И.С. Фролов

ЭЛЕМЕНТЫ МАТЕМАТИЧЕСКОЙ ЛОГИКИ

Самара
2001

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра алгебры и геометрии

И.С. Фролов

ЭЛЕМЕНТЫ МАТЕМАТИЧЕСКОЙ ЛОГИКИ

Учебное пособие для студентов математических специальностей

Издательство «Самарский университет»
2001

УДК 517.11
ББК 22.12
Ф 912

Фролов И.С. Элементы математической логики: Учеб. пособие для студентов математических специальностей. — Самара: Изд-во «Самарский университет», 2001. С. 80.

Учебное пособие написано на основе курса лекций, читаемого автором в течение ряда лет студентам-математикам. В нем рассматриваются основные понятия и вопросы, относящиеся к элементарным разделам математической логики: логические функции, нормальные формы, исчисление высказываний, формальные теории. Изложение сопровождается примерами и иллюстрациями вводимых понятий и применяемых методов.

Предназначено для студентов первого и второго курсов математических специальностей университетов, изучающих курсы дискретной математики и математической логики.

ББК 22.12

Рецензент канд. физ.-мат. наук, доц. В.Л. Шур

Редактор Т.И. Кузнецова

Компьютерная верстка, макет И.С. Фролов

Л.Р. № 020316 от 04.12.96. Подписано в печать 21.06.2001. Формат 60×84/16.
Бумага офсетная. Печать офсетная. Усл. печ. л. 4,65; уч.-изд.л. 5,0.
Тираж 300 экз. Заказ №
Издательство «Самарский университет».
443011 г. Самара, ул. Акад. Павлова, 1.
УОП СамГУ, ПЛД № 67-43 от 19.02.98.

Введение

1. Традиционная логика

Логикой называется наука о законах и формах мышления. Развитие логики на Востоке (Древняя Индия) и на Западе (Древняя Греция) шло различными путями. Одним из важнейших моментов в истории всей западной цивилизации было создание Аристотелем (384–322 гг. до н.э.) *формальной логики*, изучающей формы правильных рассуждений.

Математическая логика есть часть формальной логики, в которой, с одной стороны, рассматриваются формы рассуждений, принятые в математике, прежде всего доказательства, а с другой — применяются математические методы исследования. Идея построения универсального логического языка для всей математики была выдвинута немецким математиком Лейбницем (1646–1716), но систематическое развитие математической логики началось только после опубликования в 1847 г. английским математиком Джорджем Булем (1815–1864) трактата «Математический анализ логики», посвященного алгебраизации формальной логики.

Традиционная логика Аристотеля имеет дело с *понятиями*, *суждениями* и *умозаключениями*. Суждения описывают простейшие взаимоотношения между понятиями. Четыре классических типа суждений:

$$\begin{array}{llll}
A(S,P) & — & \text{общеутвердительное}: & \text{«все } S \text{ суть } P\text{»};\\
E(S,P) & — & \text{общеотрицательное}: & \text{«ни одно } S \text{ не есть } P\text{»};\\
I(S,P) & — & \text{частноутвердительное}: & \text{«некоторые } S \text{ суть } P\text{»};\\
O(S,P) & — & \text{частноотрицательное}: & \text{«некоторые } S \text{ не суть } P\text{»}
\end{array}$$

в современной символике представляются так:

$$\begin{array}{llll}
A & : \forall x(S(x) \Rightarrow P(x)), & I & : \exists x(S(x) \wedge P(x)),\\
E & : \forall x(S(x) \Rightarrow \neg P(x)), & O & : \exists x(S(x) \wedge \neg P(x)).
\end{array}$$

Формальная логика устанавливает ряд свойств суждений. Одно из таких свойств — отношение противоречия между суждениями типов A и O (а также между I и E): *суждение типа A истинно тогда и только тогда, когда суждение типа O с теми же членами ложно.* Например, из истинности суждения «Все птицы — животные» вытекает ложность суждения «Некоторые птицы — не животные».

