Н. К. Верещагин

ВВЕДЕНИЕ В МАТЕМАТИЧЕСКУЮ ЛОГИКУ
Конспекты лекций для 1 курса механико-математического факультета МГУ

Москва, 2000

Оглавление

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

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

Таблица 1. Логические связки, обозначения и названия

импликации $A \Rightarrow B$ высказывание A называют *посылкой*, или *антецедентом импликации*, а B — *заключением*, или *консеквентом.*

Говорят также, что высказывание имеет *истинностное 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.

Из всех связок больше всего вопросов вызывает импликация. В самом деле, не очень понятно,

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

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 — это 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 смысла 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?

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

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 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 $((p \to q) \wedge (q \to p))$, 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.* ▷

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.

◁ 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, $(a+b)\times(c+(d\times e))$ 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.

$\triangleleft$ 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). $\triangleright$

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 число 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 *дизъ-*

юнктов. 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.

$\triangleleft$ 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 правилами де Моргана, чтобы внести отрицание внутрь. $\triangleright$

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:

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

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

$$(p \lor q) \ \leftrightarrow \ \neg(\neg p \land \neg q),$$

или только дизъюнкцией и отрицанием, так как

$$(p \land q) \ \leftrightarrow \ \neg(\neg p \lor \neg q)$$

(обе эквивалентности вытекают из законов де Моргана; их легко проверить и непосредственно). Как говорят, система связок $\land, \neg$, а также система связок $\lor, \neg$ 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 $\land, \lor, \to$ 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 $\land$ и $\lor$, 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 $\land$ и $\lor$.

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

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

(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.)

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) $(A \wedge B) \to A$;
(4) $(A \wedge B) \to B$;
(5) $A \to (B \to (A \wedge B))$;
(6) $A \to (A \vee B)$;
(7) $B \to (A \vee B)$;
(8) $(A \to C) \to ((B \to C) \to (A \vee B \to C))$;
(9) $\neg A \to (A \to B)$;
(10) $(A \to B) \to ((A \to \neg B) \to \neg A)$;
(11) $A \vee \neg A$.

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):

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

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

$\triangleleft$ 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 6 (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. $(D \to ((D \to D) \to D)) \to ((D \to (D \to D)) \to (D \to D))$
   [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 MP. (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 MP 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 MP. 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.

11. 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 $A \to B, B \to C, A \vdash \vdash C$.)

12. Докажите, что если $\Gamma_1 \vdash A$ и $\Gamma_2, A \vdash B$, то $\Gamma_1 \cup \Gamma_2 \vdash B$. (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.)

13. 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).

14. Докажите, что формула $(A \to (B \to C)) \to ((A \wedge B) \to C)$, 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 $(A \to C) \to ((B \to C) \to ((A \vee B) \to \to C))$.

15. 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 $\neg B$).

16. 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 2.2 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).

17. Докажите, что формула $(\neg B \to \neg A) \to (A \to B)$ является теоремой исчисления высказываний. (Указание: здесь также необходим закон исключённого третьего.)

18. 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.

19. 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. Интуиционистская пропозициональная логика

Исключим из числа аксиом закон исключённого третьего $A \vee \neg A$. Полученное исчисление называется *интуиционистским исчислением высказываний.*

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.

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*. Каждый символ имеет фиксированную 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 $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$ 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:

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

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

20. Как записать с помощью формулы свойство линейной упорядоченности? свойство не иметь наибольшего элемента? свойство плотности (отсутствия соседних элементов)? свойство фундированности? 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:

$$\begin{aligned}
&\forall x\,\forall y\,\forall z(((x \times y) \times z) = (x \times (y \times z))),\\
&\forall x\,(((x \times 1) = x) \land ((1 \times x) = x)),\\
&\forall x\,(((x \times \mathrm{inv}(x)) = 1) \land ((\mathrm{inv}(x) \times x) = 1)).
\end{aligned}$$

Если не хотеть включать в сигнатуру операцию взятия обратного, то последнюю аксиому придётся переписать так:

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

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

22. 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*:

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

23. Сформулировать словесно эту аксиому.

24. 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.

25. 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 $(A(x) \land \forall x\,B(x,x))$ 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.

26. Проведите это индуктивное рассуждение подробно.

27. 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 $A(x)$.)

28. 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 $M^k \to \mathbb{B} = \{\textbf{И},\textbf{Л}\}$, 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 также называют выразимыми.

29. 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.

30. 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 3.5.

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».

31. 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».

32. Запишите соответствующую формулу.

Аналогичным образом можно двигаться и дальше.

33. 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.)

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

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

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

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

38. 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. 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 7. 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.) $\rhd$

Теорема 7 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.

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

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

3.5. 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 8. Для всякой формулы рассматриваемой нами сигнатуры существует эквивалентная ей бескванторная формула.

