального символа f соответствующая аксиома выглядит так:

$$\forall x_1 \forall x_2 \forall y_1 \forall y_2\,(((x_1 = x_2) \land (y_1 = y_2)) \to \\ \to (f(x_1, y_1) = f(x_2, y_2))).$$

Для предикатных символов аксиомы равенства говорят, что истинный предикат остаётся истинным, если заменить аргументы на равные. Например, для двуместного предикатного символа A аксиома такова:

$$\forall x_1 \forall x_2 \forall y_1 \forall y_2\, (((x_1 = x_2) \wedge (y_1 = y_2) \wedge A(x_1, y_1) \to \\ \to A(x_2, y_2)).$$

(Нет необходимости специально говорить, что предикат остаётся ложным при замене аргументов на равные, так как равенство симметрично.)

Теорема 59 (полноты для нормальных моделей). Теория T сигнатуры σ с равенством имеет нормальную модель тогда и только тогда, когда она остаётся непротиворечивой при добавлении аксиом равенства.

$\triangleleft$ Прежде всего заметим, что теоремы о корректности и полноте (раздел 4.5) позволяют говорить о совместности вместо непротиворечивости.

В нормальной модели теории T аксиомы равенства истинны, так что в одну сторону утверждение теоремы очевидно. Нам осталось показать, что если теория T совместна с аксиомами равенства, то она имеет нормальную модель.

Возьмём произвольную интерпретацию, в которой истинны формулы из T и аксиомы равенства. Пусть M — её носитель. В этой интерпретации предикат $=$ не обязан быть настоящим равенством; он представляет собой некоторое бинарное отношение на M. Поскольку выполнены аксиомы равенства, это отношение рефлексивно, симметрично и транзитивно (является отношением эквивалентности). Следовательно, множество M разбивается на классы эквивалентности; множество этих классов обозначим M' (его можно назвать фактор-множеством M по данному отношению эквивалентности). Класс элемента x будем обозначать $[x]$.

Аксиомы равенства позволяют корректно определить интерпретацию с носителем M'. В самом деле, истинность аксиомы для функционального символа f (приведённой выше в качестве примера) гарантирует, что класс $[f(x,y)]$ зависит лишь от классов $[x]$ и $[y]$, но не от выбора x и y внутри класса. Аналогичным образом аксиомы для предикатных символов позволяют корректно определить предикаты на классах.

Полученная интерпретация с носителем M' по построению нормальна. Осталось убедиться, что в ней истинны те же самые формулы, что и в M (в том числе все формулы теории T). Это почти очевидно с интуитивной точки зрения: M отличается от M' лишь тем, что каждый элемент представлен несколькими равноправными копиями, которые со всех точек зрения ведут себя одинаково.

Формально говоря, мы доказываем, что формула φ истинна в интерпретации M на оценке π тогда и только тогда, когда φ истинна в M' на оценке π', при которой значение любой переменной ξ есть класс, содержащий значение переменной ξ при оценке π. Это легко сделать индукцией по построению формулы φ. $\triangleright$

111. Покажите, что из аксиом равенства для сигнатуры σ выводится формула

$$\varphi \wedge (x = y) \to \varphi(y/x),$$

если подстановка в правой части корректна. (Указание: это очевидно следует из теоремы о полноте, но можно провести и чисто синтаксическое рассуждение индукцией по построению формулы φ.)

112. Покажите, что если теория T (не обязательно с равенством) имеет модель мощности α, то она имеет и модель любой большей мощности. (Указание: элементы модели можно «клонировать» в произвольном количестве.)

Из теоремы о полноте для нормальных моделей легко следует аналог теоремы о компактности (теорема 50, с. 189) для нормальных моделей.

Теорема 60 (компактности для нормальных моделей). Если всякое конечное подмножество теории T в сигнатуре с равенством имеет нормальную модель, то и теория T имеет нормальную модель.

$\triangleleft$ Любое конечное подмножество теории T остаётся непротиворечивым при добавлении аксиом равенства (поскольку имеет нормальную модель). Значит, и вся теория T остаётся непротиворечивой при добавлении аксиом равенства (вывод противоречия использует конечное число формул) и потому имеет нормальную модель. $\triangleright$

113. Применив теорему о компактности, докажите, что всякий частичный порядок может быть продолжен до линейного. (Указание. Рассмотрим частично упорядоченное множество как модель теории, в сигнатуре которой есть равенство, порядок и константы для всех элементов множества, а формулами являются равенства и неравенства между константами. Добавим к ней утверждение о сравнимости любых двух элементов. Покажите, что любое конечное множество формул полученной теории непротиворечиво, используя тот факт, что частичный порядок на конечном множестве продолжается до линейного.)

114. Используя теорему о компактности, докажите, что для всякого поля k существует его расширение k', в котором всякий многочлен с коэффициентами из k имеет корень. (Указание. Утверждение о существовании корня у многочлена с данными коэффициентами можно записать в виде формулы. Любое конечное множество таких формул совместно с аксиомами поля, так как можно по очереди присоединить корни соответствующих многочленов.)

115. Пусть Γ — множество замкнутых формул в сигнатуре с равенством. Покажите, что замкнутая формула φ этой сигнатуры истинна во всех нормальных моделях Γ тогда и только тогда, когда она выводима из Γ и аксиом равенства.

Утверждение последней задачи является аналогом теоремы 51 (с. 190) для теорий с равенством. Иногда вообще рассматривают только такие теории. При этом равенство является обязательным элементом сигнатуры, аксиомы равенства (их число зависит от сигнатуры) считаются частью исчисления предикатов, а интерпретации рассматриваются только нормальные. При этом теория имеет [нормальную] модель тогда и только тогда, когда она непротиворечива [вместе с аксиомами равенства]; формула выводима из теории Γ [и аксиом равенства] тогда и только тогда, когда она верна во всех [нормальных] моделях теории Γ и т. п.. (в квадратных скобках указаны подразумеваемые слова).

5.2. Повышение мощности

Теорема Левенгейма – Сколема (раздел 3.11, теорема 42) позволяла уменьшать мощность интерпретации (она утверждала, что для любой бесконечной интерпретации конечной или счётной сигнатуры существует элементарно эквивалентная ей счётная подструктура). В этом разделе мы рассмотрим обратную задачу — расширение интерпретации до элементарно эквивалентной интерпретации большей мощности. Соответствующее утверждение также называют теоремой Левенгейма – Сколема.

Прежде всего отметим, что без требования нормальности это утверждение бессодержательно: как уже говорилось на с. 208, мы можем дублировать элементы сигнатуры в произвольном количестве. Поэтому мы предполагаем, что все рассматриваемые интерпретации нормальны (равенство интерпретируется как тождественное совпадение).

Теорема 61 (Левенгейма – Сколема о повышении мощности). Пусть A — бесконечная нормальная интерпретация некоторой сигнатуры σ с равенством. Тогда существует нормальная интерпретация $B \supset A$ сколь угодно большой мощности, являющаяся элементарным расширением A.

(Это означает, согласно определению на с. 142, напомним, что интерпретация предикатных и функциональных символов в B продолжает их интерпретацию в A и что формулы сигнатуры σ, параметрам которых приданы значения из A, одновременно истинны в A и в B.)

$\triangleleft$ Сформулируем утверждение теоремы в терминах теорий и моделей. Пусть A — произвольная нормальная интерпретация сигнатуры σ. Рассмотрим сигнатуру σ_A, которая получается из σ добавлением констант — по одной для каждого элемента множества A. Эта сигнатура имеет естественную нормальную интерпретацию с носителем A: значением каждой константы является соответствующий ей элемент. (Возможно, что в σ изначально было достаточно констант и всякий элемент A был значением некоторой константы. Тогда эта процедура лишняя, но и вреда от неё нет.)

Рассмотрим теорию $\mathrm{Th}_A(A)$, состоящую из формул сигнатуры σ_A, истинных в A при указанной интерпретации. Всякое элементарное расширение B интерпретации A будет моделью теории $\mathrm{Th}_A(A)$. В самом деле, замкнутая формула $\varphi(a_1, \ldots, a_n)$ сигнатуры σ_A получается подстановкой констант $a_1, \ldots, a_n$ вместо параметров из какой-то формулы $\varphi(x_1, \ldots, x_n)$ сигнатуры σ. (Мы используем не вполне корректные обозначения, в частности, отождествляем элементы $a_1, \ldots, a_n$ множества A с константами для них.) Её истинность в B (или в A) равносильна истинности формулы $\varphi(x_1, \ldots, x_n)$ при значениях параметров $x_1 \mapsto a_1, \ldots, x_n \mapsto a_n$ — формально говоря, следует воспользоваться леммой 2 на с. 169. Поэтому по определению элементарного расширения все формулы из $\mathrm{Th}_A(A)$ будут истинны и в B.

Верно и обратное: любая нормальная модель теории $\mathrm{Th}_A(A)$ естественно определяет элементарное расширение интерпретации A. В самом деле, пусть дана нормальная модель этой теории с носителем B. Тогда каждый элемент множества A (точнее, соответствующая этому элементу константа) интерпретируется некоторым элементом множества B. Разным элементам множества A соответствуют разные элементы в B, так как формула $a_1 \neq a_2$, истинная в A, должна быть истинной и в B. Таким образом, A вкладывается в B и можно отождествить его с некоторым подмножеством множества B. Это отождествление корректно в том смысле, что предикаты и функциональные символы интерпретируются согласованным образом. В самом деле, атомарные формулы вида $P(a_1, \ldots, a_n)$, а также формулы $\neg P(a_1, \ldots, a_n)$ и $f(a_1, \ldots, a_n) = a$, истинные в A, истинны и в B. Истинные в A формулы вида $\varphi(a_1, \ldots, a_n)$ принадлежат $\mathrm{Th}_A(A)$ и потому истинны и в B; ложные в A формулы имеют отрицания в $\mathrm{Th}_A(A)$ и потому ложны в B.

Таким образом, для доказательства теоремы Левенгейма – Сколема о повышении мощности осталось построить нормальную модель теории $\mathrm{Th}_A(A)$, имеющую сколь угодно большую мощность. Это можно сделать так: добавим множество новых констант c_i и формулы $c_i \ne c_j$ (для всех $i \ne j$) к теории $\mathrm{Th}_A(A)$. Полученная теория будет совместной по теореме компактности для нормальных моделей. (В самом деле, любая конечная часть её имеет нормальную модель, поскольку содержит конечное число новых констант, и им можно придать различные значения в A.) Поэтому и вся теория имеет нормальную модель. Всем константам c_i соответствуют в этой модели разные элементы (поскольку истинна формула $c_i \ne c_j$), поэтому мощность этой модели может быть сколь угодно большой, если использовать достаточно много констант.

Этот же приём будет использован нами при построении нестандартной модели арифметики (с. 236). $\triangleright$

Приведённое рассуждение даёт оценку мощности снизу. Можно получить и в точности нужную мощность:

Теорема 62. Пусть A — бесконечная нормальная интерпретация сигнатуры σ (с равенством) и пусть β — мощность, не меньшая мощностей сигнатуры σ и интерпретации A. Тогда существует нормальное элементарное расширение $B \supset A$ мощности β.

$\triangleleft$ Мощность сигнатуры σ_A есть максимум из мощностей σ и A; после добавления новых констант в количестве β штук получится сигнатура мощности β, и согласно теореме 48 (с. 188) найдётся модель множества $\mathrm{Th}_A(A)$ мощности β. Преобразование её в нормальную модель (факторизация) может лишь уменьшить мощность, но β различных элементов у нас заведомо есть. $\triangleright$

Аналогичный приём (добавление констант) позволяет легко доказать такое утверждение:

Теорема 63. Если теория (в произвольной сигнатуре с равенством) имеет сколь угодно большие конечные нормальные модели, то она имеет и бесконечную нормальную модель.

$\triangleleft$ Добавим к теории бесконечное число новых констант и аксиомы о том, что все они различны. Любой конечный фрагмент расширенной теории имеет нормальную модель (возьмём достаточно большую конечную модель и проинтерпретируем в ней константы). По теорме компактности и вся расширенная теория имеет нормальную модель, которая и будет бесконечной нормальной моделью исходной теории. $\triangleright$

Вообще можно задать себе такой естественный вопрос. Пусть есть некоторая теория (или даже просто одна формула). Каковы могут быть мощности её нормальных моделей? Как мы видели, для теорий с конечной сигнатурой верно одно из двух: либо бесконечных моделей вовсе нет, либо есть бесконечные модели всех мощностей. Это гарантируют теоремы Левенгейма – Сколема об элементарной подмодели (теорема 42) и о повышении мощности (теорема 61).

Что можно сказать про мощности конечных моделей? Для каждой формулы рассмотрим множество всех возможных мощностей её конечных моделей. Его иногда называют *спектром* формулы. Это множество может быть устроено довольно сложным образом: например, для формулы, выражающей аксиомы поля, спектр состоит из всех степеней простых чисел.

116. (**а**) Укажите формулу, спектр которой состоит из всех чётных положительных чисел. (**б**) Укажите формулу, спектр которой состоит из всех нечётных чисел. (**в**) Укажите формулу, спектр которой состоит из всех составных чисел.

Любопытно, что *проблема конечного спектра* (приведённая в книге Кейслера и Чэна под номером 1 среди «старых проблем теории моделей»), неожиданно оказалась связана с центральной проблемой теории сложности вычислений — так называемой «проблемой перебора». (Проблема конечного спектра состоит в следующем: верно ли, что дополнение (до $\mathbb{N}$) к спектру любой формулы является спектром некоторой другой формулы?)

В качестве примера использования теоремы о повышении мощности докажем теорему Гильберта о нулях (теорема 40), не проводя элиминацию кванторов. Пусть система уравнений имеет решение в поле k', являющемся расширением алгебраически замкнутого поля k. Покажем, что она имеет решение и в k. Построим элементарное расширение $k'' \supset k$ очень большой мощности. Теперь k' можно вложить в k'' (это вложение строится по трансфинитной рекурсии: добавляя алгебраический элемент, мы пользуемся алгебраической замкнутостью k'', добавляя трансцендентный элемент, мы пользуемся большой мощностью k''). Значит, система имеет решение в k''. Поскольку k'' было элементарным расширением, то система имеет решение в k.

Другое любопытное применение теоремы о повышении мощности таково. Назовём линейно упорядоченное множество M *однородным*, если для любых двух возрастающих последовательностей $x_1 < x_2 < \ldots < x_n$ и $y_1 < y_2 < \ldots < y_n$ найдётся автоморфизм множества M, переводящий x_i в y_i (при всех $i = 1, \ldots, n$).

Теорема 64. Для всякой бесконечной мощности найдётся однородное линейно упорядоченное множество такой мощности.

$\lhd$ Множество рациональных чисел (и вообще любое счётное плотное линейно упорядоченное множество) однородно. В самом деле, соответствие между двумя наборами его элементов постепенно продолжается до автоморфизма (добавляем элементы поочерёдно с той или другой стороны). Другой способ убедиться в этом — вспомнить о том, что это рациональные числа, и взять кусочно-линейный автоморфизм.

Для каждого n фиксируем способ продолжения автоморфизмов с n-элементных подмножеств в виде функции f_n с $2n+1$ аргументами: $f(z, x_1, \ldots, x_n, y_1, \ldots, y_n)$ означает элемент, в который переходит z при автоморфизме, переводящем x_i в y_i. Рассмотрим теперь $\mathbb{Q}$ как интерпретацию сигнатуры, включающей порядок и все f_i. По теореме о повышении мощности можно найти элементарно эквивалентную интерпретацию любой заданной мощности. Поскольку свойства функций f_n выражаются формулами, получится однородное линейно упорядоченное множество заданной мощности. ▷

5.3. Полные теории

В этом разделе мы попытаемся систематизировать уже известные нам понятия и факты.

- Начнём с напоминаний. *Сигнатурой* мы называли набор предикатных и функциональных символов. Среди формул данной сигнатуры выделяют *замкнутые* (формулы без параметров). Сигнатура имеет *интерпретации*, в которых замкнутые формулы этой сигнатуры бывают *истинными* и *ложными*. Произвольное множество замкнутых формул данной сигнатуры называется *теорией* в этой сигнатуре. *Моделью* теории называется интерпретация, в которой все формулы теории истинны. Теория называется *совместной*, если она имеет модель.

- Теория называется *теорией с равенством*, если она включает в себя аксиомы равенства (а её сигнатура содержит символ равенства). Интерпретация теории с равенством называется *нормальной*, если равенство интерпретируется как совпадение элементов носителя интерпретации. Совместная теория с равенством имеет нормальную модель (получаемую из произвольной модели факторизацией по отношению равенства).

- Говорят, что замкнутая формула φ *выводима в теории* T (является *теоремой теории* T), если формула φ получается из аксиом исчисления предикатов и формул теории T по правилам вывода. (Обозначение: $T \vdash \varphi$.)