Другим важнейшим разделом традиционной логики является учение о *силлогизмах* — элементарных умозаключениях, с помощью которых суждение с *субъектом* S и *предикатом* P (*заключение* силлогизма) выводится из двух других суждений (*посылок* силлогизма). Посылки силлогизма, помимо членов S и P, содержат еще один, средний член M. Пример:

$$\begin{array}{l} \text{Во всяком прямоугольнике диагонали равны.} \\ \text{Всякий квадрат есть прямоугольник.} \\ \hline \text{Следовательно, во всяком квадрате диагонали равны.} \end{array}$$

Этот силлогизм построен по следующей схеме, содержащей три общеутвердительных суждения:

$$\begin{array}{c} A(M,P) \\ A(S,M) \\ \hline A(S,P) \end{array} \quad .$$

В современных обозначениях ему соответствует схема вывода

$$\begin{array}{c} \forall x(M(x) \Rightarrow P(x)) \\ \forall x(S(x) \Rightarrow M(x)) \\ \hline \forall x(S(x) \Rightarrow P(x)) \end{array}$$

и даже более короткая логическая формула

$$((M \Rightarrow P) \ \wedge \ (S \Rightarrow M)) \Rightarrow (S \Rightarrow P).$$

Какие еще существуют аналогичные правила умозаключения? Возможны четыре схемы, или, как принято говорить, четыре *фигуры* силлогизма:

$$\begin{array}{cccc} \text{I} & \text{II} & \text{III} & \text{IV} \\ \cdot(M,P) & \cdot(P,M) & \cdot(M,P) & \cdot(P,M) \\ \cdot(S,M) & \cdot(S,M) & \cdot(M,S) & \cdot(M,S) \\ \hline \cdot(S,P) & \cdot(S,P) & \cdot(S,P) & \cdot(S,P) \end{array} \quad .$$

В каждой из схем вместо точек можно $4^3 = 64$ способами расставить буквы A, E, I, O. Получается 256 мыслимых правил (в традиционной терминологии — *модусов* силлогизма). Однако не все из них будут правильны, а лишь 19. Им даны следующие названия:

I фигура	II фигура	III фигура	IV фигура
Barbara	Cesare	Darapti	Bramantip
Celarent	Camestres	Disamis	Camenes
Darii	Festino	Datisi	Dimaris
Ferio	Baroco	Felapton	Fesapo
		Bocardo	Fresison
		Ferison	

Гласные буквы в этих бессмысленных, но служащих мнемонике словах указывают на выбор букв A, E, I, O. Выше уже был приведен пример силлогизма, относящегося к модусу I фигуры bArbArA. Рассмотрим еще один пример. Модус III фигуры fElAptOn имеет вид:

$$\frac{\begin{array}{c}E(M,P)\\ A(M,S)\end{array}}{O(S,P)}\quad.$$

К этому модусу относится умозаключение:

Ни один дельфин — не рыба.
Все дельфины — морские обитатели.
Следовательно, некоторые морские обитатели — не рыбы.

Формальная логика Аристотеля, маленький фрагмент которой представлен выше, оказала большое влияние на всю европейскую культуру — в течение многих веков знание ее считалось необходимым всякому образованному человеку и было одним из средств дисциплинирования ума.

2. Логические парадоксы

Новый этап в развитии логики, начавшийся с середины XIX в., был связан с возникновением абстрактного аксиоматического метода. Не менее важным явилось открытие на рубеже XIX–XX вв. парадоксов теории множеств, т.е. рассуждений, совершенно справедливых с интуитивной точки зрения, но приводящих тем не менее к противоречиям. Некоторые из них были известны еще с древности.

Парадокс лжеца — самый старый и самый известный из логических парадоксов. Легенда приписывает жившему на острове Крит в VI в. до н.э. поэту Эпимениду изречение «Все критяне — лжецы». Такое высказывание в устах критянина, конечно, странно, хотя противоречия здесь еще нет: можно просто заключить, что это предложение ложно. Но ситуация изменится, если, как заметил Эвбулид из Милета

(IV в. до н.э.), кто-либо скажет: «Предложение, которое я сейчас произношу, ложно». Из истинности этой фразы следует, что она ложна, а из ложности — что она не ложна, т.е. истинна. Это и есть парадокс лжеца.

Парадокс Рассела. Назовем множество особым, если оно является своим собственным элементом (например, множество всех множеств). Пусть R — множество всех неособых множеств. Если R — особое множество, то $R \in R$ по определению особого множества и $R \notin R$ по определению R. Если R — неособое множество, то опять $R \in R$, но на этот раз по определению R, и $R \notin R$, т.к. R не является особым. Любое из предположений: «R – особое множество», «R – неособое множество» ведет к противоречию.