$\triangleleft$ 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

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

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

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

с формулой

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

которую мы будет обозначать φ'. Формула φ' представляет собой дизъюнкцию формул, полученных в результате подстановки различных t_i вместо x в бескванторную формулу $\tau(x, x_1, \ldots, x_n)$. (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 $x_1, \ldots, x_n$ формула φ' истинна, то для этих значений $x_1, \ldots, x_n$ 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. ▷

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

◁ 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. ▷

41. 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, бо́льшим x». Однако при этом мы использовали кванторы, так что для $(\mathbb{Z}, =, <)$ элиминация кванторов невозможна.

42. 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).

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

Теорема 10. Всякая формула в $(\mathbb{Q}, =, <)$ эквивалентна некоторой бескванторной формуле.

◁ 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. 8). 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 $\exists x\,((x = y) \wedge A(y))$ можно заменить на $A(x)$.

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.

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.

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.

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).

43. Будет ли общезначима формула (**а**) $\forall x\, \exists y\, B(x,y) \to \exists y\, \forall x\, B(x,y)$? (**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.

44. Напишите формулы R, T, A и проверьте, что приведённая нами формула не общезначима, хотя истинна во всех конечных интерпретациях.

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.

45. 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.

46. 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 выполнить 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.

47. 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

$$A(f(y)) \land \exists x\, B(f(y), f(y)),$$

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 $(\varphi \land \psi)$, $(\varphi \lor \psi)$ 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 $A(x) \land \exists x\, B(x, x)$.

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.

48. 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: формулы

(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).

49. 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 11. 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 все наши определения вступают в игру. Пусть φ имеет вид $\forall\eta\,\psi$. Есть два принципиально разных случая: либо ξ является параметром формулы $\varphi = \forall\eta\,\psi$, 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

- 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 аксиомам. Используя их, 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 $\exists\xi\,\varphi \to \to \exists\xi\,\psi$, 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 $\varphi \to \to \psi$ 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.

- 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.

- 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 $(\neg B \to A) \to (\neg A \to B)$ 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 B, то из $\neg B$ 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.

В исчислении высказываний важную роль играло понятие выводимости из посылок и связанная с ним лемма о дедукции (с. 10). Для исчисления предикатов ситуация немного меняется. Если определить вывод из посылок по аналогии с исчислением высказываний (разрешается использовать посылки наравне с аксиомами), 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. 32 при обсуждении правила обобщения). Но импликация $A(x) \to \forall x\, A(x)$ не является выводимой (поскольку не общезначима).

Поэтому мы определим понятие выводимости из множества формул иначе. Пусть Γ — произвольное множество формул (возможно, содержащих параметры), а φ — некоторая формула (она тоже может содержать параметры). Говорят, что *из* Γ *выводится* φ, если найдётся конечное число формул $\gamma_1, \ldots, \gamma_n \in \Gamma$, для которых формула $(\gamma_1 \wedge \ldots \wedge \gamma_n) \to \varphi$ выводима в исчислении предикатов. (Для пустого Γ определение совпадает с исходным определением выводимости в исчислении предикатов; мы считаем, как обычно, что пустая конъюнкция тождественно истинна, а импликация с истинной посылкой равносильна своему заключению.)

Покажем, что это определение выводимости обладает многими свойствами, известными нам для исчисления высказываний.

- Если $\Gamma \vdash A$ и $\Gamma' \supset \Gamma$, то $\Gamma' \vdash A$. (Очевидно следует из определения.)

- Если Γ конечно и равно $\{\gamma_1, \ldots, \gamma_n\}$, то $\Gamma \vdash A$ равносильно выводимости формулы $(\gamma_1 \wedge \ldots \wedge \gamma_n) \to A$. В самом деле, разница с определением лишь в том, что в посылке формулы не обязательно использовать все элементы множества Γ. Но если выводима формула $(\gamma_1 \wedge \ldots \wedge \gamma_k) \to A$ при некотором $k < n$, то выводима и формула $(\gamma_1 \wedge \ldots \wedge \gamma_n) \to A$, поскольку связывающая эти две формулы импликация является пропозициональной тавтологией (и можно применить MP).

- Если $A \in \Gamma$, то $\Gamma \vdash A$. (В самом деле, формула $A \to A$ выводима как частный случай пропозициональной тавтологии.)

- Если $\Gamma \vdash A$ и $\Gamma \vdash (A \to B)$, то $\Gamma \vdash B$ (аналог правила MP). В самом деле, если выводимы формулы $\gamma_1 \wedge \ldots \wedge \gamma_k \to A$ и $\gamma'_1 \wedge \ldots \wedge \gamma'_l \to (A \to B)$, то выводима и формула $\gamma_1 \wedge \ldots \wedge \gamma_k \wedge \gamma'_1 \wedge \ldots \wedge \gamma'_l \to B$. (Чтобы в этом убедиться, достаточно составить подходящую пропозициональную тавтологию и дважды применить правило MP.)