  Формула φ выводима в теории T тогда и только тогда, когда в исчислении предикатов выводится некоторая формула вида $\tau \to \varphi$, где τ — конъюнкция конечного числа формул из T.

Формула φ *семантически следует* из T, если она истинна в любой модели теории T (обозначение: $T \vDash \varphi$). Семантическое следование равносильно выводимости (теорема 51, с. 190). Взяв в качестве φ тождественно ложную формулу $\perp$ (скажем, отрицание тавтологии), приходим к понятиям *противоречивости* ($T \vdash \perp$) и *несовместности* ($T \vDash \perp$, T не имеет моделей). В противоречивой теории выводима любая формула (соответствующей сигнатуры).

- Непротиворечивая теория T *полна* (в данной сигнатуре), если для любой замкнутой формулы φ этой сигнатуры либо формула φ, либо её отрицание $\neg\varphi$ выводится из T.

- Для произвольной интерпретации M произвольной сигнатуры σ можно рассмотреть *элементарную теорию интерпретации* M, обозначаемую $\mathrm{Th}(M)$ и состоящую из всех истинных в M замкнутых формул сигнатуры σ. Очевидно, эта теория полна (одна из формул φ и $\neg\varphi$ ей принадлежит). Две интерпретации M_1 и M_2 *элементарно эквивалентны*, если $\mathrm{Th}(M_1) = \mathrm{Th}(M_2)$.

- Теория T называется *конечно аксиоматизируемой*, если существует конечное множество T' теорем теории T, из которых выводятся все утверждения из T (другими словами, если существует конечная теория, имеющая то же самое множество теорем).

- Теория с равенством, имеющая конечную или счётную сигнатуру, называется *категоричной в счётной мощности*, если все её счётные нормальные модели изоморфны. Категоричность в данной несчётной мощности определяется аналогично.

- Теория с конечной сигнатурой называется *разрешимой*, если существует алгоритм, который по произвольной замкнутой формуле определяет, выводима ли она в этой теории или нет.

117. Покажите, что добавление к теории любой её теоремы не меняет множества теорем.

Прежде чем переходить к примерам, сделаем два простых наблюдения.

Теорема 65 (критерий Лося – Воота). Непротиворечивая теория T с равенством в конечной или счётной сигнатуре, не имеющая конечных моделей и категоричная в счётной мощности, полна.

$\triangleleft$ Предположим, что ни одна из формул φ и $\neg\varphi$ не выводима в теории T. Тогда обе теории $T \cup \{\neg\varphi\}$ и $T \cup \{\varphi\}$ непротиворечивы. По теореме 47 (с. 188) они имеют счётные модели, которые остаются счётными после факторизации (перехода к нормальным моделям), поскольку теория T не имеет конечных моделей. Эти счётные модели должны быть изоморфными (в силу категоричности). С другой стороны, в одной из них истинна формула $\neg\varphi$, а в другой — формула φ, так что они даже не элементарно эквивалентны (мы знаем из раздела 3.9, что такого быть не может). $\triangleright$

Аналогично доказывается и общая форма критерия Лося – Воота:

Теорема 66. Непротиворечивая теория с равенством в конечной или счётной сигнатуре, не имеющая конечных моделей и категоричная в данной несчётной мощности α, полна.

$\triangleleft$ Пусть теория T не полна и к ней можно присоединить без противоречия любую из формул φ и $\neg\varphi$. Рассмотрим счётные нормальные модели теорий $T \cup \{\varphi\}$ и $T \cup \{\neg\varphi\}$. По теореме 62 увеличим их мощности до α и получим противоречие. $\triangleright$

118. Условие конечности или счётности сигнатуры в этой теореме можно ослабить. Как это сделать?

Вот пример применения теоремы 66. Теория алгебраически замкнутых полей характеристики 0 категорична в любой несчётной мощности. (Это можно доказать с использованием понятия базиса трансцендентности: такое поле имеет базис трансцендентности над полем алгебраических чисел, мощность которого равна мощности всего поля, а два поля с равномощными базисами трансцендентности изоморфны). Следовательно, эта теория полна.

Заметим, что это наблюдение согласовано со знаменитой (и трудной!) теоремой Морли; эта теорема утверждает, что теория с равенством, категоричная в одной несчётной мощности, категорична и во всех несчётных мощностях. (Подробно о теореме Морли можно прочесть, например, в учебнике Кейслера и Чэна [13].)

Теорема 67. Конечно аксиоматизируемая полная теория в конечной сигнатуре разрешима.

$\triangleleft$ Пусть дана произвольная формула φ. Будем перебирать все выводы в исчислении предикатов и проверять, не обнаружилась ли выводимость одной из формул φ или $\neg\varphi$ из конъюнкции некоторых аксиом теории T. Рано или поздно одна из них окажется выводимой (поскольку теория полна), и тем самым мы узнаем, какая из формул выводима в теории. $\triangleright$

Это доказательство неконструктивно в том смысле, что не даёт никакой оценки на время работы алгоритма. Отметим также, что не обязательно требовать конечной аксиоматизируемости теории; достаточно, чтобы она имела разрешимое или перечислимое множество аксиом (см. [5]).

Проиллюстрируем все эти понятия на нескольких (в основном уже обсуждавшихся нами) примерах.

Плотные линейно упорядоченные множества

Рассмотрим сигнатуру, содержащую отношения порядка и равенства. Рассмотрим *теорию плотных линейно упорядоченных множеств без первого и последнего элемента*, которая включает в себя следующие аксиомы:

- аксиомы равенства (в том числе сохранение порядка при замене элементов на равные);
- $\forall x\,(x \leqslant x)$ (рефлексивность порядка);

- $\forall x \forall y \forall z\, ((x \leqslant y) \wedge (y \leqslant z) \to (x \leqslant z))$ (транзитивность порядка);
- $\forall x \forall y\, ((x \leqslant y) \wedge (y \leqslant x) \to (x = y))$ (антисимметричность порядка);
- $\forall x \forall y\, ((x \leqslant y) \vee (y \leqslant x))$ (линейность порядка);
- $\forall x \exists y\, (y > x)$ (нет максимального элемента; $(y > x)$ можно считать сокращением для $\neg(y \leqslant x)$ или для $(x \leqslant y) \wedge \neg(x = y)$ — при наличии остальных аксиом это одно и то же);
- аналогичная аксиома про отсутствие минимального элемента;
- $\forall x \forall y\, ((x < y) \to \exists z\, ((x < z) \wedge (z < y))$ (плотность).

Рациональные числа образуют счётную модель этой теории, а действительные — несчётную. Как мы уже упоминали, эта теория категорична в счётной мощности, все её счётные нормальные модели изоморфны. Отсюда по теореме 65 получаем, что она полна. Следовательно, в ней выводятся все истинные в $\mathbb{Q}$ (или в любой другой модели, в частности, в $\mathbb{R}$) формулы её сигнатуры (в самом деле, из формул φ и $\neg\varphi$ ровно одна истинна и ровно одна выводима, и выводимая формула должна быть истинной). Наконец, по теореме 67 эта теория разрешима.

Другое доказательство тех же фактов даёт элиминация кванторов (теорема 30, с. 115). Как мы отмечали в разделе 3.6, для каждой формулы φ нашей сигнатуры существует бескванторная формула φ', эквивалентная φ в любой нормальной интерпретации теории плотных линейно упорядоченных множеств без первого и последнего элементов. Поэтому эквивалентность $\varphi \leftrightarrow \varphi'$ (с кванторами всеобщности) является теоремой этой теории. Если формула φ была замкнутой, то формула φ' будет тождественно истинной или тождественно ложной. В первом случае в теории выводима формула φ, во втором случае — её отрицание. Следовательно, теория полна.

Сказанное можно интерпретировать и так: мы доказали конечную аксиоматизируемость теории $\mathrm{Th}(\mathbb{Q}, =, <)$, предъявив список аксиом.

119. Покажите, что эта теория не является категоричной в мощности континуум.

Отсюда следует (по теореме Морли), что теория плотных линейно упорядоченных множеств без первого и последнего элемента не будет категоричной ни в какой несчётной мощности.

120. Не используя теоремы Морли, укажите примеры неизоморфных плотных линейно упорядоченных множеств заданной несчётной мощности.

121. Покажите, что элементарные теории $\mathrm{Th}([0,1], =, <)$ и $\mathrm{Th}([0, +\infty), =, <)$ конечно аксиоматизируемы, полны и разрешимы. Будут ли они категоричными в мощности континуум?

122. Рассмотрим теорию плотных линейно упорядоченных множеств (не добавляя аксиом про наименьший и наибольший элемент). Будет ли она категорична в какой-либо мощности? полна? разрешима?

Теория $\mathrm{Th}(\mathbb{Z}, =, S, 0)$

В этом примере мы действуем в обратном порядке, начав с конкретной интерпретации (целые числа с равенством, функцией прибавления единицы и константой 0) и построив явную систему аксиом. Для этого вспомним процедуру элиминации кванторов из раздела 3.6 (теорема 28). Какими свойствами должна обладать нормальная интерпретация языка, чтобы преобразования, использованные при элиминации кванторов, были эквивалентными? Помимо аксиом равенства, нам нужно, чтобы функция S была биекцией и чтобы для любого x все элементы

$$\ldots, S^{-1}(S^{-1}(x)), S^{-1}(x), x, S(x), S(S(x)), \ldots$$

были различны. Другими словами, элиминация кванторов даёт формулу, эквивалентную исходной во всех моделях такой теории:

- аксиомы равенства;
- $\forall x \forall y\, ((S(x) = S(y)) \to (x = y))$;

- $\forall x \exists y\,(S(y) = x)$;
- $\forall x\,\neg(x = S(x))$;
- $\forall x\,\neg(x = S(S(x)))$;
- $\forall x\,\neg(x = S(S(S(x))))$ и т. д.

Ограничиваясь замкнутыми формулами, мы (как и в предыдущем примере) видим, что $\mathrm{Th}(\mathbb{Z}, =, S, 0)$ совпадает с множеством всех формул, выводимых из перечисленных аксиом, так что теория с этими аксиомами полна. Она разрешима (как любая полная теория с разрешимым множеством аксиом; кроме того, явный алгоритм даётся элиминацией кванторов).

В отличие от предыдущего примера, эта теория не является категоричной в счётной мощности — например, $\mathbb{Z}+\mathbb{Z}$ является её моделью, не изоморфной исходной.

123. Опишите все модели этой теории.

124. Покажите, что эта теория категорична в любой несчётной мощности.

Покажем в заключение, что эта теория не является конечно аксиоматизируемой. В самом деле, пусть имеется конечное множество F теорем этой теории, из которой следуют все остальные теоремы. Каждая из теорем множества F выводима из аксиом, и этот вывод использует конечное число аксиом. Это означает, что все остальные аксиомы (не используемые в выводе формул из F) вообще лишние. А это не так: в конечной модели, составленной из остатков по модулю N, верны все аксиомы, кроме $S^N(x) \ne x$, $S^{2N}(x) \ne x, \ldots$, поэтому эти аксиомы не следуют из остальных.

125. Докажите, что использованное нами рассуждение носит общий характер: если теория бесконечна, но конечно аксиоматизируема, то некоторая её конечная часть равносильна всей теории (имеет те же теоремы).

Теория $\mathrm{Th}(\mathbb{Z}, =, <, S, 0)$

Что изменится, если мы добавим к сигнатуре, помимо прибавления единицы, ещё и отношение порядка? Как мы видели (см. доказательство теоремы 29 и задачу после него, с. 113), элиминация кванторов по-прежнему возможна. Для придания законности нам нужны такие свойства интерпретации (которую мы предполагаем нормальной): она представляет собой линейно упорядоченное множество, в котором каждый элемент имеет непосредственно следующий (совпадающий с значением функции S) и непосредственно предшествующий. В отличие от предыдущего примера, нам достаточно конечного набора аксиом. Таким образом, теория $\mathrm{Th}(\mathbb{Z}, =, <, S, 0)$ конечно аксиоматизируема, а также (как и в предыдущем примере) полна, разрешима, но не категорична в счётной мощности.

Можно обойтись и без элиминации кванторов, рассуждая иначе. Рассмотрим теорию линейно упорядоченных множеств со следующим и предыдущим элементом и опишем все её модели. Именно, мы покажем, что любая нормальная модель M этой теории имеет вид $\mathbb{Z} \times A$, где A — произвольное линейно упорядоченное множество (порядок на парах таков: сначала сравниваются A-компоненты, а в случае равенства — $\mathbb{Z}$-компоненты.) В самом деле, будем говорить, что элементы x и y лежат «в одной галактике», если между ними конечное число элементов. (Легко проверить, что это действительно отношение эквивалентности, и наше множество разбивается на галактики.) Далее проверяем, что каждая галактика изоморфна $\mathbb{Z}$ (как упорядоченное множество) и что на галактиках естественно определяется порядок.

Теперь с помощью игры Эренфойхта (см. раздел 3.9, теорема 37) мы показываем, что все нормальные модели этой теории элементарно эквивалентны. Отсюда заключаем, что теория полна (как в доказательстве теоремы 65, где мы по существу использовали элементарную эквивалентность моделей, а не их изоморфизм).

126. Покажите, что теория $\mathrm{Th}(\mathbb{Z}, =, <, S, 0)$ не категорична ни в какой несчётной мощности.

127. Будет ли теория $\mathrm{Th}(\mathbb{Z}, =, <)$ конечно аксиоматизируемой? разрешимой? категоричной?

128. Будет ли теория $\mathrm{Th}(\mathbb{N}, =, <)$ конечно аксиоматизируемой? разрешимой? категоричной?

Теория $\mathrm{Th}(\mathbb{Q}, =, <, +, 0, 1)$

Эту теорию мы рассматривали в разделе 3.6, с. 118. Мы ограничимся двумя константами 0 и 1, поскольку любую атомарную формулу можно привести к общему знаменателю и получить целые константы, которые можно выразить через 0 и 1.

Мы хотим указать набор явный набор аксиом этой теории, то есть множество формул, из которых выводятся все теоремы этой теории и только они. Как и в предыдущих примерах, это можно сделать, проанализировав процесс элиминации кванторов и выявив все использованные при этом свойства интерпретации. (Все рассматриваемые нами интерпретации предполагаются нормальными, а аксиомы равенства изначально включаются в строимую нами теорию.)

Прежде всего, нам важно, что по сложению мы имеем абелеву группу (и 0 является её нулём). Это позволяет в равенствах переносить члены с одной стороны в другую. Для операций с неравенствами нам надо знать, что порядок является линейным и что он согласован со сложением (то есть что из $x < y$ следует $x + z < y + z$). Кроме того, мы умножали равенства и неравенства на рациональные числа. Чтобы это было законно, мы должны знать, что группа является делимой: для всякого a уравнения $x + x = a$, $x + x + x = a$, $x + x + x + x = a$, $\ldots$ имеют решения. (В упорядоченной группе такое решение, как легко показать, единственно.) Наконец, нам надо знать, что $1 > 0$.

Кроме этих аксиом (которых счётное число) мы при элиминации ничего не использовали, так что для любой формулы φ есть бескванторная формула φ', которая эквивалентна φ в любой делимой упорядоченной группе. Поэтому любая замкнутая формула, истинная в стандартной интерпретации (в $\mathbb{Q}$), истинна в любой делимой упорядоченной группе, и мы получили счётную систему аксиом для теории $\mathrm{Th}(\mathbb{Q}, =, <, +, 0, 1)$.

129. Покажите, что эта теория не является конечно аксиоматизируемой. (Указание: делимость любого элемента группы на простое число p не вытекает из делимости на все меньшие простые числа — рассмотрим рациональные числа, знаменатель которых взаимно прост с p.)

130. Покажите, что эта теория разрешима.

131. Покажите, что эта теория не является категоричной.

132. Покажите, что теория $\mathrm{Th}(\mathbb{Q}, =, +, 0)$ не является категоричной в счётной мощности, но категорична в любой несчётной мощности. (Указание: её модели — векторные пространства над полем рациональных чисел.)

Арифметика Пресбургера

В разделе 3.7 мы занимались элиминацией кванторов в теории $(\mathbb{Z}, =, <, +, 0, 1)$, которая потребовала добавления бесконечного числа дополнительных предикатов (сравнимость по модулю N для всех целых $N > 1$).

Проанализировав это рассуждение, можно извлечь из него явную аксиоматизацию для теории $(\mathbb{Z}, =, <, +, 0, 1)$ (без дополнительных предикатов). Какие свойства порядка и сложения на целых числах мы используем? Нам важно, что целые числа образуют абелеву группу, что порядок согласован со сложением и что $x + 1$ есть непосредственно следующий за x элемент. В любой группе можно рассмотреть подгруппу делящихся на N элементов (для любой целой константы $N > 1$) и сравнивать элементы по модулю этой подгруппы. Но этого мало: нам нужно ещё иметь возможность делить на N с остатком. Это гарантируется такой аксиомой (при каждом N — своя аксиома): для любого элемента x ровно один из N элементов $x, x-1, x-2, \ldots, x-N+1$ делится на N.