Парадокс Греллинга. Некоторые прилагательные русского (или английского) языка обозначают свойство, которым они сами обладают, например, «абстрактный», «многосложный», «русский». Назовем их автологичными, а все остальные — гетерологичными (например, «французский», «односложный», «зеленый»). Тогда, если прилагательное «гетерологичный» гетерологично, то оно автологично, и наоборот.

Тщательный анализ логических парадоксов, а также способов образования математических понятий и методов математических рассуждений, предпринятый математиками в XX в., привел к появлению ветви математической логики, близкой к философии, — основания математики.

В настоящее время математическая логика имеет трудно оценимое прикладное значение, проявившееся в связи с компьютеризацией и ростом уровня технологии. На это указывают новые ее разделы — теория алгоритмов и математическая лингвистика.

§1. Логика высказываний

1. Логические связки

В логике высказываний нас интересуют утвердительные предложения, которые могут быть истинными или ложными, но не теми и другими одновременно. Каждое такое утвердительное предложение называется *высказыванием*. Примеры высказываний: «Волга впадает в Каспийское море», «Все киты суть рыбы», «5 — нечетное число».

Высказывания будем обозначать буквами $A, B, C, \ldots$, например, A : «15 делится на 3», B : «во всяком треугольнике все углы — острые».

Буквы, использующиеся для обозначения высказываний, называются логическими *атомами*. При фиксированном множестве атомов $\mathcal{A} = \{A, B, C, \ldots\}$ *интерпретацией* называется функция I, отображающая это множество в множество *истинностных (логических) значений* $\mathcal{T} = \{\texttt{истина}, \texttt{ложь}\}, \quad I : \mathcal{A} \to \mathcal{T}$.

Иными словами, интерпретация — это приписывание каждому атому истинностного значения — `истина` или `ложь`. Если атом обозначает некоторое конкретное высказывание, например, $C : 2 \times 2 = 4$, $D : 3 < 2$, то существует естественная интерпретация этих атомов: $I(C) =$, $I(D) =$.

Истинностные значения `истина`, `ложь` сокращенно обозначаются И, Л, или T, F, или 1, 0.

Из высказываний можно составлять новые, более сложные высказывания, используя *логические связки*, или *логические операции*. К числу логических связок относятся следующие.

Отрицание. $\neg A$: «не-A», «неверно, что A». Если A интерпретировано, то $\neg A$ также получит истинностное значение с помощью следующей *таблицы истинности (таблицы значений)*:

A	$\neg A$
0	1
1	0

Итак, $\neg A$ ложно, если A истинно, и $\neg A$ истинно, если A ложно.

Конъюнкция. $A \wedge B$: «A и B». Смысл этой связки очевиден: высказывание $A \wedge B$ истинно, если A и B одновременно истинны.

Дизъюнкция. $A \vee B$: «A или B». (Лат. «Vel»— соединительное «или» в отличие от «aut»— разделительного «или»). В русском языке слово «или» используется в двух значениях: соединительном и разделительном. В математической логике эти значения следует строго различать. Высказывание $A \vee B$ истинно, если A истинно, или B истинно, или и A, и B истинны одновременно.

Импликация. $A \Rightarrow B$: «если A, то B», «из A следует B», «A влечет B». Импликация $A \Rightarrow B$ истинна, когда A и B истинны, и ложна, когда A истинно, а B ложно. Но нет оснований считать импликацию ложной, если A ложно.

Например, пусть о целом числе x мы делаем высказывание: «Если x — полный квадрат, то x неотрицательно». Это истинное составное высказывание — импликация. Однако и при $x = -1$, и при $x = 5$ его первая часть «x — полный квадрат» ложна.

Поэтому высказывание $A \Rightarrow B$ считается истинным, и когда A ложно, независимо от логического значения B.

Эквиваленция. $A \Leftrightarrow B$: «A тогда и только тогда, когда B». Иными словами, высказывание $A \Leftrightarrow B$ истинно, если истинностные значения A и B совпадают.

Таблицы истинности для четырех бинарных[1] логических связок можно объединить в одну:

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Каждая строка в таблице истинности соответствует определенной интерпретации.