- Имеет место аналог леммы о дедукции: $\Gamma, A \vdash B$ тогда и только тогда, когда $\Gamma \vdash (A \to B)$. (Напомним, что Γ, A есть сокращение для $\Gamma \cup \{A\}$.) В самом деле, если $\Gamma \vdash (A \to B)$, то и $\Gamma, A \vdash$ $\vdash (A \to B)$. Кроме того, $\Gamma, A \vdash A$, поэтому (согласно предыдущему утверждению) $\Gamma, A \vdash B$. Напротив, $\Gamma, A \vdash B$ по определению означает, что $\vdash (\gamma_1 \wedge \ldots \wedge \gamma_k \wedge A) \to B$. Но тогда и $\vdash (\gamma_1 \wedge$ $\wedge \ldots \wedge \gamma_k) \to (A \to B)$, поскольку соединяющая эти формулы импликация является частным случаем пропозициональной тавтологии.

- Правила Бернайса теперь можно переписать так:

$$\frac{\Gamma, A \vdash B}{\Gamma, A \vdash \forall\xi\, B} \qquad \frac{\Gamma, B \vdash A}{\Gamma, \exists\xi\, B \vdash A}$$

 (предполагая, что переменная ξ не является параметром формулы A, а также параметром формул из Γ). Для симметрии в первом правиле мы написали формулу A, хотя она ничем не отличается от остальных формул множества Γ. Чтобы обосновать первое правило, достаточно по лемме о дедукции перенести Γ в правую часть (получив $\vdash (\Gamma \wedge A) \to B$), применить правило Бернайса и вернуть Γ обратно. Во втором правиле нужно перейти к выводимой формуле $B \to (\neg\Gamma \vee A)$ с помощью пропозициональных тавтологий, а затем применить правило Бернайса и, наконец, вернуть Γ обратно.

- Пусть Γ — множество замкнутых формул. Присоединим их временно к аксиомам. Какие формулы станут выводимыми? Легко проверить, что все те, для которых $\Gamma \vdash \varphi$, и только они. В самом деле, если $\Gamma \vdash \varphi$, то выводима формула $\gamma \to \varphi$, где γ — конъюнкция некоторых формул из Γ. Имея формулы из Γ в качестве дополнительных аксиом, мы можем вывести γ и затем применить modus ponens.

 Обратно, пусть существует «вывод» формулы φ, в котором наряду с аксиомами используются формулы из Γ. Тогда все формулы этого «вывода» выводимы из Γ в смысле нашего определения. В самом деле, правило modus ponens, а также правила Бернайса, как мы только что видели, сохраняют выводимость из посылок (для правил Бернайса важно, что все формулы множества Γ замкнуты).

 Этот факт объясняет употребление названия «выводимость» для введённого нами понятия.

50. 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 $\Gamma \vdash \varphi$.

Теорема 12 (полнота исчисления предикатов, слабая форма). Всякая общезначимая формула выводима в исчислении предикатов.

4.5. Теории и модели

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. Назовём формулу *общезначимой в нормальных интерпретациях*, если она истинна в любой нормальной интерпретации на любой оценке. Ясно, что любая общезначимая формула общезначима в нормальных интерпретациях. Обратное неверно как показывает пример формулы $\forall x\, x = x$.

Возникает естественный вопрос. Пусть имеется некоторая формула сигнатуры, включающей равенство. Мы знаем она общезначима тогда и только тогда, когда она выводима в исчислении предикатов. В каком случае она общезначима в нормальных интерпретациях.

Чтобы ответить на этот вопрос, введём аксиомы равенства. Пусть σ — произвольная сигнатура. *Аксиомами равенства* в сигнатуре σ будут формулы

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

(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:

$$\forall x_1 \forall x_1 \forall y_1 \forall y_2\,(((x_1 = x_2) \wedge (y_1 = y_2)) \to$$
$$\to (f(x_1, y_1) = f(x_2, y_2))).$$

Для предикатных символов аксиомы равенства говорят, что истинный предикат остаётся истинным, если заменить аргументы на равные. Например, для двуместного предикатного символа A аксиома такова:

$$\forall x_1 \forall x_1 \forall y_1 \forall y_2\,(((x_1 = x_2) \wedge (y_1 = y_2) \wedge A(x_1, y_1) \to$$
$$\to A(x_2, y_2)).$$

(Нет необходимости специально говорить, что предикат остаётся ложным при замене аргументов на равные, так как равенство симметрично.) *Исчислением предикатов с равенством* называется исчисление, полученное добавлением к обычному исчислению предикатов аксиом равенства.

Теорема 13 (полноты для исчисления предикатов с равенством). Любая формула, общезначимая в нормальных интерпретациях, выводима в исчислении предикатов с равенством.

Теорема 14 (полнота исчисления предикатов, сильная форма). Любое непротиворечивое множество совместно.

Теорема 15 (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.

$\triangleleft$ 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. $\triangleright$

51. Покажите, что теорема о полноте в сильной форме является следствие 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 ...)

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 следует* 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 16.

$$\Gamma \vdash \varphi \Leftrightarrow \Gamma \vDash \varphi.$$

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.