Можно проверить, что все шаги элиминации кванторов сохраняют равносильность в такой ситуации. Проверим, например, что сравнения можно умножать на целое положительное число. Почему, скажем, $a \equiv b \pmod 3$ равносильно $a + a \equiv b + b \pmod 6$? По определению первое означает, что $a - b = u + u + u$ для некоторого u, а второе — что $(a - b) + (a - b) = v + v + v + v + v + v$ для некоторого v, и достаточно сослаться на то, что в упорядоченной группе из $x + x = 0$ следует $x = 0$ (поскольку из $x > 0$ следует $x + x > x > 0$). Наиболее сложный шаг — доказательство представительности набора. Здесь надо рассмотреть все случаи расположения произвольного y относительно правых частей. В каждом из случаев мы заменяли y на первый элемент из окрестности правых частей, встречающийся при движении шагами D (как описано на с. 123). Эту процедуру можно понимать как деление расстояния (до ближайшей правой части) на D с остатком; возможность этого гарантируется нашими аксиомами.

133. Покажите, что теория $(\mathbb{Z}, =, <, +, 0, 1)$ разрешима.

134. Покажите, что эта теория не категорична в счётной мощности и опишите все её счётные модели. (Указание: они имеют вид $\mathbb{Z} \times A$, где A — делимая упорядоченная группа.)

135. Покажите, что эта теория не конечно аксиоматизируема. (Указание: рассмотрите интерпретацию $\mathbb{Z} \times A$, когда в A возможно деление на простые числа, меньшие некоторого p, но не на p.)

Алгебраически замкнутые поля характеристики 0

Теорема 34 устанавливает возможность элиминации кванторов в поле комплексных чисел. Как мы уже отмечали (теорема 38 на с. 142), это преобразование даёт формулу, равносильную во всех алгебраически замкнутых полях характеристики 0. Отсюда следует, как обычно, теория алгебраически замкнутых полей характеристики 0 полна. (Её аксиомы таковы: аксиомы равенства, аксиомы поля, счётный набор утверждений о том, что любой многочлен степени $n > 0$ с ненулевым старшим коэффициентом имеет корень, а также счётный набор утверждений вида $1 + 1 + 1 + \ldots + 1 \neq 0$.) Эта теория совпадает с элементарной теорией поля комплексных чисел.

Другое доказательство полноты этой теории можно получить с помощью критерия Лося – Воота (теорема 66, с. 217) и утверждения следующей задачи.

136. Покажите, что теория алгебраически замкнутых полей характеристики 0 не категорична в счётной мощности, но категорична в любой несчётной мощности. (Указание: алгебраически замкнутое поле имеет базис трансцендентности над $\mathbb{Q}$; если поле несчётно, то базис равномощен полю.)

137. Покажите, что теория алгебраически замкнутых полей данной характеристики p полна.

138. Покажите, что если некоторая формула в сигнатуре $(=, +, \times)$ истинна в алгебраически замкнутых полях характеристики 0, то она истинна и во всех алгебраически замкнутых полях достаточно большой конечной характеристики.

Вещественно замкнутые поля

Более сложно сформулировать, какие свойства вещественных чисел реально используются при доказательстве теоремы Тарского–Зайденберга (раздел 3.8). Дело в том, что мы ссылались на разные факты из анализа (понятие производной, теорема Ролля, асимптотика многочленов). Однако на самом деле достаточно некоторых алгебраических свойств поля — как говорят, поле должно быть «вещественно замкнутым».

Поле называется *упорядоченным*, если на нём задан линейный порядок, причём он согласован со сложением ($x < y$ влечёт $x + z < y + z$) и умножением ($x, y > 0$ влечёт $xy > 0$).

139. Покажите, что любое упорядоченное поле имеет характеристику 0 и что в любом упорядоченном поле сумма квадратов не может равняться -1.

Упорядоченное поле называется *вещественно замкнутым*, если любой многочлен, имеющий на концах отрезка разные знаки, имеет корень на этом отрезке. (Отметим в скобках, что существует несколько эквивалентных определений вещественно замкнутого поля, см. учебник ван дер Вардена [4]; мы выбрали наиболее удобное для наших целей.)

Мы не можем записать определение вещественной замкнутости в виде формулы, поскольку степень многочлена может быть любой. Но можно написать много формул — по одной для каждой степени многочлена. Например, для многочленов степени 2 получится формула

$$(u < v) \ \wedge \ (a \neq 0) \ \wedge \ ((au^2 + bu + c)(av^2 + bc + c) < 0) \rightarrow \\ \rightarrow \exists x \, ((u < x) \wedge (x < v) \wedge \ (ax^2 + bx + c = 0)).$$

Теория, состоящая из аксиом упорядоченного поля (в том числе аксиом равенства) и этих дополнительных аксиом, называется *теорией вещественно замкнутых полей*. Покажем, что в любом вещественно замкнутом поле выполнены основные факты о многочленах и их производных. Прежде всего заметим, что в алгебре естественно определять производную многочлена не как предел, а чисто формально: $(x^n)' = nx^{n-1}$ (для любого положительного целого n), далее по линейности. Степень производной многочлена на единицу меньше степени самого многочлена. Выполнены основные правила дифференцирования (линейность, правило дифференцирования произведения, формула Тейлора).

Теперь отметим некоторые свойства многочленов, связанные с порядком. Пусть многочлен в какой-то точке равен нулю, а производная его в этой точке больше нуля. Тогда в некоторой окрестности этой точки он положителен справа и отрицателен слева. (В самом деле, можно применить формулу Тейлора и оценки, показывающие, что вблизи нуля знак определяется линейной частью.)

Справедливо и свойство сохранения знака: если в какой-то точке многочлен положителен, то и в достаточно близких точках он положителен. Слова «достаточно близких» понимаются в обычном смысле ($\exists \varepsilon > 0$), только теперь ε — не действительное число, а элемент поля.

Аналогичным образом можно сформулировать и доказать такое утверждение: при всех достаточно больших значениях аргумента знак многочлена определяется его старшим коэффициентом (обычные оценки вполне годятся).

Более сложно доказывается, что что если производная многочлена $P(x)$ положительна на интервале (a, b), то он неубывает на отрезке $[a, b]$. Пусть это не так. Добавив к многочлену константу, можно считать, что для каких-то точек c, d этого отрезка имеют место неравенства $c < d$, $P(c) > 0$, $P(d) < 0$ и потому P имеет корень на интервале (c, d) (вещественная замкнутость).

Число корней многочлена (в любом поле) конечно, поэтому среди корней многочлена $P(x)$ на интервале (c, d) есть наименьший корень α. Слева от α многочлен P должен быть положительным (поскольку корень первый), но одновременно вблизи α и отрицательным (так как $P'(\alpha) > 0$ по предположению).

Теперь легко понять, что многочлен с положительной производной на (a, b) строго возрастает на $[a, b]$: если бы в двух точках он принимал одинаковые значения, то между ними он был бы константой (чего не может быть для непостоянного многочлена).

Следствие: многочлен, производная которого не имеет корней на (a, b), либо строго возрастает, либо строго убывает на $[a, b]$. В самом деле, свойство вещественной замкнутости можно применить и к производной, следовательно она либо всюду положительна, либо всюду отрицательна. В частности, справедлива теорема Ролля (многочлен с равными значениями на концах отрезка имеет нуль производной).

После такой тренировки наши рассуждения про знаки многочленов диаграммы легко провести для произвольного поля. Легко понять также, что деление с остатком (точнее, операция модифицированного остатка) имеет смысл для любого поля, и что целые числа (которые были коэффициентами многочленов) содержатся в любом поле.

Итак, элиминация кванторов даёт формулу, равносильную исходной в любом вещественно замкнутом поле. Отсюда, как обычно, следует, что теория вещественно замкнутых полей совпадает с элементарной теорией упорядоченного поля вещественных чисел и потому полна, а также разрешима, и что все вещественно замкнутые упорядоченные поля элементарно эквивалентны.

5.4. Неполные и неразрешимые теории

Предыдущий раздел мог создать впечатление, что наугад взятая теория скорее всего окажется полной, разрешимой, а возможно, и конечно аксиоматизируемой. Это совсем не так.

Откуда вообще берутся в математике аксиоматические теории? Иногда мы пытаемся построить аксиоматически теорию какой-то конкретной структуры (скажем, теорию действительных чисел со сложением и умножением). В других случаях мы стараемся выделить общие свойства различных структур. Например, аксиомы группы фиксируют общие свойства различных групп, и с самого начала ясно, что такая теория не должна и не может быть полной. То же самое можно сказать и про теорию линейно упорядоченных множеств — полнота такой теории означала бы, что все линейно упорядоченные множества (или группы) элементарно эквивалентны, то есть обладают одними и теми же свойствами, выражаемыми формулами. Это, конечно, не так.

Что касается конкретных структур, то и для них естественные теории не всегда оказываются полными. Классический пример — натуральные числа со сложением и умножением. Для них имеется естественная формальная теория (называемая формальной арифметикой). Её аксиомы включают в себя обычные свойства сложения и умножения, а также аксиомы индукции. Опыт показывает, что любое рассуждение теории чисел, в котором речь идёт только о конечных объектах, может быть формально записано в виде вывода из аксиом этой теории. Более того, многие доказательства, использующие бесконечные объекты (скажем, важнейшую в теории чисел ζ-функцию Римана), могут быть модифицированы и погружены в эту формальную теорию. Тем не менее эта теория неполна (и не может быть полна, как мы увидим в этом разделе).

Среди естественных неполных теорий бывают разрешимые и неразрешимые. Например, теория линейно упорядоченных множеств разрешима, теория абелевых групп разрешима, а теория групп неразрешима. Подробный рассказ об этом далеко выходит за рамки нашей книжки; написанный М. О. Рабином обзор соответствующих результатов можно найти в справочнике по математической логике (часть III, *Теория рекурсии* [26], глава 4).

Мы же ограничимся тремя примерами (теория равенства, теория полугрупп, формальная арифметика).

Теория равенства

Рассмотрим сигнатуру, содержащую единственный двуместный предикат равенства, и теорию, состоящую из трёх аксиом равенства (рефлексивность, симметричность и транзитивность). Эти аксиомы рассматривались в разделе 5.1; заметим, что у нас нет других предикатных и функциональных символов (и связанных с ними аксиом равенства).

Моделями этой теории являются всевозможные множества с отношениями эквивалентности. Нормальными моделями этой теории являются множества различной мощности; поскольку никакой дополнительной структуры нет, такая модель определяется мощностью (с точностью до изоморфизма). Теоремами этой теории будут формулы с равенством, истинные в множествах любой мощности.

Теорема 68. Множество теорем теории равенства является разрешимым.

$\triangleleft$ Заметим, что истинность формулы в нормальной модели может зависеть от её мощности. Например, формула $\exists x \exists y \neg(x = y)$ ложна в одноэлементной модели и истинна во всех остальных. Поэтому процедура элиминации кванторов в чистом виде здесь неприменима.

Но идея остаётся той же. От чего зависит истинность формулы этой сигнатуры (с параметрами)? Во-первых, от значений параметров (важно, какие параметры равны друг другу, а какие нет). Во-вторых, от числа элементов модели. (Если бы этой зависимости не было, то можно было бы написать бескванторную формулу, эквивалентную данной во всех моделях теории.)

Например, формула $\exists z\,(\neg(z = x) \wedge \neg(z = y))$ при $x = y$ истинна во всех моделях, начиная с двухэлементной, а при $x \neq y$ истинна во всех моделях, начиная с трёхэлементной. Можно ожидать, что модели с большим числом элементов неотличимы друг от друга и от бесконечных моделей.

Лемма. Истинность формулы языка с равенством, содержащей k параметров и имеющей кванторную глубину l, определяется тем, какие из параметров равны друг другу, а также мощностью носителя, при этом все мощности, большие $k + l$, одинаковы.

Доказательство леммы проводится индукцией по построению формулы. Для атомарной (и вообще для любой бескванторной) формулы мощность вообще не играет роли. Если утверждение леммы верно для формул φ и ψ, то оно очевидным образом верно и для $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \to \psi$ и $\neg\varphi$. При этом используется такой факт: кванторная глубина (число вложенных кванторов) и число параметров у части формулы не больше, чем у всей формулы.

Содержательный случай — когда формула начинается с квантора. Когда, скажем, формула

$$\exists x \varphi(x, x_1, \ldots, x_k)$$

с параметрами $x_1, \ldots, x_k$ будет истинной (в данной интерпретации при данных значениях параметров)? Достаточно попробовать в качестве x значения $x_1, \ldots, x_k$ а также какой-нибудь элемент, отличный от всех этих значений. (Все такие элементы ничем не отличаются.) Истинность формулы $\varphi(x, x_1, \ldots, x_k)$ при $x = x_i$ определяется соотношениями между параметрами и мощностью модели (по предположению индукции; заметим, что число параметров увеличилось на 1, а кванторная глубина уменьшилась на 1, так что сумма осталась прежней). Существование элемента, отличного от всех x_i, определяется мощностью модели и числом различных элементов среди $x_1, \ldots, x_k$ (то есть в конечном счёте равенствами вида $x_i = x_j$). При этом модели всех мощностей, начиная с $k+1$, ведут себя одинаково. Кроме того, истинность формулы $\varphi(x, x_1, \ldots, x_k)$ при $x \notin \{x_1, \ldots, x_k\}$ по предположению индукции также определяется равенствами вида $x_i = x_j$ и мощностью модели.

Квантор всеобщности рассматривается точно так же (а можно его выразить через квантор существования и вообще не рассматривать). Лемма доказана.

Доказательство леммы конструктивно, то есть указывает способ узнать, будет ли формула истинной, если известно, какие её параметры равны и какова мощность носителя. В частности, для замкнутых формул получаем способ проверять их истинность для всех значений мощности, то есть выводимость в теории равенства. $\triangleright$

140. Рассмотрим теорию, в сигнатуре которой есть равенство и конечное число одноместных предикатных символов, а аксиомами являются аксиомы равенства (включая устойчивость предикатов относительно равенства, как в разделе 5.1). Покажите, что эта теория разрешима.

Эта задача показывает, что добавление одноместных предикатов в сигнатуру не делает теорию равенства неразрешимой. Отметим, что расширение сигнатуры (без изменения множества аксиом) может превратить разрешимую теорию в неразрешимую: например, добавив конечное число одноместных функциональных символов к теории равенства, получим неразрешимую теорию (как видно из доказательства теоремы Чёрча с помощью проблемы тождества для полугрупп, см. [5]). Добавление одного двуместного предикатного символа также даёт неразрешимую теорию.

Теория полугрупп

Наш второй пример — теория полугрупп. Её сигнатура состоит из равенства и единственного двуместного функционального символа, называемого умножением; результат умножения x и y мы будем обозначать (xy).

Теория состоит из аксиом равенства (включая корректность умножения: $(x_1 = x_2) \wedge (y_1 = y_2) \to (x_1y_1 =$

$= x_2y_2)$; мы опускаем внешние кванторы всеобщности) и аксиомы ассоциативности

$$\forall x \forall y \forall z\, ((xy)z = x(yz)).$$

Нормальные модели этой теории называются *полугруппами*.

Теорема 69. Множество теорем теории полугрупп (множество замкнутых формул указанной сигнатуры, истинных во всех полугруппах) неразрешимо.

$\lhd$ Нам понадобится конкретный способ задания полугрупп с помощью образующих и соотношений. Пусть фиксирован некоторое конечное множество, называемое *алфавитом*. Элементы его называют *буквами*, а конечные последовательности букв — *словами* (данного алфавита). На словах определена операция соединения (приписывания), относительно которой они образуют полугруппу, которая называется *свободной полугруппой*. Эта полугруппа имеет нейтральный элемент — пустое слово, приписывание которого к любому слову не меняет последнего.

Пусть фиксирован алфавит A, а также конечное число пар слов $(X_1, Y_1), \ldots, (X_n, Y_n)$ этого алфавита. Два слова алфавита A назовём эквивалентными, если одно можно превратить в другое, многократно делая замены подслов вида $X_i \leftrightarrow Y_i$. Легко проверить, что получается отношение эквивалентности и что операция приписывания корректно определена на классах эквивалентности и ассоциативна. Получается полугруппа. Её называют полугруппой с *образующими* из A и *соотношениями* $X_i = Y_i$.

141. Сколько элементов в полугруппе образующими a и b и соотношениями $a^2 = \Lambda$, $b^2 = \Lambda$, $ab = ba$ (через Λ мы обозначаем пустое слово)? (Ответ: 4; это группа $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.)