2. Логические формулы

Объекты, конструируемые из атомов с помощью логических связок, называются формулами логики высказываний. Определим более точно понятие логической формулы.

Определение. *Формулами* называются выражения, сконструированные из атомов A, B, C, ... и связок $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ по следующим правилам:

(1) атом есть формула;

(2) если G и H — формулы, то $(\neg G)$, $(G \wedge H)$, $(G \vee H)$, $(G \Rightarrow H)$, $(G \Leftrightarrow H)$ — формулы.

Часть формулы, которая сама является формулой, называется *подформулой* данной формулы.

Пример 1. Формула $F_1 = ((A \wedge (\neg B)) \vee C)$ имеет подформулы: $A, B, C, (\neg B), (A \wedge (\neg B))$; сама формула F_1 также считается своей подформулой.

[1] т.е. двуместных.

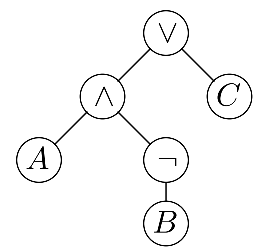
Как видно из определения, каждая формула, если это не атом, начинается и заканчивается скобкой, причем внутри формулы должен соблюдаться баланс открывающих и закрывающих скобок. Это можно проиллюстрировать на нашем примере, сопоставив каждой паре соответствующих друг другу скобок один и тот же номер:

$$\underset{1}{(}\underset{2}{(}A \wedge \underset{3}{(}\neg B\underset{3}{)}\underset{2}{)} \vee C\underset{1}{)}$$

или выделив каждую подформулу (не являющуюся атомом) подчеркиванием — от скобки до скобки:

$$\underline{(\underline{(A \wedge \underline{(\neg B)})} \vee C)}.$$

Структура формулы, ее конструкция из связок и подформул еще более явно выражена в *дереве* формулы F_1. В каждой вершине такого дерева находится логическая связка, и из нее выходит две (для бинарных связок) или одна (для отрицания) ветвь, ведущая к дереву соответствующей подформулы. В концевых вершинах (листьях дерева) находятся атомы.



Часто принимается соглашение о приоритетах логических связок:

$$\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow \quad \text{(в порядке убывания приоритета)},$$

позволяющее сократить число скобок. Мы тогда можем записать: $F_1 = A \wedge \neg B \vee C$.

При заданной интерпретации нетрудно определить истинностное значение любой формулы. Для этого можно использовать таблицы значений.

Пример 2. Построим таблицу значений для формулы $F_2 = \neg A \vee B \Rightarrow C$:

A	B	C	$\neg A$	$\neg A \vee B$	F
0	0	0	1	1	0
0	0	1	1	1	1
0	1	0	1	1	0
0	1	1	1	1	1
1	0	0	0	0	1
1	0	1	0	0	1
1	1	0	0	1	0
1	1	1	0	1	1

Другой способ вычисления логических значений состоит в следующем. Будем обозначать $|F|_I$ или просто $|F|$ значение формулы F при заданной интерпретации I. В предположении, что логические значения формул суть числа 0 или 1, легко проверить, что

$$|\neg A| = 1 - |A|,$$
$$|A \wedge B| = |A| \cdot |B| = \min(|A|, |B|),$$
$$|A \vee B| = |A| + |B| - |A| \cdot |B| = \max(|A|, |B|),$$
$$|A \Rightarrow B| = 1 - |A| + |A| \cdot |B| = \begin{cases} 1, \text{ если } |A| \leqslant |B|, \\ 0, \text{ если } |A| > |B|, \end{cases}$$
$$|A \Leftrightarrow B| = 1 - \Big||A| - |B|\Big| = \begin{cases} 1, \text{ если } |A| = |B|, \\ 0, \text{ если } |A| \neq |B|. \end{cases}$$

Пример 3. Найдем логическое значение формулы $F_3 = (A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$:
$|F_3| = 1 - \Big||A \Rightarrow B| - |\neg A \vee B|\Big| = 1 - \Big|(1 - |A| + |A| \cdot |B|) - ((1 - |A|) + |B| - (1 - |A|) \cdot |B|)\Big| = 1 - \Big|(1 - |A| + |A| \cdot |B|) - (1 - |A| + |A| \cdot |B|)\Big| = 1$,
т.е. формула F_3 всегда истинна.