Известно, что существуют такие образующие и соотношения, при которых проблема равенства слов (выяснить, принадлежат ли два данных слова одному классу эквивалентности) является алгоритмически неразрешимой (подробнее см. в [5]). Мы сейчас покажем, что этот вопрос можно свести к вопросу о выводимости некоторой формулы в теории полугрупп, так что если бы она была разрешимой, то получилось бы противоречие.

Построение такой формулы происходит весьма естественным образом; мы поясним его на примере. Пусть мы хотим узнать, будут ли слова bb и a равны в полугруппе с образующими a и b и соотношениями $ab = aa$ и $bab = b$. (Другими словами, мы хотим узнать, можно ли из слова bb получить слово a с помощью замен подслов $ab \leftrightarrow aa$ и $bab \leftrightarrow b$.) Как сформулировать этот вопрос в терминах формул? Напишем такую формулу:

$$\forall a \forall b\, ((ab = aa) \wedge (bab = b) \to (bb = a)).$$

Она является теоремой теории полугрупп (истинна во всех полугруппах, выводима из аксиом полугрупп) тогда и только тогда, когда слова bb и a эквивалентны в указанной полугруппе, заданной образующими и соотношениями. В самом деле, если одно слово можно получить из другого заменами, то эти замены (в предположении $ab = aa$ и $bab = a$) ничего не меняют и $bb = a$, так что написанная формула истинна во всех полугруппах.

Напротив, если слово a не получается из bb заменой, то есть полугруппа, в которой эта формула не истинна: надо взять как раз полугруппу с образующими a и b и соотношениями $ab = aa$ и $bab = b$, значением переменной a считать класс слова a, а значением переменной b считать класс слова b. Тогда значением терма ab будет класс слова ab, равный классу слова aa по построению полугруппы. Аналогичным образом при такой оценке будет истинно и равенство $bab = b$. А равенство $bb = a$ не будет истинно, так как значение терма bb есть класс слова bb, значение терма a есть класс слова a, а эти классы различны по предположению.

Таким образом, любой алгоритм, проверяющий истинность формул в классе всех полугрупп, можно было бы использовать для проверки равенства двух слов в полугруппе, заданной образующими и соотношениями.

А среди таких полугрупп есть неразрешимые. ▷

Теория групп (в которой, помимо ассоциативности, есть ещё аксиомы существования единицы и обратного), также неразрешима, но доказательство этого сложнее, чем для полугрупп. Это и не удивительно, поскольку из неразрешимости теории групп формально выводится неразрешимость теории полугрупп, как показывает следующая задача.

142. Пусть теория T разрешима, а теория T' той же сигнатуры получается из T добавлением конечного числа аксиом. Тогда теория T' разрешима. (Указание: дополнительные аксиомы соединяем конъюнкциями и помещаем в посылку импликации.)

Добавление аксиом может сделать неразрешимую теорию разрешимой. Например, как мы уже упоминали, это происходит с теорией групп при добавлении аксиомы коммутативности.

Формальная арифметика

Рассмотрим множество натуральных чисел с операциями сложения и умножения и его элементарную теорию $\mathrm{Th}(\mathbb{N}, =, +, \times)$, то есть множество всех истинных (в натуральном ряду) формул со сложением и умножением. Это множество, очевидно, полно. Можно доказать (см. [5]), что оно неразрешимо (и, более того, неарифметично, как говорит теорема Тарского).

Отсюда следует, что теория $\mathrm{Th}(\mathbb{N}, =, +, \times)$ не является конечно аксиоматизируемой. (В самом деле, эта теория полна и неразрешима, и можно сослаться на теорему 67.) Более того, это же рассуждение показывает, что не существует разрешимого множества теорем этой теории, из которых бы выводились все другие теоремы. Отсюда следует, что классическая система аксиом формальной арифметики, называемая также *арифметикой Пеано* (свойства арифметических операций плюс аксиомы индукции), не может быть полной: существуют истинные формулы, невыводимые в формальной арифметике. Это утверждение составляет содержание знаменитой *теоре-*

мы Гёделя о неполноте.

143. Покажите, что нельзя добавить к языку теории $\mathrm{Th}(\mathbb{N},=,+,\times)$ конечное число выразимых предикатов так, чтобы после этого проходила элиминация кванторов. (Указание: арифметическая иерархия не ограничивается никаким конечным числом уровней.)

144. Покажите, что элементарная теория целых чисел со сложением и умножением сводится к элементарной теории натуральных чисел со сложением и умножением: по замкнутой формуле φ со сложением и умножением можно алгоритмически построить формулу φ' с таким свойством: φ истинна в $\mathbb{Z}$ тогда и только тогда, когда φ' истинна в $\mathbb{N}$. (Указание: целые числа можно кодировать парами натуральных.)

145. (Продолжение) Покажите, что верно и обратное: элементарная теория натуральных чисел сводится к элементарной теории целых чисел. (Указание. Если бы в целых числах был порядок, это было бы совсем просто. Чтобы его ввести, можно использовать теорему Лагранжа о том, что всякое натуральное число представимо в виде суммы четырёх квадратов.)

Будет ли теория $\mathrm{Th}(\mathbb{N},=,+,\times)$ категоричной в счётной мощности? Другими словами, имеет ли она счётную модель, не изоморфную стандартной? Раньше, для более простых ситуаций, нам удавалось указать такие модели явно. Теперь это не удастся, но есть простое общее рассуждение, устанавливающее существование нестандартной модели. (Оно аналогично рассуждению, использованному при доказательстве теоремы 5.2.)

Рассмотрим последовательность формул $E_0(x)$, $E_1(x)$, $E_2(x), \ldots$ с единственным параметром x, где $E_i(x)$ — любая формула, выражающая в стандартной модели свойство $x = i$. (Если бы у нас в языке была константа 1, можно было бы считать $E_i(x)$ бескванторной формулой $x = 1 + 1 + \ldots + 1$, в правой части которой стоит терм с i единицами.)

Добавим к сигнатуре новую константу c и рассмотрим теорию, получаемую из $\mathrm{Th}(\mathbb{N},=,+,\times)$ добавлением счётного семейства формул $\neg E_i(c)$ (по существу мы добавляем формулы $c \neq 0$, $c \neq 1, \ldots$, записанные подходящим образом). Любое конечное подмножество полученной теории имеет модель (возьмём стандартный натуральный ряд и в качестве c выберем достаточно большое число). Следовательно (теорема 50 о компактности), и вся эта теория совместна. Рассмотрим её счётную нормальную модель и забудем о символе c; получится некоторая интерпретация сигнатуры $(=, +, \times)$. Она будет элементарно эквивалентна стандартному натуральному ряду (все истинные в $\mathbb{N}$ формулы будут истинны по построению, а все ложные будут ложны, так как их отрицания истинны).

Осталось показать, что она не будет изоморфной натуральному ряду. В самом деле, рассмотрим элемент, который является значением константы c в нестандартной модели. Он не может переходить ни в какое натуральное число i, поскольку для соответствующих (друг другу при изоморфизме) элементов выполнены одни и те же формулы, $E_i(i)$ истинно в натуральном ряду и $E_i(c)$ ложно в новой интерпретации.

146. Покажите, что найдётся нормальная интерпретация сколь угодно большой мощности, элементарно эквивалентная натуральным числам со сложением и умножением.

5.5. Диаграммы и расширения

В разделе 5.2 мы видели, что элементарные расширения интерпретации A суть модели теории $\mathrm{Th}_A(A)$. А что можно сказать о расширениях (без требования элементарности)? Оказывается, что ситуация тут аналогична, только теория будет бескванторной.

Пусть дана нормальная интерпретация A сигнатуры σ (включающей равенство). Как и в прошлом разделе, рассмотрим сигнатуру σ_A, которая получается добавлением к σ констант для всех элементов интерпретации A. Рассмотрим теперь все бескванторные формулы сигнатуры σ_A, истинные в A. Это множество называется *диаграммой* интерпретации A и обозначается $D(A)$.

Всякое расширение $B \supset A$ (в котором A является подструктурой) является моделью теории $D(A)$. В самом деле, истинность бескванторных формул из $D(A)$ никак не зависит от присутствия или отсутствия дополнительных элементов, раз операции на элементах из A те же самые). Обратно, любую модель B теории $D(A)$ можно считать расширением интерпретации A, если отождествить $a \in A$ со значением соответствующей константы в B. (Как и раньше, различные элементы A не склеиваются — формула $a_1 \neq a_2$ является бескванторной.)

Теперь мы готовы дать ответ на такой вопрос. Пусть есть нормальная интерпретация A сигнатуры σ и некоторая теория T (с равенством) этой сигнатуры. В каком случае существует расширение B интерпретации A, являющееся нормальной моделью теории T?

Теорема 70. Нормальная интерпретация A сигнатуры σ может быть расширена до нормальной модели теории T (с равенством) тогда и только тогда, когда все Π_1-формулы сигнатуры σ, выводимые из T, истинны в A.

$\lhd$ Если Π_1-формула истинна в некоторой структуре, то она истинна и в подструктуре (область, по которой пробегают переменные в кванторах всеобщности, только уменьшается). Если некоторое расширение B интерпретации A является моделью теории T, то все Π_1-формулы, выводимые из T, истинны в B, а потому и в A.

Осталось доказать обратное: если в A истинны все Π_1-следствия формул из T, то существует искомое расширение. Согласно сказанному выше, достаточно доказать, что теория $D(A) \cup T$ непротиворечива. Если это не так, то из T выводится некоторая бескванторная формула $\varphi(a_1, \ldots, a_n)$, ложная в A. Но в формулы теории T константы $a_1, \ldots, a_n$ не входят, поэтому их можно заменить на свежие переменные $x_1, \ldots, x_n$ и вывести формулу $\varphi(x_1, \ldots, x_n)$ и затем $\forall x_1 \forall x_2 \ldots \forall x_n\, \varphi(x_1, \ldots, x_n)$ Таким образом, мы нашли Π_1-теорему теории T, которая ложна в A (поскольку формула $\varphi(a_1, \ldots, a_n)$ ложна), вопреки нашему предположению. $\rhd$

Рассмотрим пример из алгебры. Пусть F — множество с заданной на нём операцией. В каком случае его можно вложить в коммутативную группу? Согласно теореме 70, для этого необходимо и достаточно, чтобы в F выполнялись все Π_1-следствия аксиом коммутативной группы (записанных в сигнатуре с единственной операцией умножения). Некоторые из этих аксиом сами являются Π_1-формулами. Таковы, например, свойства коммутативности и ассоциативности. Другие аксиомы (существование единицы и обратного) не лежат в Π_1 (например, аксиома о существовании единицы имеет вид $\exists e\forall x\ldots$). Поэтому они не обязаны выполняться в F. Но их Π_1-следствия, например, правило сокращения

$$\forall x\forall y\forall z\,((xy = xz) \to (y = z)),$$

должны выполняться. В данном случае оказывается, что этих трёх утверждений достаточно: всякая коммутативная полугруппа с сокращением может быть вложена в коммутативную группу.

147. Докажите это утверждение. (Указание. Элементами группы можно считать классы формальных выражений вида $x - y$, как это делается, когда от натуральных чисел переходят к целым. В общей ситуации эту группу называют группой Гротендика.)

Вот ещё один хорошо известный пример из алгебры. В каком случае коммутативное кольцо K может быть вложено в поле? Теорема 70 требует, чтобы в K выполнялись все Π_1-теоремы теории полей. Оказывается, что достаточно выполнения единственного Π_1-свойства: отсутствия делителей нуля:

$$\forall x\forall y\,((xy = 0) \to ((x = 0) \vee (y = 0))).$$

В этом случае кольцо может быть вложено в поле.

148. Докажите это утверждение. (Указание. Это поле называют *полем частных*; его элементами являются формальные дроби вида m/n при естественных определениях равенства и операций.)

Не всегда, однако, можно указать простые критерии вложимости. Мы не зря требовали коммутативности: известный советский алгебраист и логик А. И. Мальцев доказал, что не всякое некоммутативное кольцо без делителей нуля вкладывается в тело и что никакое конечное число Π_1-формул не дают критерия вложимости полугруппы в группу (подробнее см. в книге Куроша [14], глава II, параграф 5).

Мы знаем теперь, когда данную интерпретацию можно расширить до модели данной теории. Это позволяет легко ответить и на такой вопрос: когда существует модель данной теории и её расширение, являющееся моделью другой теории.

Теорема 71. Пусть даны две теории (с равенством) T_1 и T_2 некоторой сигнатуры. Тогда следующие свойства равносильны:

(**а**) существует нормальная модель теории T_1 и её расширение, являющееся нормальной моделью теории T_2;

(**б**) объединение T_1 со всеми Π_1-теоремами теории T_2 совместно;

(**в**) объединение T_2 со всеми Σ_1-теоремами теории T_1 совместно.

$\triangleleft$ Прежде всего отметим, что из (а) очевидно следуют (б) и (в). В самом деле, если $M_1 \subset M_2$ — модели соответствующих теорий, то в M_1 истинны все теоремы теории T_1 и все Π_1-теоремы теории T_2 (поскольку они наследуются из M_2), а в M_2 истинны все теоремы теории T_2 и все Σ_1-теоремы теории T_1.

Легко проверить, что симметричные условия (б) и (в) равносильны друг другу, а также такому свойству: не существует Σ_1-теоремы $\exists x_1 \ldots \exists x_n\, \varphi$ теории T_1 и отрицающей её Π_1-теоремы $\forall x_1 \ldots \forall x_n\, \neg\varphi$ теории T_2. Пусть, например, теория T_1 несовместна с Π_1-следствиями теории T_2. В этом противоречии участвует конечное число Π_1-формул, которые можно объединить в одну (см. раздел 4.7, с. 197). Получится Π_1-формула, она будет выводима в теории T_2, а её отрицание — в T_1.

Нам осталось доказать, что любое из свойств (б) и (в) влечёт (а). Здесь нам придётся нарушить симметрию и использовать именно (б). По условию есть интерпретация M_1, в которой истинны все теоремы теории T_1 и все Π_1-теоремы теории T_2. Согласно теореме 70 найдётся её расширение M_2, являющееся моделью T_2, что и требовалось доказать. $\triangleright$

Можно было бы пытаться рассуждать симметричным образом, начав с модели теории T_2, в которой истинны все Π_1-теоремы теории T_1, и пытаться выделить в ней подструктуру, являющуюся моделью теории T_1. Однако этот план не проходит, поскольку аналог теоремы 70 для подструктур неверен.

149. Покажите, что возможна такая ситуация: все Σ_1-теоремы некоторой теории T истинны в некоторой интерпретации M, но M не имеет подструктуры, являющейся моделью теории T. (Указание. Рассмотрим теорию линейно упорядоченных множеств без минимального элемента. Все её Σ_1-следствия верны в $\mathbb{N}+\mathbb{Z}$, поскольку переносятся из $\mathbb{Z}$, поэтому в силу элементарной эквивалентности верны и в $\mathbb{N}$.)

Вот ещё одно следствие доказанных в этом разделе результатов. Теорию T называют Π_1-*аксиоматизируемой*, если существует множество Π_1-формул, из которого выводятся все теоремы теории T и только они.

Напомним, что нормальная интерпретация A сигнатуры σ является *подструктурой* нормальной интерпретации B той же сигнатуры, если B является расширением A, то есть носитель интерпретации A есть подмножество носителя интерпретации B и функциональные и предикатные символы интерпретируются одинаково на аргументах из A. (Другими словами, чтобы задать какую-либо подструктуру данной нормальной интерпретации B, нужно выбрать подмножество носителя B, замкнутое относительно сигнатурных операций.)

Теорема 72 (Лося – Тарского). Теория Π_1-аксиоматизируема тогда и только тогда, когда она устойчива относительна перехода к подструктурам, то есть когда любая подструктура любой её нормальной модели является её моделью.

$\lhd$ Очевидно, Π_1-аксиоматизируемая теория устойчива относительно перехода к подструктурам (все формулы из её Π_1-аксиоматизации остаются истинными). Обратно, пусть T — произвольная теория, устойчивая относительно перехода к подструктурам. Рассмотрим множество T_1 всех Π_1-формул, выводимых в T. Проверим, что все теоремы T выводятся из T_1. Пусть какая-то формула φ выводится из T, но не из T_1. Тогда теория $T_1 + \neg\varphi$ непротиворечива и по теореме 71 найдётся (нормальная) модель теории $\{\neg\varphi\}$ и её расширение, являющееся моделью теории T, что противоречит предположению. $\rhd$

150. Докажите, что если формула устойчива относительно перехода к подструктурам, то она выводимо эквивалентна Π_1-формуле той же сигнатуры.

Симметричное рассуждение доказывает симметричное утверждение про Σ_1-аксиоматизируемые теории.

Теорема 73. Теория является Σ_1-аксиоматизируемой тогда и только тогда, когда она устойчива относительно перехода к расширениям.

151. Проведите подробно соответствующее рассуждение (дав необходимые определения).

152. Докажите, что если формула устойчива относительно перехода к расширениям, то она выводимо эквивалентна Σ_1-формуле той же сигнатуры.

Теоретико-модельные критерии существуют и для других классов формул, в частности Π_2-формул (то есть формул типа $\forall\exists$). Такие формулы не устойчивы ни относительно расширений, ни относительно подструктур. Рассмотрим, например, утверждение об отсутствии наибольшего элемента в упорядоченном множестве. Оно записывается в виде $\forall\exists$-формулы. Истинность его в некотором множестве вовсе не влечёт его истинность в подмножествах и в расширениях. Тем не менее кое-что об этом утверждении сказать можно: если ни одно из множеств возрастающей цепи $M_0 \subset M_1 \subset M_2 \subset \ldots$ не имеет наибольшего элемента, то и объединение $\cup_i M_i$ не имеет наибольшего элемента (проверьте). Именно это свойство, как мы вскоре увидим, характеризует Π_2-формулы.

Пусть дана последовательность

$$M_0 \subset M_1 \subset M_2 \subset \ldots$$

нормальных (в этом разделе мы другие не рассматриваем) интерпретаций сигнатуры σ, причём M_i является подструктурой M_{i+1} (предикаты и функции согласованы). Тогда объединение этой возрастающей цепи интерпретаций также является (нормальной) интерпретацией сигнатуры σ. (Подобная конструкция используется в теории полей, когда строится алгебраическое замыкание счётного поля: мы расширяем поле, добавляя по очереди корни различных многочленов, а потом берём объединение этих полей.)

Заметим, что любая Π_2-формула устойчива относительно объединения цепей: если она истинна во всех M_i, то она истинна и в их объединении. В самом деле, пусть формула $\forall x \exists y\, \varphi(x,y)$ с бескванторной частью $\varphi(x,y)$ истинна во всех M_i. Тогда она истинна и в их объединении. В самом деле, любое x из объединения принадлежит какому-то M_i, и в том же самом M_i можно найти подходящее y. (Если переменных несколько, рассуждение аналогично.)

Поэтому и любая теория, имеющая Π_2-аксиоматизацию, устойчива относительно объединения. Обратное утверждение также верно:

Теорема 74 (Чэна – Лося – Сушко). Теория является Π_2-аксиоматизируемой тогда и только тогда, когда она устойчива относительно объединения возрастающих цепей (объединение любой цепи её моделей также является её моделью).

$\lhd$ Доказательство этой теоремы использует понятие элементарного расширения. Напомним, что M_2 называется элементарным расширением M_1, если $M_1 \subset M_2$ и в M_2 истинны те же формулы с константами из M_1, что и в M_1. (Обозначение: $M_1 \prec M_2$.)

153. Покажите, что если $M_1 \prec M_2 \prec M_3$, то M_3 есть элементарное расширение M_1.

Лемма Тарского. Объединение цепи элементарных расширений $M_1 \prec M_2 \prec M_3 \prec \ldots$ является элементарным расширением каждой из моделей цепи.

Доказательство леммы. Пусть параметрам формулы φ приданы значения в каком-либо из M_i. Нам надо доказать, что полученная формула одновременно истинна или ложна в M_i и в объединении цепи, которое мы обозначим через M. (Из условия леммы мы знаем, что она одновременно истинна или ложна во всех $M_i, M_{i+1}, \ldots$)

Это утверждение доказывается индукцией по построению формулы φ. Для атомарных формул оно очевидно; для логических операций индукция также проходит автоматически. Единственный содержательный случай — это кванторы. Пусть формула φ начинается с квантора $\exists\xi$. Если подходящее значение ξ найдётся уже в M_i, то оно годится и для M (пользуемся предположением индукции). В обратную сторону: если подходящее ξ найдётся в M, то оно принадлежит M_j при достаточно большом j, поэтому формула истинна в M_j (предположение индукции). Остаётся вспомнить, что M_j элементарно эквивалентно M_i.

Как всегда, квантор всеобщности можно выразить с помощью квантора существования (или провести двойственное рассуждение). Лемма Тарского доказана.

Теперь докажем теорему Чэна – Лося – Сушко. Предположим, что теория T устойчива относительно объединения цепей. Обозначим через T' множество всех Π_2-теорем T. Нам надо доказать, что любая модель T' является моделью T.

Для этого, начав с любой модели M' теории T', мы построим цепь интерпретаций

$$M' = M_0 \subset M_1 \subset M_2 \subset M_3 \subset \ldots,$$

в которой чередуются модели теории T' (интерпретации $M_0, M_2, M_4, \ldots$), которые являются элементарными расширениями друг друга, и модели теории T (интерпретации $M_1, M_3, M_5, \ldots$; они, впрочем, также будут моделями теории T').

Объединение всех M_i будет моделью теории T, так как эта теория устойчива относительно расширений. С другой стороны, по лемме Тарского это объединение элементарно эквивалентно интерпретациям $M_0, M_2, M_4, \ldots$ Поэтому все они, включая исходную модель $M' = M_0$, будут моделями теории T, что и требовалось доказать.

Осталось построить требуемую цепь. Интерпретация $M_0 = M'$ уже есть. Будем строить цепь по шагам, продолжая её на каждом шаге на два звена вперёд. Возможность этого обеспечивает такая лемма:

Лемма о расширении. Если все Π_2-следствия теории T истинны в интерпретации A, то можно построить её расширения $A \subset B \subset C$ так, чтобы B было моделью теории T, а C было элементарным расширением A.

Прежде чем доказывать лемму о расширении, покажем (хотя это нам и не понадобится), что сформулированное условие необходимо. Пусть $A \subset B \subset C$, причём C — элементарное расширение A. Тогда любое Π_2-утверждение, истинное в B, истинно и в A. В самом деле, пусть утверждение $\forall x \exists y \varphi(x, y)$ с бескванторной формулой φ истинно в B. Проверим его истинность в A. Если оно ложно при $x = a$, то $\exists y\, \varphi(a, y)$ ложно и в A, и в C (элементарность расширения) и потому не может быть истинным в B (поскольку всякое y из B лежит и в C).

Доказательство леммы о расширении. Что требуется от данного расширения B интерпретации A, чтобы можно было построить C с требуемыми свойствами? Свойства эти состоят в том, что C должно быть моделью теории $\mathrm{Th}_A(A)$ и расширением интерпретации B. Как раз про это говорит теорема 70, надо лишь в качестве σ в этой теореме взять нашу сигнатуру σ с добавленными константами для A (мы обозначали её σ_A), а в качестве теории T из теоремы 70 взять $\mathrm{Th}_A(A)$, то есть множество всех истинных в A формул с константами из A.

Применяя указанный в теореме 70 критерий, можно сформулировать утверждение, которое нам осталось доказать, так: найдётся модель B теории T, которая является расширением A и в которой истинны все Π_1-формулы сигнатуры σ_A, выводимые из $\mathrm{Th}_A(A)$. Вспоминая метод диаграмм, можно сказать, что нас интересует совместность теории T с $D(A)$ и со всеми Π_1-следствиями теории $\mathrm{Th}(A)$ в сигнатуре σ_A. В данном случае $D(A)$ можно и не упоминать явно, так как оно содержится в $\mathrm{Th}_A(A)$.

Итак, осталось доказать, что теория T совместна со всеми Π_1-формулами с константами из A, истинными в A. Если это не так, из T выводится отрицание какой-то из этих формул, то есть некоторая Σ_1-формула

$$\exists\beta_1 \ldots \exists\beta_m \neg\varphi(a_1, \ldots, a_n, \beta_1, \ldots, \beta_m),$$

ложная в A. Константы $a_1, \ldots, a_n$ не входят в теорию T, поэтому из T выводится и формула

$$\forall\alpha_1 \ldots \forall\alpha_n \exists\beta_1 \ldots \exists\beta_m \neg\varphi(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m),$$

которая будет выводимой из T формулой класса Π_2, ложной в A, а таких формул не бывает по условию.

Лемма о расширении (а с ней и теорема Чэна–Лося–Сушко) доказана. $\triangleright$

154. Докажите, что если формула устойчива относительно объединения возрастающих цепей, то она выводимо эквивалентна некоторой Π_2-формуле той же сигнатуры.

155. Покажите, что две интерпретации одной сигнатуры элементарно эквивалентны тогда и только тогда, когда они имеют изоморфные элементарные расширения.

5.6. Ультрафильтры и компактность

В этом разделе мы дадим прямое доказательство теоремы о компактности (теорема 50, с. 189).

Пусть S — непустое множество, а F — непустое семейство подмножеств множества S. Семейство F называется *фильтром* на S, если выполнены следующие три свойства (для наглядности множества из F мы называем далее *большими*):

- $\varnothing \notin F$ (пустое множество не является большим);
- $A \in F,\ B \in F \Rightarrow A \cap B \in F$ (пересечение двух больших множеств — снова большое множество); отсюда следует, что пересечение конечного числа больших множеств — большое множество и что любые два больших множества пересекаются;
- $A \in F,\ A \subset B \Rightarrow B \in F$ (любое надмножество большого множества является большим); отсюда следует, что всё множество S является большим.

Дополнения к большим множествам естественно назвать *малыми.* (Отметим, что множество может не быть ни большим, ни малым; это отличает фильтры от ультрафильтров, которые мы вскоре определим.)

Тривиальным примером фильтра является семейство, состоящее из единственного множества S. Другой пример — семейство всех подмножеств S, содержащих некоторый выделенный элемент $s \in S$. Такой фильтр называется *главным.* Третий пример: пусть S бесконечно, тогда фильтром будет множество всех *коконечных* подмножеств S, то есть подмножеств, дополнение которых конечно. (Другими словами, малыми будут конечные множества.) Последний пример — из анализа: фильтром на $\mathbb{R}$ является семейство всех окрестностей некоторой фиксированной точки a, то есть всех множеств, для которых a является внутренней точкой.

156. Переформулировать определение фильтра в терминах малых множеств.

Заметим, что одно и то же множество не может быть одновременно и большим, и малым, поскольку любые два больших множества пересекаются (по большому, и потому непустому, множеству). Но, как мы уже говорили, множество может не быть ни большим, ни малым. Если таких «промежуточных» множеств нет, фильтр называют ультрафильтром.

Иными словами, *ультрафильтром* называется фильтр на S с таким свойством: $A \in F$ или $S \setminus A \in F$ для любого множества $A \subset S$.

Очевидно, любой главный фильтр является ультрафильтром. Фильтры остальных наших примеров не были ультрафильтрами.

157. Докажите, что на конечном множестве любой ультрафильтр является главным.

158. Докажите, что любой неглавный ультрафильтр содержит все коконечные множества.

159. Докажите, что если ультрафильтр не является главным, то вместе с каждым множеством A он содержит и все множества B, для которых симметрическая разность $A \triangle B$ конечна.

Определение ультрафильтра можно переформулировать следующим образом: ультрафильтры — это фильтры, не имеющие собственных расширений (максимальные по включению). Докажем это. Если фильтр F не максимален, то найдётся больший фильтр F'. Тогда множество $A \in F' \setminus F$ и его дополнение до S не принадлежит F (иначе и A, и его дополнение принадлежали бы фильтру F'). Следовательно, F не является ультрафильтром.

Обратно, пусть фильтр F не является ультрафильтром, и ни множество A, ни его дополнение $S \setminus A$ не принадлежат F. Добавим к F все множества вида $A \cap B$ (для всех $B \in F$) и все их надмножества. Получится фильтр. В самом деле, пустое множество ему не принадлежит, так как иначе бы A не пересекалось с некоторым множеством из F и $S \setminus A$ содержало бы некоторое множество из F потому лежало бы в F. Остальные свойства фильтра очевидны; новый фильтр (в отличие от исходного) содержит A и потому расширяет F.

Теорема 75. Всякий фильтр F на множестве S можно расширить до ультрафильтра $F' \supset F$.

$\lhd$ Доказательство этой теоремы неконструктивно: мы не предъявляем такого фильтра, а устанавливаем его существование с помощью леммы Цорна (см. [6]). Нужно только заметить, что объединение любой цепи фильтров является фильтром (что непосредственно следует из определения).

Другими словами, пока фильтр не станет ультрафильтром, мы берём «промежуточное» множество и расширяем фильтр, объявляя его большим, повторяя этот процесс по трансфинитной индукции. $\triangleright$

160. Докажите, что на любом бесконечном множестве есть неглавный ультрафильтр. (Указание: расширим фильтр коконечных множеств до ультрафильтра.)

Можно представлять себе элементы множества S как голосующих (которые никогда не воздерживаются от голосования). При этом фильтр на S определяет регламент: решение принимается, если множество проголосовавших «за» является большим. Аксиомы фильтра тогда звучат так: решение, против которого все, принято быть не может; если каждое из двух решений принимается, то они принимаются и в совокупности; наконец, принятое решение не может быть отвергнуто, если некоторые из голосовавших против него передумали.

Свойство ультрафильтра также имеет ясный смысл: по любому вопросу можно принять решение (одно из двух противоположных мнений набирает большинство). Главные ультрафильтры соответствуют диктатуре (существенно мнение лишь одного голосующего); задача 157 показывает, что для конечного числа голосующих любые другие способы не позволяют принять решения по некоторым вопросам.

Ультрафильтры можно использовать для построения любопытных примеров. Вот один из них. Рассмотрим игру двух участников, в которой они по очереди объявляют некоторые натуральные числа «своими». На первом шаге начинающий игру объявляет своими числа от нуля до некоторого числа n_1, на втором шаге его противник присваивает числа от n_1 (не включая его) до некоторого большего числа n_2 (включая его), затем первый игрок присваивает числа от n_2 до n_3 и так далее. Партия продолжается неограниченно и делит натуральный ряд между первым и вторым (на два взаимно дополнительных множества). Выигрывает тот, чьё множество большое (принадлежит некоторому фильтру).

Если этот фильтр является ультрафильтром, то в этой игре не может быть ничьей. Если ультрафильтр главный, то игра тривиальна — побеждает тот, кто захватит решающее число, и потому первый может гарантировать выигрыш на первом же ходу.

Теорема 76. Если ультрафильтр неглавный, то ни один из игроков не имеет выигрышной стратегии. (*Стратегия* — это функция, предписывающая следующий ход в зависимости от истории игры. Стратегия считается *выигрышной*, если её использование гарантирует выигрыш при любой игре противника.)

$\triangleleft$ Прежде всего отметим, что оба игрока не могут одновременно иметь выигрышные стратегии. (Что будет, если они оба ими воспользуются?) Покажем теперь, что если выигрышную стратегию имеет один, то её имеет и второй. Совсем просто понять, что если у ходящего вторым есть выигрышная стратегия, то и первый может ей воспользоваться (он должен представить себя вторым, считая, что первый на первом ходу ничего не взял).

Не столь ясно, что выигрышная стратегия первого может быть использована вторым, но и это верно — поскольку конечные множества не влияют на принадлежность ультрафильтру (задача 159), второй может забыть про ход, с которого началась игра, и вообразить себя первым. (Это сделает его первый ход бессмысленным, если этот ход окажется меньше хода противника. В этом случае можно сделать любой ход, а стратегию начать применять со следующего хода.) $\triangleright$

161. Проведите это рассуждение подробно.

Сейчас мы докажем теорему компактности с помощью ультрафильтров. Для этого нам понадобится понятие произведения интерпретаций.

Пусть M_s — семейство интерпретаций некоторой (одной и той же) сигнатуры σ, индексированное множеством S (для каждого $s \in S$ имеется своя интерпретация M_s). Определим произведение интерпретаций

$$\prod_{s\in S} M_s.$$

Элементами носителя будут отображения, сопоставляющие с каждым индексом $s \in S$ некоторый элемент интерпретации M_s. Иными словами, носитель строимой интерпретации будет декартовым произведением всех M_s.

Функциональные символы интерпретировать легко: они применяются отдельно в каждой компоненте. Именно так определяется произведение групп или колец в алгебре. Остаётся определить предикатные символы. В алгебре два элемента в произведении колец или групп считаются равными, если все их компоненты равны. По аналогии будем считать, что два элемента $s \mapsto a_s$ и $s \mapsto b_s$ делают истинным двуместный предикат P, если $P(a_s, b_s)$ истинно в интерпретации M_s для всех s. (Мы взяли двуместный символ для примера, то же самое можно сделать и для символов любой валентности.)

Для произведения двух упорядоченных множеств (индексное множество S равно $\{1, 2\}$, сигнатура есть $(=, \leqslant)$) возникает покомпонентный порядок на парах: $\langle a_1, a_2\rangle \leqslant \langle b_1, b_2\rangle$, если $a_1 \leqslant a_2$ и $b_1 \leqslant b_2$. Заметим, что такой порядок на произведении двух линейно упорядоченных множеств уже не будет линейным (если сомножители состоят более чем из одного элемента).