Формула называется *тождественно истинной* (или *общезначимой*) формулой, если она получает значение `истина` при любой интерпретации. Другое название общезначимой формулы — *тавтология*. Общезначимость формулы G обозначается $\models G$.

Формула называется *тождественно ложной* формулой (или *противоречием*), если ее значение при любой интерпретации — `ложь`.

Пример 4. Формула $A \Rightarrow A$ является тавтологией, формула $A \wedge \neg A$ — противоречием, как показывает следующая таблица значений:

A	$A \Rightarrow A$	$A \wedge \neg A$
0	1	0
1	1	0

Формула называется *выполнимой*, если существует интерпретация, при которой она истинна (такая интерпретация называется *моделью* формулы), и *опровержимой*, если найдется интерпретация, при которой она ложна. Например, для формулы F_2 (см. пример 2) имеется пять моделей, соответствующих строкам с единицей в последней колонке — одна из них представляет собой интерпретацию $I(A, B, C) = (0, 0, 1)$; остальные: $(0, 1, 1)$, $(1, 0, 0)$, $(1, 0, 1)$, $(1, 1, 1)$.

Упражнение 1. Что является отрицанием высказываний: «Формула F общезначима», «Формула F выполнима»?

Упражнение 2. Докажите, что если формула не общезначима и не противоречива, то она выполнима и опровержима одновременно.

3. Логические эквивалентности

Необходимо знать простые примеры общезначимых формул и уметь применять их для получения других общезначимых формул.

Теорема 1. *Следующие формулы тождественно истинны:*

(1)	$A \vee B \Leftrightarrow B \vee A$	
	$A \wedge B \Leftrightarrow B \wedge A$	*(коммутативность)*
(2)	$(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$	
	$(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$	*(ассоциативность)*
(3)	$(A \vee B) \wedge C \Leftrightarrow (A \wedge C) \vee (B \wedge C)$	
	$(A \wedge B) \vee C \Leftrightarrow (A \vee C) \wedge (B \vee C)$	*(дистрибутивность)*
(4)	$\neg(A \vee B) \Leftrightarrow (\neg B \wedge \neg A)$	
	$\neg(A \wedge B) \Leftrightarrow (\neg B \vee \neg A)$	*(законы Де Мóргана)*
(5)	$\neg\neg A \Leftrightarrow A$	*(закон двойного отрицания)*
(6)	$\neg(A \wedge \neg A)$	*(закон отрицания противоречия)*
(7)	$A \vee \neg A$	*(закон исключенного третьего)*
(8)	$A \Leftrightarrow A$	*(закон тождества)*
(9)	$A \vee A \Leftrightarrow A$	
	$A \wedge A \Leftrightarrow A$	*(законы идемпотентности)*
(10)	$A \Rightarrow B \Leftrightarrow \neg A \vee B$	*(закон импликации)*
(11)	$(A \Leftrightarrow B) \Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow A)$	*(закон эквиваленции).*

$\triangleleft$ Доказательство проводится с помощью построения таблиц истинности. Например, для 1-го закона Де Моргана (4):

A	B	$A \vee B$	F_1	$\neg A$	$\neg B$	F_2	F
0	0	0	1	1	1	1	1
0	1	1	0	1	0	0	1
1	0	1	0	0	1	0	1
1	1	1	0	0	0	0	1

Обозначения F, F_1, F_2 использованы для всей формулы и ее подформул, стоящих слева и справа от символа $\Leftrightarrow$: $F_1 = \neg(A \vee B)$, $F_2 = (\neg B \wedge \neg A)$, $F = \neg(A \vee B) \Leftrightarrow (\neg B \wedge \neg A)$. $\triangleright$

Формулы F и G называются *(логически) эквивалентными*, если $\models F \Leftrightarrow G$. Будем обозначать (логическую) эквивалентность формул следующим образом: $F \sim G$. Мы уже имеем некоторый запас эквивалентных формул, с помощью которых можно производить эквивалентные преобразования, аналогичные принятым в алгебре: переставлять члены в конъюнкции и дизъюнкции, опускать скобки в выражениях вида $(A \vee B) \vee C$ и $A \wedge (B \wedge C)$, раскрывать скобки и т.д. Рассмотрим теперь средства получения новых эквивалентностей.