Нам это не нравится: мы хотим, чтобы произведение интерпретаций обладало бы всеми свойствами, которыми обладают сомножители. Введём понятие *фильтрованного произведения* (по модулю данного фильтра). Пусть на множестве индексов S задан фильтр F. Изменим определение истинности предикатов и будем считать, что элементы $s \mapsto a_s$, $s \mapsto b_s, \ldots$ делают истинным предикат P, если $P(a_s, b_s, \ldots)$ истинно «для большинства s», то есть если множество $\{s \mid P(a_s, b_s, \ldots)\}$ принадлежит фильтру F. В остальном (носитель, функциональные символы) определение остаётся прежним.

Что будет равенством в фильтрованном произведении нормальных интерпретаций? Два элемента произведения (то есть функции на множестве индексов) равны, если они «совпадают почти всюду», то есть множество индексов, где они совпадают, принадлежит фильтру. При этом полученная интерпретация не будет нормальной. Чтобы перейти к нормальной, нужно рассмотреть классы равных элементов — как это делается, скажем, для пространства L_2 интегрируемых с квадратом функций, где элементами являются не сами функции, а их классы с точностью до совпадения почти всюду.

162. Что можно сказать про фильтрованное произведение по главному фильтру?

Вернёмся к нашему примеру: произведению линейно упорядоченных множеств. Будет ли оно линейно упорядоченным? Это зависит от фильтра. Например, если фильтр состоит только из множества S, то фильтрованное произведение совпадает с определённым ранее, и линейного порядка не получится. Но если фильтр является ультрафильтром, то будет. В самом деле, рассмотрим два элемента $s \mapsto a_s$ и $s \mapsto b_s$ в произведении и два множества $\{s \mid a_s \leqslant b_s\}$ и $\{s \mid a_s \geqslant b_s\}$. В объединении они покрывают всё S, и потому (если у нас ультрафильтр) одно из них должно быть большим (если оно не большое, так малое, его дополнение большое и содержится во втором множестве).

163. Докажите, что в фильтрованном произведении нормальных интерпретаций функции и предикаты корректны относительно равенства (то есть совпадения почти всюду): при замене аргументов на равные значение функции совпадает с прежним почти всюду, а значение предиката не меняется.

Это утверждение можно сформулировать так: аксиомы равенства истинны в фильтрованном произведении нормальных интерпретаций. Для ультрафильтров верно и более общее свойство: любая формула, истинная во всех интерпретациях, истинна в фильтрованном произведении по модулю ультрафильтра. Поэтому именно такие *ультрапроизведения* (фильтрованные по модулю ультрафильтра) представляют основной интерес для логики.

Мы сейчас докажем это свойство по индукции. Как обычно, надо предварительно распространить его на формулы с параметрами.

Теорема 77 (Лося об ультрапроизведениях). Пусть параметрами формулы φ являются переменные $a, b, \ldots$ Она будет истинной в ультрапроизведении $\prod_{s\in S} M_s$ при значениях параметров $\alpha, \beta, \ldots$ тогда и только тогда, когда множество тех s, при которых φ истинна в M_s при значениях параметров $\alpha_s, \beta_s, \ldots$, принадлежит ультрафильтру.

Наглядно утверждение теоремы можно сформулировать так: голосование можно проводить не только по атомарным вопросам, а для любых формул. Для замкнутых формул про параметры можно ничего не говорить, и мы получаем, что формула истинна в ультрапроизведении, если и только если она истинна в большинстве (с точки зрения ультрафильтра) сомножителей. В частности, если формула истинна во всех сомножителях, то она истинна и в ультрапроизведении. Это важное утверждение заслуживает особого упоминания:

Следствие. Ультрапроизведение семейства моделей некоторой теории является моделью той же теории.

$\lhd$ Докажем теорему Лося индукцией по построению формулы. Для атомарных формул оно непосредственно следует из определения истинности предикатов.

Пусть формула φ является конъюнкцией двух других формул $\psi \wedge \eta$, для которых утверждение уже верно. Тогда множество тех индексов, для которых φ истинно, является пересечение множеств тех индексов, где истинны ψ и η. Тем самым нам нужно такое свойство ультрафильтра: пересечение двух множеств является большим тогда и только тогда, когда оба они большие. Оно непосредственно следует из определения фильтра (здесь неважно, что это ультрафильтр), поскольку пересечение содержится в обоих множествах.

Для объединения соответствующее свойство звучит так: объединение $S \cup T$ двух множеств большое тогда и только тогда, когда хотя бы одно из множеств S и T большое. В одну сторону (если одно из множеств большое, то и объединение таково) это вытекает из определения фильтра. В обратную сторону надо воспользоваться свойствами ультрафильтра: если $S \cup T$ большое, а оба множества S и T — нет, то они малые, их дополнения большие, пересечение дополнений большое, и не пересекается с $S \cup T$, что невозможно.

Пусть формула φ имеет вид $\neg\psi$. Тогда имеет место такая цепочка: (φ истинна в ультрапроизведении) $\Leftrightarrow$ $\Leftrightarrow$ (ψ ложна в нём) $\Leftrightarrow$ (множество индексов тех сомножителей, где ψ истинна, не является большим) $\Leftrightarrow$ $\Leftrightarrow$ (это множество является малым) $\Leftrightarrow$ (его дополнение большое) $\Leftrightarrow$ (множество номеров тех сомножителей, где ψ ложна (то есть φ истинна), большое).

Импликация сводится к уже рассмотренным случаям ($\psi \to \eta$ эквивалентна $\neg\psi \vee \eta$); можно также сразу заменить формулу на эквивалентную без импликации.

Наиболее интересен случай кванторов. Можно ограничиться квантором существования (квантор всеобщности сводится к нему и к отрицаниям). Он разбирается так (мы используем не вполне корректные обозначения — надеемся, они не вызовут путаницы). Пусть формула $\exists x\, \varphi(x, y, z, \ldots)$ истинна в ультрапроизведении. Это значит, что существует функция $x\colon s \mapsto x_s$, для которой $\varphi(x, y, z, \ldots)$ истинно в ультрапроизведении. По предположению индукции это означает, что для большинства s формула $\varphi(x_s, y_s, z_s, \ldots)$ истинна в M_s. Но тогда для этих индексов s и формула $\exists x\, \varphi(x, y, z, \ldots)$ истинна в M_s, что и требовалось. Обратное рассуждение аналогично: если для большинства s найдётся соответствующее значение x_s, то эти x_s можно собрать в функцию (доопределив её как угодно на малом множестве остальных s), и эта функция будет искомым значением x в ультрапроизведении.

Теорема Лося доказана. $\triangleright$

Мы уже говорили, что произведение нормальных интерпретаций может не быть нормальным. Но теорема Лося гарантирует, что в ультрапроизведении нормальных интерпретаций выполнены аксиомы равенства (поскольку они выполнены в каждом сомножителе), и потому равенство является отношением эквивалентности, и классы эквивалентности уже дают нормальную интерпретацию (с теми же истинными формулами), как мы видели в разделе 5.1.

Теорема Лося позволяет дать прямое доказательство теоремы компактности (теорема 50, с. 189). Она утверждает, что если всякое конечное подмножество данного множества замкнутых формул T совместно (имеет модель), то и всё множество T совместно.

Модель для всего множества T строится как ультрапроизведение. Индексами будут конечные подмножества множества T. Для каждого из них сомножителем будет существующая по условию модель. Теперь надо правильно подобрать фильтр на семействе конечных подмножеств множества T. Нам нужно, чтобы для каждого $t \in T$ семейство всех конечных подмножеств, содержащих t, было бы большим. (В этом случае теорема Лося гарантирует, что t будет истинно в ультрапроизведении.)

Как построить такой фильтр? Для каждого конечного $T' \subset T$ рассмотрим семейство $S(T')$ всех конечных подмножеств, содержащих T'. Очевидно, пересечение таких семейств снова будет семейством такого вида ($S(T') \cap S(T'') = S(T' \cup T'')$), так что после добавления всех надмножеств всех таких множеств получится фильтр. Остаётся расширить этот фильтр до ультрафильтра по теореме 75. Теорема компактности доказана.

Поучительно проследить до конца, что даёт такого рода построение для какого-нибудь конкретного примера. Вспомним построение нестандартного натурального ряда на с. 236. Оно использовало теорему компактности. Сочетая его с приведённым только что доказательством теоремы компактности (и кое-что упростив), получаем такую конструкцию.

Рассмотрим натуральные числа как интерпретацию сигнатуры $(=, +, \times)$. Рассмотрим ультрапроизведение $^*\mathbb{N}$ счётного числа таких интерпретаций по модулю какого-либо неглавного ультрафильтра. Теорема Лося говорит, что в этой интерпретации будут истинны те же формулы, что в натуральном ряду, то есть что $^*\mathbb{N}$ элементарно эквивалентна стандартной интерпретации $\mathbb{N}$.

Покажем, что $\mathbb{N}$ не изоморфна $^*\mathbb{N}$. В самом деле, при таком изоморфизме нуль обязан переходить в элемент $(0, 0, 0, \ldots)$ (точнее, в класс этого элемента относительно равенства), поскольку такой класс обладает свойствами нуля, однозначно его определяющими (в $\mathbb{N}$, а потому и в $^*\mathbb{N}$). По аналогичным причинам единица переходит в класс $(1, 1, 1, \ldots)$ и вообще число k соответствует классу $(k, k, k, \ldots)$. А класс $(0, 1, 2, 3, 4, \ldots)$ отличается от любого класса $(k, k, k, \ldots)$ (они совпадают в единственном сомножителе, а одноэлементное множество является малым, так как ультрафильтр неглавный). Таким образом, построенная нами модель $^*\mathbb{N}$ не является стандартной.

Аналогичное рассуждение позволяет построить и нестандартные модели действительных чисел (о которых мы будем говорить в следующем разделе).

5.7. Нестандартный анализ

Один из создателей теории моделей, А. Робинсон, заметил, что с её помощью можно придать точный смысл понятиям «бесконечно малых» и «бесконечно больших» величин, с которыми оперировали ещё Ньютон и Лейбниц и которые затем были изгнаны и заменены рассуждениями с эпсилонами и дельтами.

Это направление получило название *нестандартного анализа*. Целей тут две: во-первых, упростить доказательства известных теорем, во-вторых, использовать методы нестандартного анализа для получения новых результатов. Насколько эти цели достигнуты за тридцать с лишним лет?

Простота доказательств — дело вкуса. Конечно, всякий преподаватель курса математического анализа мечтает избавиться от утомительных рассуждений с выбором достаточно малых эпсилонов. Но если вместо этого нужно постоянно переходить от модели к её элементарному расширению и обратно, лекарство может оказаться страшнее болезни. Во всяком случае, «нестандартные» учебники математического анализа для нематематиков (один из них написан Кейслером [34]) большого распространения не получили.

Новые результаты действительно были получены; отметим, что многие из них (хотя и не все) впоследствии были передоказаны «стандартными» методами, так что и здесь революции не произошло.

Так или иначе, нестандартный анализ — интересное приложение теории моделей, и мы разберём несколько простых примеров. Более подробно об этом можно прочесть в книгах Дэвиса [11] и Успенского [27], а также в последней главе книги Робинсона [22].

Идея нестандартного анализа проста. Среди действительных чисел, увы, нет бесконечно малых (которые были бы меньше $1/n$ при всех $n = 1, 2, 3, \ldots$) — как говорят, поле вещественных чисел удовлетворяет *аксиоме Архимеда.* (Оригинальная формулировка этой аксиомы: каковы бы ни были два отрезка, можно отложить меньший из них столько раз, чтобы превзойти больший.) Но можно рассмотреть элементарное расширение поля $\mathbb{R}$, в котором такие бесконечно малые элементы есть, и использовать их для определения пределов, производных и прочего в исходном поле.

Перейдём к формальным определениям. Мы будет рассматривать вещественную прямую как модель очень богатой сигнатуры. Для каждого отношения на $\mathbb{R}$ (с произвольным числом аргументов) введём свой предикатный символ. Получится $2^{\mathfrak{c}}$ предикатных символов. Кроме того, для каждой функции из $\mathbb{R}^n$ в $\mathbb{R}$ (при всех $n = 0, 1, 2, \ldots$) введём свой функциональный символ. Это даст ещё $2^{\mathfrak{c}}$ символов.

Пусть $^*\mathbb{R}$ — любая нормальная интерпретация этой сигнатуры, элементарно эквивалентная $\mathbb{R}$. Её можно считать полем, расширяющим поле $\mathbb{R}$. В самом деле, среди функциональных символов есть двуместные символы для сложения и умножения. Они задают некоторые операции в $^*\mathbb{R}$ и относительно этих операций множество $^*\mathbb{R}$ будет полем, так как аксиомы поля можно записать в виде формул (эти формулы истинны в $\mathbb{R}$, а потому и в $^*\mathbb{R}$). Аналогичное рассуждение с предикатом «меньше» показывает, что $^*\mathbb{R}$ является упорядоченным полем.

Это поле можно считать расширением поля $\mathbb{R}$. В самом деле, для каждого действительного числа x в сигнатуре имеется константа. Значения таких констант образуют подполе в $^*\mathbb{R}$, изоморфное $\mathbb{R}$. В самом деле, утверждения вида $a \ne b$, $a + b = c$ и $ab = c$ являются формулами, и переносятся из $\mathbb{R}$ в $^*\mathbb{R}$. Аналогичным образом это вложение сохраняет порядок.

Если поле $^*\mathbb{R}$ исчерпывается значениями констант из $\mathbb{R}$, то ничего интересного не получается. Поэтому мы будем предполагать, что это не так. Возможность построить $^*\mathbb{R}$, не совпадающее с $\mathbb{R}$, следует (например) из теоремы Лёвенгейма–Сколема о повышении мощности. Другой способ: добавим в сигнатуру новую константу c и рассмотрим теорию

$$\mathrm{Th}(\mathbb{R}) + \{c > \bar{a} \mid a \in \mathbb{R}\},$$

где $\mathrm{Th}(\mathbb{R})$ — множество всех истинных в $\mathbb{R}$ формул нашей сигнатуры, а $\bar{a}$ — константа для числа a. Совместность этой теории доказывается с помощью теоремы компактности. Любая её модель годится в качестве $^*\mathbb{R}$, поскольку значение константы c должно быть больше всех элементов из $\mathbb{R}$.

164. Проведите это рассуждение подробно.

В дальнейшем мы предполагаем, что выбрана и зафиксирована некоторая интерпретация $^*\mathbb{R}$, являющаяся элементарным расширением $\mathbb{R}$ и не совпадающая с $\mathbb{R}$. Её элементы мы называем *гипердействительными* числами. Среди них есть и действительные числа, которые мы будем называть также *стандартными* элементами $^*\mathbb{R}$. Остальные элементы $^*\mathbb{R}$ будут *нестандартными* гипердействительными числами. (По нашему предположению таковые существуют.)

Утверждение об элементарной эквивалентности $^*\mathbb{R}$ и $\mathbb{R}$ называют *принципом переноса*: он позволяет перенести истинность формулы из $\mathbb{R}$ в $^*\mathbb{R}$ (или наоборот).

Возможность переноса не ограничивается алгебраическими свойствами. Например, в нашей сигнатуре есть функция sin. В интерпретации $^*\mathbb{R}$ ей соответствует функция, которую можно было бы назвать «гипердействительным синусом». Эта функция продолжает обычный синус (для стандартных аргументов), поскольку утверждения вида $\sin a = b$ для конкретных стандартных a и b можно перенести в $^*\mathbb{R}$. Более того, она обладает обычными свойствами синуса: скажем, гипердействительный синус любого гипердействительного числа не превосходит единицы (в смысле порядка на $^*\mathbb{R}$), поскольку формула $\forall x \sin x \leqslant 1$ выдерживает перенос. Аналогично можно поступать и с предикатами: например, предикат «быть натуральным числом» задаёт в $^*\mathbb{R}$ некоторое подмножество, элементы которого естественно назвать *гипернатуральными* числами. Гипернатуральные числа делятся на стандартные (соответствующие обычным натуральным числам в $\mathbb{R}$) и нестандартные. (Мы увидим, что нестандартные числа обязательно найдутся.) Множество гипернатуральных чисел обозначается $^*\mathbb{N}$.

Аналогично определяется множество $^*\mathbb{Z}$ *гиперцелых чисел* и вообще множество $^*M$ для любого множества M действительных чисел. (Множеству M соответствует одноместный предикатный символ; $^*M$ — интерпретация этого символа в $^*\mathbb{R}$.) Множество $^*M$ называют нестандартным расширением M. В нём содержатся те же стандартные числа, что и в M (формулы вида $a \in M$ для стандартных чисел a переносятся), и, возможно, некоторые нестандартные числа.