Теорема 2. *Если* $\models F$ *и* $\models F \Rightarrow G$, *то* $\models G$.

$\lhd$ Зафиксируем произвольную интерпретацию I. По условию $|F| = 1$ и $|F \Rightarrow G| = 1$, т.е. $|F| \leqslant |G|$. Отсюда заключаем, что $|G| = 1$. $\rhd$

Теорема 3. $F \sim G$ *тогда и только тогда, когда формулы* F *и* G *имеют одинаковые таблицы значений.*

$\lhd$ Если $F \sim G$, то при любой интерпретации I имеем $|F \Leftrightarrow G|_I = 1$, т.е. $|F|_I = |G|_I$. Справедливо и обратное. $\rhd$

Пример 5. Запишем закон импликации в виде $A \Rightarrow B \ \sim \ \neg A \vee B$. Для его доказательства, согласно теореме 3, достаточно проверить совпадение таблиц истинности формул $A \Rightarrow B$ и $F = \neg A \vee B$:

A	B	$A \Rightarrow B$	$\neg A$	F
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	1	0	1

Упражнение 3. Проверьте аналогичным образом другие логические законы.

Теорема 4. *Если* $F \sim G$ *и* $G \sim H$, *то* $F \sim H$.

$\lhd$ Действительно, в силу теоремы 3 все три формулы F, G и H должны иметь одинаковые таблицы истинности. $\rhd$

Вместе с очевидными свойствами: a) $F \sim F$, b) если $F \sim G$, то $G \sim F$, теорема 4 означает, что логическая эквивалентность определяет на множестве всех логических формул отношение эквивалентности. В частности, из теоремы 4 непосредственно вытекает *правило цепи эквивалентностей*:

$$\textit{Если } F_1 \sim F_2, F_2 \sim F_3, \ldots, F_{n-1} \sim F_n, \textit{ то } F_1 \sim F_n.$$

В данном случае обычно используют запись $F_1 \sim F_2 \sim F_3 \sim \ldots \sim F_n$ и говорят, что формула F_n получена из F_1 эквивалентными преобразованиями.

Упражнение 4. Сформулируйте и докажите правило цепи импликаций, соответствующее принятой в математике записи $F_1 \Rightarrow F_2 \Rightarrow F_3 \Rightarrow \ldots \Rightarrow F_n$. Используйте теорему 2.

Пусть F — формула, содержащая атом A. Обозначим F_H^A формулу, получаемую из F подстановкой вместо A (всякий раз, когда A встречается) формулы H, становящейся, таким образом, подформулой в F_H^A.

Теорема 5. *Если* $F \sim G$, *то* $F_H^A \sim G_H^A$ *(правило подстановки).*

$\triangleleft$ Интерпретации для формул F_H^A и G_H^A надо задавать на множестве всех атомов формул F и G, исключая, быть может, A. Какое бы значение ни получила формула H при этом, оно уже учтено в таблицах значений для формул F и G (так как таблицы значений отражают все возможные интерпретации). Поскольку эти таблицы совпадают, также совпадают таблицы значений формул F_H^A и G_H^A. $\triangleright$

Обозначим F_G формулу, в которой выделена некоторая подформула G. Очевидно, эта формула может быть получена подстановкой формулы G вместо некоторого атома. Естественно в таком случае обозначить F_H формулу, получаемую из F_G заменой выделенной подформулы G на формулу H.

Теорема 6. *Если* $G \sim H$, *то* $F_G \sim F_H$ *(правило замены).*

$\triangleleft$ В процессе построения таблицы значений для формул F_G и F_H колонки таблиц, соответствующие подформулам G и H, совпадут в силу $G \sim H$, но все дальнейшие построения в обеих таблицах совершенно идентичны. В результате мы получим совпадение колонок таблиц для формул F_G и F_H. $\triangleright$

Пример 6. $\neg A \Rightarrow B \;\sim\; \neg\neg A \vee B$ по правилу подстановки, примененному к закону импликации; $\neg\neg A \vee B \;\sim\; A \vee B$ по правилу замены, примененному к закону двойного отрицания; таким образом $\neg A \Rightarrow B \;\sim\; A \vee B$ по правилу цепи эквивалентностей.