Принцип переноса гарантирует, что для конечного M нестандартных элементов в $^*M$ не появится. В самом деле, пусть, скажем, в M ровно три элемента a, b и c. Тогда формула

$$\forall x\,(M(x) \leftrightarrow ((x = a) \vee (x = b) \vee (x = c))),$$

в которой $M(x)$ — предикат, соответствующий множеству M, истинна в $\mathbb{R}$. По принципу переноса она истинна и в $^*\mathbb{R}$, так что и $^*M$ состоит из трёх элементов, являющихся значениями констант a, b и c (отождествлённых со стандартными действительными числами).

Впоследствии мы увидим, что бесконечное множество M обязательно приобретёт новые нестандартные элементы при переходе к $^*\mathbb{R}$.

Несколько простых следствий принципа переноса:

- $M \subset N \Leftrightarrow {}^*M \subset {}^*N$ (применяем принцип переноса к формуле $\forall x\,(M(x) \to N(x)))$;
- $^*(M \cup N) = {}^*M \cup {}^*N$, (применяем принцип переноса к формуле $\forall x((M(x) \vee N(x)) \leftrightarrow K(x))$, где K — объединение M и N);
- аналогичные утверждения верны и для пересечения и разности множеств.

165. Покажите, что для счётного объединения аналогичное утверждение может не быть верным и $^*(M_0 \cup M_1 \cup M_2 \cup \ldots)$ может отличаться от $({}^*M_0 \cup {}^*M_1 \cup {}^*M_2 \cup \ldots)$.

Нестандартные аналоги имеют не только множества, но и функции. Мы уже говорили о нестандартном аналоге синуса. Точно так же можно определить нестандартный аналог любой всюду определённой функции (любого числа аргументов). Для не всюду определённых функций (например, для функции квадратного корня) надо рассмотреть её график как предикат (для корня это будет предикат двух аргументов) и взять его нестандартный аналог. Этот нестандартный аналог будет графиком частичной функции (ибо свойство «быть графиком частичной функции» записывается формулой). Соответствующая функция и будет нестандартным аналогом исходной.

166. Покажите, что (построенный по этой схеме) нестандартный квадратный корень имеет областью определения множество неотрицательных гипердействительных чисел и что $(\sqrt{x})^2 = x$ для любого неотрицательного гипердействительного числа x.

167. Покажите, что для всюду определённой функции два способа её продолжения (как функции и через график) дают одну и ту же функцию.

168. Покажите, что если множество A является областью определения частичной функции φ, то его нестандартный аналог ${}^*A$ совпадает с областью определения функции ${}^*\varphi$.

Мы будем часто опускать звёздочки в записях вида ${}^*f(x)$, пользуясь таким соглашением: если речь идёт о значении функции на гипердействительном числе, то подразумевается нестандартный аналог этой функции. (Путаницы не будет, так как на стандартных числах значения функции и её гипердействительного аналога совпадают.)

169. Абсолютную величину гипердействительного числа x можно определить как x при $x \geqslant 0$ и как $(-x)$ при $x \leqslant 0$. С другой стороны, можно рассмотреть нестандартный аналог функции $x \mapsto |x|$. Покажите, что получится одно и то же.

170. Покажите, что поле гипердействительных чисел является вещественно замкнутым (согласно определению на с. 226)

Любое гипердействительное число x можно представить в виде суммы гиперцелого числа n и некоторого гипердействительного числа α, для которого $0 \leqslant \alpha < 1$. Чтобы убедиться в этом, достаточно рассмотреть нестандартные аналоги функций целой и дробной части. Принцип переноса гарантирует, что они сохранят свои свойства. В частности, в сумме они дают исходное число, а дробная часть всегда не меньше нуля и меньше единицы.

Целью расширения было получить возможность рассматривать бесконечно большие и бесконечно малые числа. Дадим соответствующие определения.

Гипердействительное число α, большее всех стандартных чисел, называется *положительным бесконечно большим.* Аналогично определяются отрицательные бесконечно большие числа.

171. Докажите, что число α является отрицательным бесконечно большим тогда и только тогда, когда $-\alpha$ является положительным бесконечно большим. Докажите, что $|\alpha|$ является положительным бесконечно большим тогда и только тогда, когда α является либо положительным, либо отрицательным бесконечно большим.

Гипердействительные числа, не являющиеся бесконечно большими, называют конечными. Другими словами, гипердействительное число x называется *конечным*, если оно лежит в промежутке $a \leqslant x \leqslant b$ со стандартными концами a и b.

Наконец, гипердействительное число называется *бесконечно малым*, если его абсолютная величина меньше любого стандартного положительного числа. (Согласно этому определению нуль тоже является бесконечно малым числом.) Легко проверить, что ненулевое число e является бесконечно малым тогда и только тогда, когда $1/e$ бесконечно велико. В самом деле, пусть, например, $e > 0$ бесконечно мало. Тогда $1/e$ больше любого стандартного числа $c > 0$, так как $e < 1/c$. Остальные случаи разбираются аналогично.

Сумма и произведение двух конечных чисел конечны. Если α по модулю меньше стандартного числа a, а β — стандартного числа b, то $\alpha + \beta$ по модулю меньше стандартного числа $a + b$, а $\alpha\beta$ по модулю меньше ab. (Неравенства в гипердействительных числах можно складывать и умножать, так как обычные свойства неравенств записываются формулами и допускают перенос.)

В обычном курсе математического анализа аналогом этого рассуждения является утверждение о том, что сумма и произведение ограниченных последовательностей ограничены. Другое стандартное утверждение из курса анализа — о произведении ограниченных и бесконечно малых (сходящихся к нулю) последовательностей — также имеет естественный аналог: произведение конечного и бесконечно малого гипердействительных чисел является бесконечно малым гипердействительным числом. Доказательство также вполне традиционно: если α не превосходит стандартного числа a, а $|\beta|$ меньше любого стандартного положительного числа, то $\alpha\beta$ меньше любого стандартного положительного e, так как $|\beta| < e/a$.

Два гипердействительных числа α, β называются *бесконечно близкими*, если их разность бесконечно мала. Обозначение: $\alpha \approx \beta$.

172. Докажите, что если $\alpha \approx \beta$, то $\alpha+\gamma \approx \beta+\gamma$ для любого гипердействительного γ, а $\alpha\gamma \approx \beta\gamma$ для любого конечного гипердействительного γ. Покажите, что условие конечности существенно.

173. Покажите, что два конечных гипердействительных числа бесконечно близки тогда и только тогда, когда между ними нельзя вставить двух разных стандартных чисел.

Легко проверить, что отношение бесконечной близости является отношением эквивалентности на множестве гипердействительных чисел. Классы эквивалентности этого отношения иногда называют *монадами* (термин, использовавшийся ещё Лейбницем).

Теорема 78. Любое конечное гипердействительное число бесконечно близко к некоторому стандартному числу.

(Заметим, что обратное утверждение очевидно: всякое гипердействительное число, бесконечно близкое к некоторому стандартному a, конечно, поскольку содержится между стандартными числами $a-1$ и $a+1$.)

$\triangleleft$ Пусть α — конечное гипердействительное число. Рассмотрим множество множество L всех стандартных действительных чисел, меньших или равных α, а также множество R всех стандартных действительных чисел, больших или равных α. Конечность числа α гарантирует, что оба этих множества непусты (если бы, скажем, R было пусто, то α было бы положительным бесконечно большим). Заметим, что L и R не пересекаются (если только α само не является стандартным, и тогда доказывать нечего) и в объединении дают всё $\mathbb{R}$.

По аксиоме полноты существует действительное число a, для которого $L \leqslant a \leqslant R$. Покажем, что $\alpha - a$ бесконечно мало. Проверим, например, что для любого стандартного $e > 0$ выполнено неравенство $\alpha - a < e$, то есть $\alpha < a + e$. Это понятно: если $a + e \leqslant \alpha$, то $a + e \in \in L$, что противоречит свойству $L \leqslant a$. По аналогичным причинам $\alpha - a > -e$. $\triangleright$

Стандартное число a, бесконечно близкое к конечному гипердействительному α, называется *стандартной частью* числа α. Стандартная часть определена однозначно, так как два разных стандартных числа не могут быть бесконечно близки к одному и тому же гипердействительному числу (тогда бы они были близки друг к другу, что невозможно). Поэтому можно ввести обозначение $\operatorname{st}\alpha$ для стандартной части конечного числа α.

174. Докажите, что если α и β конечны, причём $\alpha \leqslant \beta$, то и $\operatorname{st}\alpha \leqslant \operatorname{st}\beta$.

Теорема 79. Среди гипердействительных чисел есть ненулевые бесконечно малые, а также бесконечно большие числа.

$\triangleleft$ Напомним, что по нашему предположению $^*\mathbb{R}$ не совпадает с $\mathbb{R}$, то есть существует некоторое нестандартное гипердействительное число α. Если α бесконечно, то $1/\alpha$ — искомое ненулевое бесконечно малое число. Если α конечно, то $\alpha - \operatorname{st}(\alpha)$ — искомое ненулевое бесконечно малое число (а обратное к нему будет бесконечно большим). $\triangleright$

Заметим, что при построении гипердействительных чисел с помощью формул $c > a$ (для новой константы c и всех стандартных a) и теоремы компактности существование бесконечно больших элементов очевидно: таковым будет значение этой самой константы c.

Теперь обратимся к натуральным и целым числам.

Теорема 80. Существуют нестандартные гипернатуральные числа, при этом все они бесконечно велики.

(Таким образом, для гипернатуральных чисел конечность и стандартность равносильны.)

$\triangleleft$ Всякое положительное действительное число есть сумма натурального и числа из $[0, 1)$. Принцип переноса гарантирует, что всякое положительное гипердействительное число α есть сумма гипернатурального ν и гипердействительного τ, для которого $0 \leqslant \tau < 1$. Возьмём α бесконечно большим, тогда и ν будет бесконечно большим. Первое утверждение доказано.

Пусть теперь ν — конечное гипернатуральное число. По определению конечности оно меньше некоторого стандартного числа a, скажем, числа 5. Но в стандартной модели верна формула

$$\forall x\,(((x \in \mathbb{N}) \wedge (x < 5)) \to \\ \to ((x = 0) \vee (x = 1) \vee (x = 2) \vee (x = 3) \vee (x = 4))).$$

По принципу переноса она верна и в ${}^*\mathbb{R}$, поэтому число ν совпадает с одним из стандартных чисел $0, 1, 2, 3, 4$. $\triangleright$

175. Покажите, что для всякого гипердействительного числа существует большее его гипернатуральное.

176. Рассмотрим гипернатуральные числа как упорядоченное множество. Покажите, что оно изоморфно $\mathbb{N} + \mathbb{Z} \times F$, где F — плотное линейно упорядоченное множество без первого и последнего элементов. (Порядок на $\mathbb{Z} \times F$: сравниваются сначала вторые элементы, а при равенстве — первые.)

Гипернатуральные числа позволяют говорить о бесконечно далёких членах (стандартных) последовательностей действительных чисел. Пусть $a_0, a_1, \ldots$ — такая последовательность. Рассмотрим её график, то есть множество пар $\langle 0, a_0\rangle, \langle 1, a_1\rangle, \ldots$, как двуместный предикат. Утверждение о том, что этот предикат задаёт график функции, определённой на натуральных числах, можно записать в виде формулы. Принцип переноса гарантирует, что гипердействительный аналог этого предиката будет функцией, определённой на гипернатуральных числах и принимающей гипердействительные значения. Значение этой функции на гипернатуральном числе n можно обозначать a_n, не опасаясь путаницы (при стандартных n мы получаем одно и то же).

Таким образом, любая последовательность приобретает — помимо своего желания — бесконечный «хвост».

177. Покажите, что если две последовательности отличаются лишь в конечном числе членов, то их бесконечные хвосты одинаковы.

Сейчас мы используем продолжение последовательностей для доказательства такого факта:

Теорема 81. Нестандартный аналог ${}^*A$ множества A действительных чисел совпадает с A тогда и только тогда, когда множество A конечно.

$\triangleleft$ Если A конечно, и, скажем, состоит из трёх элементов p, q, r, то можно записать формулу

$$\forall x\,((x \in A) \leftrightarrow ((x = p) \vee (x = q) \vee (x = r)).$$

По принципу переноса эта формула остаётся истинной в ${}^*\mathbb{R}$, так что ${}^*A$ состоит из тех же трёх элементов.

Пусть теперь A бесконечно. Покажем, что ${}^*A$ содержит элементы, не входящие в A. Пусть $a_0, a_1, \ldots$ — последовательность различных элементов множества A. Напишем формулу, которая утверждает, что все элементы этой последовательности различны и принадлежат A. По принципу переноса все бесконечные члены этой последовательности (точнее, её гипердействительного аналога) также различны, принадлежат ${}^*A$ и отличаются от всех конечных членов последовательности. Они и будут искомыми нестандартными элементами ${}^*A$. В самом деле, бесконечный член a_ν при бесконечном гипернатуральном ν не может совпасть с конечными членами, а также не может совпасть со стандартным элементом $a \in A$, не входящим в исходную последовательность (ибо утверждение «$a_n \neq a$ при всех n» записывается формулой). $\triangleright$

Галактикой гипердействительного числа α называют множество всех гипердействительных β, для которых разность $\alpha - \beta$ конечна.

178. Покажите, что множество гипердействительных чисел разбивается на галактики. Определите на галактиках естественное отношение линейного порядка и покажите, что этот порядок плотный и не имеет наибольшего и наименьшего элементов.

179. Каждое действительное число a, не являющееся двоично-рациональным, можно единственным образом записать в виде бесконечной двоичной дроби $\ldots, a_0 a_1 \ldots$; другими словами, ему соответствует последовательность нулей и единиц (нас будет интересовать лишь дробная часть после запятой). Фиксируем бесконечное гипернатуральное ν и рассмотрим те числа a, у которых $a_\nu = 0$. Покажите, что множество таких чисел переходит в своё дополнение при симметрии относительно любой двоично-рациональной точки (другими словами, $a \in M \Leftrightarrow r - a \in M$ для двоично-рациональных r) и потому не может быть измеримым по Лебегу.

180. Докажите, что гиперрациональными числами являются отношения гиперцелых чисел и только они. Докажите, что каждое гипердействительное число бесконечно близко к некоторому гиперрациональному числу.

Покажем теперь, как можно ввести основные понятия математического анализа, используя бесконечно малые и бесконечно большие числа.

Теорема 82. Пусть $M \subset \mathbb{R}$. Множество M ограничено (в обычном смысле) тогда и только тогда, когда все элементы его гипердействительного аналога конечны.

Таким образом, в курсе нестандартного анализа можно определять ограниченные множества как множества, не содержащие бесконечных элементов.

$\lhd$ Если все элементы M меньше некоторого стандартного a по модулю, то и все элементы ${}^*M$ меньше того же a (принцип переноса), поэтому в одну сторону утверждение очевидно.

Пусть теперь M не ограничено (скажем, сверху). Тогда в $\mathbb{R}$ верно такое утверждение: для всякого c найдётся элемент множества M, больший c. Применим принцип переноса и возьмём бесконечно большое c. Получим, что в ${}^*M$ есть бесконечно большой элемент. $\rhd$

181. Покажите, что если все элементы множества ${}^*M$ меньше некоторого гипердействительного c, то M ограничено.

182. Говорят, что множество S гипердействительных чисел является *внутренним*, если оно есть гипердействительный аналог некоторого множества A действительных чисел. Покажите, что множество конечных гипердействительных чисел не является внутренним.

183. Докажите, множество $S \subset {}^*\mathbb{R}$ выразимо (в рассматриваемой нами сигнатуре, содержащей символы для всех функций и предикатов на множестве $\mathbb{R}$) тогда и только тогда, когда оно является внутренним.

Нестандартный анализ позволяет дать естественные определения предельной точки и предела.

Теорема 83. Число a является предельной точкой последовательности действительных чисел $a_0, a_1, \ldots$ тогда и только тогда, когда найдётся бесконечно далёкий член последовательности, бесконечно близкий к a.

(Бесконечно далёкий член последовательности — значение a_ν при бесконечном гипернатуральном ν.)

$\triangleleft$ Если a является предельной точкой, то для всякого положительного ε и всякого натурального N найдётся натуральное $n > N$, для которого $|a_n - a| < \varepsilon$. Применим принцип переноса, положив ε бесконечно малым и N бесконечно большим. Получим искомый бесконечно близкий к a член с бесконечно большим гипернатуральным номером.

Напротив, если для некоторого натурального N и для некоторого $\varepsilon > 0$ все члены последовательности, начиная с N-го, отстоят от a более чем на ε, то по принципу переноса все бесконечно далёкие члены последовательности также отстоят от a более чем на ε. $\triangleright$

184. Покажите, что число a принадлежит замыканию множества $M \subset \mathbb{R}$ тогда и только тогда, когда некоторый элемент множества ${}^*M$ бесконечно близок к a.

185. Как определить в терминах нестандартного анализа понятие предельной точки множества (в любой окрестности которой бесконечно много членов множества)?

Теперь видно, что нестандартный анализ позволяет в два счёта доказать теорему о том, что всякая ограниченная последовательность имеет предельную точку: в самом деле, любой бесконечно далёкий член этой последовательности конечен, и его стандартная часть будет предельной точкой!

Теорема 84. Последовательность $a_0, a_1, \ldots$ действительных чисел сходится к числу a тогда и только тогда, когда все её бесконечно далёкие члены бесконечно близки к a.

$\triangleleft$ Пусть a является пределом. Тогда для всякого ε найдётся N, начиная с которого все члены последовательности отстоят от a менее чем на ε. В частности, все бесконечно далёкие члены таковы и их расстояние до a меньше любого стандартного ε.

Напротив, пусть a не является пределом и для всякого N найдётся член a_n с номером $n > N$, отстоящий от a более чем на $\varepsilon > 0$ (пока что все параметры стандартны). Применим принцип переноса, взяв N бесконечно большим, и найдём бесконечно далёкий член последовательности, отстоящий от a более чем на стандартное $\varepsilon > 0$. $\triangleright$

Приведём теперь нестандартные критерии стандартных топологических понятий.

Теорема 85. Множество $M \subset \mathbb{R}$ открыто тогда и только тогда, когда вместо со всякой точкой $m \in M$ оно содержит и всю её монаду, то есть все гипердействительные точки, бесконечно близкие к m.

В этой формулировке, строго говоря, следовало бы сказать «его нестандартный аналог $^*M$» вместо «оно»; напомним также, что M и $^*M$ содержат одни и те же стандартные числа.

$\triangleleft$ Если M открыто и содержит вместе с точкой $m \in M$ её ε-окрестность, то монада точки m по принципу переноса содержится в M.

Если же некоторая точка $m \in M$ не является внутренней и для всякого действительного $\varepsilon > 0$ найдётся точка вне M на расстоянии меньше ε, применим принцип переноса и возьмём бесконечно малое ε. Мы получим число, бесконечно близкое к m и не лежащее в $^*M$. $\triangleright$

Переходя к дополнениям, получаем, что множество $M \subset \mathbb{R}$ замкнуто тогда и только тогда, когда любая стандартная точка, бесконечно близкая к некоторой точке из $^*M$, принадлежит M.

На прямой компактными являются замкнутые ограниченные множества. Соединим нестандартные критерии замкнутости и ограниченности:

Теорема 86. Множество $M \subset \mathbb{R}$ компактно тогда и только тогда, когда любой элемент множества $^*M$ бесконечно близок к некоторому (стандартному) элементу множества M.

$\lhd$ В самом деле, ограниченность означает, что любой элемент множества M конечен, то есть бесконечно близок к стандартному числу, а замкнутость позволяет заключить, что это число принадлежит M. $\rhd$

186. Используя полученные только что критерии, покажите, что любой отрезок $[a, b]$ действительной прямой компактен, а любой интервал (a, b) открыт.

187. Покажите, используя нестандартный критерий открытости, что объединение любого числа открытых множеств открыто. (Напоминание: гипердействительный аналог объединения может не совпадать с объединением гипердействительных аналогов!)

188. Покажите, что пересечение двух (или любого конечного числа) открытых множеств открыто. (Где используется конечность?)

189. Докажите, что последовательность фундаментальна тогда и только тогда, когда любые два её бесконечных члена бесконечно близки (предварительно уточнив формулировку этого утверждения).

190. Докажите, что всякая фундаментальная последовательность сходится, используя приведённый критерий фундаментальности. (Указание. Ограниченность приходится доказывать, исходя из стандартных определений.)

191. Докажите, что если последовательность ограничена и имеет единственную предельную точку, то она сходится (к этой точке).

192. Докажите, что ограниченная возрастающая последовательность имеет предел.

Перейдём к функциям действительного переменного и дадим нестандартное определение предела (аналогичное приведённому выше для последовательностей).

Теорема 87. Число $b \in \mathbb{R}$ есть предел функции $f\colon \mathbb{R} \to \mathbb{R}$ в точке $a \in \mathbb{R}$ тогда и только тогда, когда $f(x) \approx b$ для всех x, бесконечно близких к a, но отличных от a.

$\triangleleft$ Пусть функция f имеет предел b согласно ε-δ-определению и для всякого $\varepsilon > 0$ найдётся $\delta > 0$ с нужными свойствами. Бесконечно близкое к a число x попадает в δ-окрестность точки a при любом стандартном $\delta > 0$, поэтому $f(x)$ попадает в ε-окрестность точки b.

Напротив, если при некотором $\varepsilon > 0$ для любого $\delta > 0$ найдётся точка x, для которой $|x - a| < \delta$, но $|f(x) - b| \geqslant \varepsilon$, то можно применить принцип переноса (для данного стандартного ε) и взять бесконечно малое δ. $\triangleright$

Непосредственным следствием является нестандартный критерий непрерывности: функция $f\colon \mathbb{R} \to \mathbb{R}$ непрерывна в (стандартной) точке a тогда и только тогда, когда $f(x) \approx f(a)$ для всех x, бесконечно близких к a.

Для функции, определённой на некотором множестве $M \subset \mathbb{R}$, критерий непрерывности в точке $m \in M$ выглядит так: $f(m) \approx f(m')$ для всякой точки $m' \in {}^*M$, бесконечно близкой к m.

193. Проверьте это.

Поучительно понять, чем это свойство отличается от равномерной непрерывности.

Теорема 88. Функция $f\colon \mathbb{R} \to \mathbb{R}$ равномерно непрерывна на множестве $M \subset \mathbb{R}$ тогда и только тогда, когда для всех $x, y \in {}^*M$ выполнено $x \approx y \Rightarrow f(x) \approx f(y)$.

$\triangleleft$ Пусть выполнено обычное ε-δ-определение непрерывности. Бесконечно близкие точки x, y отличаются менее чем на (стандартное) δ, а потому их образы отличаются менее чем на ε. Это верно для любого стандартного ε, поэтому $f(x) \approx f(y)$.

Обратно, если функция не является равномерно непрерывной, то для некоторого ε и для любого δ найдутся точки, отстоящие менее чем на δ, образы которых отстоят более чем на ε. Остаётся применить при данном ε принцип переноса и взять бесконечно малое δ. $\triangleright$

Чем это отличается от непрерывности во всех точках множества M? Непрерывность во всех точках M означает, что для любого стандартного $m \in M$ и любого бесконечно близкого к нему $m' \in {}^*M$ мы имеем $f(m) \approx f(m')$. Отсюда следует, что для любых $m', m'' \in {}^*M$, бесконечно близких к некоторому стандартному $m \in M$, выполнено $f(m') \approx f(m'')$. Но в множестве ${}^*M$ могут быть бесконечно близкие элементы, стандартная часть которых не лежит в M (или вообще не имеющие стандартной части, то есть бесконечные). Легко понять, что для компактного M такого быть не может (стандартная часть любого элемента $m' \in {}^*M$ принадлежит M согласно теореме 86). Тем самым мы получили (почти что тривиальное) нестандартное доказательство классической теоремы: непрерывная на компакте функция равномерно непрерывна.

Вот ещё несколько «нестандартных» доказательств стандартных (во всех смыслах этого слова) теорем из курса математического анализа.

Теорема 89. Непрерывная на отрезке функция, принимающая значения разных знаков на концах отрезка, имеет нуль на этом отрезке.

$\triangleleft$ Разделим отрезок на n равных частей. Среди них найдётся часть, на которой функция меняет знак. По принципу переноса и при делении отрезка на бесконечное гипернатуральное число частей найдётся часть, на которой функция меняет знак. Но концы этой части бесконечно близки к некоторой стандартной точке отрезка. Эта точка будет нулём функции (если в ней функция, скажем, положительна, то по непрерывности в бесконечно близких к ней концах отрезка изменения знака функция будет положительной). $\triangleright$

Теорема 90. Непрерывная во всех точках компакта функция ограничена на нём.

$\triangleleft$ Пусть функция f непрерывна на компакте M. Следуя нестандартному критерию ограниченности, мы должны показать, что значения функции ${}^*f$ во всех точках ${}^*M$ конечны. Но всякая точка $x \in {}^*M$ бесконечно близка к некоторой стандартной точке $y \in M$ (компактность), а потому $^*f(x) \approx {}^*f(y)$ (непрерывность), поэтому $^*f(x)$ конечно. $\triangleright$

Обратите внимание, что мы пользовались аксиомой полноты (множества действительных чисел) только один раз, при доказательстве теоремы 78. Это и не удивительно, поскольку из утверждения этой теоремы следует аксиома полноты.

194. Убедитесь в этом, следуя такой схеме. Пусть A — произвольное ограниченное множество действительных чисел. Покажите (стандартными рассуждениями), что для любого ε найдётся число c, являющееся верхней гранью, для которого $c - \varepsilon$ не будет верхней гранью. Примените принцип переноса, взяв бесконечно малое ε и рассмотрев стандартную часть соответствующего числа c.

195. Докажите, что производная стандартной функции $f\colon \mathbb{R} \to \mathbb{R}$ в стандартной точке a равна стандартному числу b тогда и только тогда, когда $(f(a+h) - f(a))/h \approx b$ для всех бесконечно малых $h \neq 0$.

196. Покажите, что $(x^n)' = nx^{n-1}$ согласно нестандартному определению производной (предыдущая задача).

197. Как использовать нестандартный анализ для определения понятия интеграла?

В наших примерах все рассмотрения были ограничены множеством гипердействительных чисел. Это ограничение кажется существенным — не вполне ясно, каким образом можно применить те же методы к произвольному топологическому пространству (в котором нет бесконечно больших чисел). Тем не менее это возможно, и об этом можно прочесть в книгах Дэвиса [11] или Успенского [27].

Литература

[1] А. Ахо, Дж. Ульман, Дж. Хопкрофт. *Построение и анализ вычислительных алгоритмов*, пер. с англ. А. О. Слисенко под редакцией Ю. В. Матиясевича. М.: Мир, 1979.

[2] Дж. Булос, Р. Джеффри. *Вычислимость и логика*, пер. с англ. В. А. Душского и Е. Ю. Ногиной под редакцией С. Н. Артёмова. М.: Мир, 1994. 396 с.

[3] Н. Бурбаки. *Начала математики. Первая часть. Основные структуры анализа. Книга первая. Теория множеств*, пер. с французского Г. Н. Поварова и Ю. А. Шихановича под редакцией В. А. Успенского. М.: Мир, 1965.

[4] Б. Л. ван дер Варден. *Алгебра*, перевод с немецкого А. А. Бельского. Под редакцией Ю. И. Мерзлякова. М.: Наука, главная редакция физико-математической литературы, 1976.

[5] Н. К. Верещагин, А. Шень. *Лекции по математической логике и теории алгоритмов. Вычислимые функции.* М.: МЦНМО, 1999. 176 с.

[6] Н. К. Верещагин, А. Шень. *Лекции по математической логике и теории алгоритмов. Начала теории множеств.* М.: МЦНМО, 1999. 128 с.

[7] А. Гейтинг. *Интуиционизм. Введение*, перевод с английского В. А. Янкова под редакцией и с комментариями А. А. Маркова. М.: Мир, 1965. 200 с.

[8] Д. Гильберт, П. Бернайс. *Основания математики. Логические исчисления и формализация арифметики*, перевод с немецкого Н. М. Нагорного под редакцией С. И. Адяна. М.: Наука, главная редакция физико-математической литературы, 1979. 560 с.

[9] С. Г. Гиндикин. *Алгебра логики в задачах.* М.: Наука, главная редакция физико-математической литературы, 1972. 288 с.

[10] А. В. Гладкий. *Математическая логика.* М.: Российский государственный гуманитарный университет, 1998. 479 с.

[11] М. Дэвис. *Прикладной нестандартный анализ*, перевод с английского С. Ф. Сопрунова под редакцией и с предисловием В. А. Успенского. М.: Мир: 1980. 236 с.

[12] Ю. Л. Ершов, Е. А. Палютин. *Математическая логика.* М.: Наука, главная редакция физико-математической литературы, 1979.

[13] Г. Кейслер, Ч. Ч. Чэн. *Теория моделей*, перевод с англ. С. С. Гончарова, С. Д. Денисова, В. А. Душского и Д. И. Свириденко. Под редакцией Ю. Л. Ершова и А. Д. Тайманова. М.: Мир, 1977. 614 с.

[14] А. Г. Курош. *Лекции по общей алгебре*, издание второе. М.: Наука, главная редакция физико-математической литературы, 1973. 399 с.

[15] С. К. Клини. *Введение в метаматематику*, перевод с английского А. С. Есенина-Вольпина под редакцией В. А. Успенского. М.: Издательство иностранной литературы, 1957. 526 с.

[16] С. К. Клини. *Математическая логика*, перевод с английского Ю. А. Гастева под редакцией Г. Е. Минца. М.: Мир, 1973. 480 с.

[17] С. Клини, Р. Весли. *Основания интуиционистской математики с точки зрения теории рекурсивных функций*, перевод с английского Ф. А. Кабакова и Б. А. Кушнера. М.: Наука, главная редакция физико-математической литературы, 1978. 272 с. (Серия: Математическая логика и основания математики.)

[18] Т. Кормен, Ч. Лейзерсон, Р. Ривест. *Алгоритмы: построение и анализ*, пер. с англ. К. Белова, Ю. Боравлёва, Д. Ботина, В. Горелика, Д. Дерягина, Ю. Калнишкана, А. Катановой, С. Львовского, А. Ромащенко, К. Сонина, К. Трушкина, М. Ушакова, А. Шеня, В. Шувалова, М. Юдашкина под редакцией А. Шеня, В. Ященко. М.: МЦНМО, 1999. 960 с.

[19] И. А. Лавров, Л. Л. Максимова. *Задачи по теории множеств, математической логике и теории алгоритмов*, издание второе. М.: Наука, 1984. 224 с.

[20] Р. Линдон. *Заметки по логике*, пер. с английского Ю. А. Гастева под редакцией И. М. Яглома. М.: Мир, 1968. 128 с.

[21] Ю. И. Манин. *Доказуемое и недоказуемое.* М.: Советское радио, 1979. 168 с.

[22] А. Робинсон. *Введение в теорию моделей и метаматематику алгебры*, пер. с англ. А. Б. Волынского под редакцией А. Д. Тайманова. М.: Наука, главная редакция физико-математической литературы, 1967. 376 с. (Серия: Математическая логика и основания математики.)

[23] Рэймонд М. Смаллиан. *Как же называется эта книга?*, пер. с англ. Ю. А. Данилова. М.: Мир, 1981. 240 с.

[24] Р. Смальян. *Теория формальных систем*, перевод с англ. Н. К. Косовского под редакцией Н. А. Шанина. М.: Наука, главная редакция физико-математической литературы, 1981. 207 с. (Серия: Математическая логика и основания математики.)

[25] *Справочная книга по математической логике в четырёх частях под ред. Дж. Барвайса. Часть II. Теория множеств*, пер. с англ. В. Г. Кановея под редакцией В. Н. Гришина. М.: Наука, 1982. 376 с.

[26] *Справочная книга по математической логике в четырёх частях под ред. Дж. Барвайса. Часть III. Теория рекурсии*, пер. с английского С. Г. Дворникова, И. А. Лаврова. Под ред. Ю. Л. Ершова. М.: Наука, 1982. 360 с.

[27] В. А. Успенский. *Что такое нестандартный анализ?* М.: Наука, главная редакция физико-математической литературы, 1987. 128 с.

[28] В. А. Успенский. *Нестандартный, или неархимедов, анализ.* М.: Знание, 1983. 61 с. (Новое в жизни, науке, технике. Математика, кибернетика, № 8.)

[29] Х. Фрейденталь. *Язык логики*, перевод с английского Ю. А. Петрова под редакцией Ю. А. Гастева. М.: Наука, главная редакция физико-математической литературы, 1969. 136 с.

[30] А. Чёрч. *Введение в математическую логику. I*, перевод с английского В. С. Чернявского под редакцией В. А. Успенского. М.: Издательство иностранной литературы, 1960. 484 с.

[31] Дж. Шенфилд. *Математическая логика*, перевод с английского И. А. Лаврова и И. А. Мальцева под редакцией Ю. Л. Ершова. М.: Наука, 1975. 528 с.

[32] Э. Энгелер. *Метаматематика элементарной математики*, перевод с немецкого Г. Е. Минца под редакцией А. О. Слисенко. М: Мир, 1987. 128 с.

[33] С. В. Яблонский. *Введение в дискретную математику*, издание второе. М.: Наука, 1986. 384 с.

[34] H. J. Keisler. *Elementary Calculus.* Weber and Schmidt, Prindle, 1976.

Предметный указатель

Указатель имён