Отметим еще ряд эквивалентностей, полезных при проведении преобразований:

(a)	$A \vee (A \wedge B) \;\sim\; A,$	$A \wedge (A \vee B) \;\sim\; A$	(правило поглощения)
(b)	$A \vee \neg A \;\sim\; 1,$	$A \wedge \neg A \;\sim\; 0,$	
(c)	$A \vee 0 \;\sim\; A,$	$A \wedge 0 \;\sim\; 0,$	
(d)	$A \vee 1 \;\sim\; 1,$	$A \wedge 1 \;\sim\; A,$	

где 1 стоит на месте тождественно истинного, а 0 — на месте тождественно ложного высказывания.

Пример 7. $A \;\sim\; A \wedge 1 \;\sim\; A \wedge (B \vee \neg B) \;\sim\; (A \wedge B) \vee (A \wedge \neg B)$.

Упражнение 5. Докажите аналогичную эквивалентность $(A \vee B) \wedge (A \vee \neg B) \;\sim$ $\sim\; A$.

Упражнение 6. Дайте обоснование правилу поглощения.

§2. Логические функции

1. Определения

Обозначим символом $\mathbb{B}$ двухэлементное множество $\{0,\ 1\}$, которое будем интерпретировать как множество логических значений: $0 =$ `ложь`, $1 =$ `истина`.

Любая функция, отображающая $\mathbb{B}^n$ в $\mathbb{B}$ $\ (n \geqslant 0)$, называется *логической функцией* от n переменных; т.е. логическая функция — это функция $f(x_1, x_2, \ldots, x_n)$ от аргументов $x_1, x_2, \ldots, x_n \in \mathbb{B}$, принимающая значения из $\mathbb{B}$. Число n называется *арностью* (или *местностью*) функции f. Множество всех логических функций от n переменных обозначим $\Lambda(n)$, множество всех логических функций от любого числа переменных — Λ. Множество $\mathbb{B}$ вместе с заданными на нем функциями из Λ иногда называется *алгеброй логики*.

Вместо двухэлементного множества $\mathbb{B}$ можно рассматривать k-элементное множество $\{0, 1, \ldots, k-1\}$ — в этом случае говорят о k-значных логических функциях и о k-значной логике.

Всякая логическая функция может быть задана таблицей значений: если функция зависит от n переменных, то в левой части этой таблицы необходимо записать 2^n различных наборов значений переменных.

Пример 1. Пусть $g(x_1, x_2, x_3)$ — функция голосования (решение принимается, если большинство из 3 голосов «за»). Построим соответствующую ей таблицу значений.

x_1	x_2	x_3	$g(x_1, x_2, x_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Наборы значений переменных, на которых функция принимает значение 1, называются *единичными наборами*, а те наборы, на которых функция принимает значение 0, — *нулевыми наборами*. В приведенном выше примере единичные наборы образуют множество $\{(0,1,1),\ \ (1,0,1),\ \ (1,1,0),\ \ (1,1,1)\}$.

Порядок перечисления наборов значений переменных в таблице значений можно зафиксировать, если рассматривать наборы как двоичные числа и располагать их порядке возрастания: 000, 001, 010, 011 и т.д. В таком случае каждая логическая функция будет задаваться одним своим столбцом, т.е. перечислением всех своих значений на упорядоченном списке наборов. Например, функция голосования будет задана в виде (0,0,0,1,0,1,1,1).

Предложение 1. $|\Lambda(n)| = 2^{2^n}$.

$\lhd$ Следует из доказанной в курсе дискретной математики теоремы о числе отображений из m-элементного множества в n-элементное, равном n^m. $\rhd$

Таким образом, имеется несколько способов представления логических функций: таблицей значений, множеством единичных наборов, перечислением значений, логической формулой.

2. Примеры логических функций

Рассмотрим логические функции от 0, 1 и 2 переменных.

a) $n = 0$, $|\Lambda(0)| = 2$. Две нульарные логические функции — это *функции-константы*: $\varphi_0 = 0$ и $\varphi_1 = 1$;

b) $n = 1$, $|\Lambda(1)| = 4$. Составим таблицу значений унарных логических функций.

x	f_0	f_1	f_2	f_3
0	0	0	1	1
1	0	1	0	1

Здесь f_0 и f_3 — функции-константы 0 и 1 соответственно; поскольку они не зависят от переменной x, эта переменная называется *несущественной*. Функция f_1 — тождественная функция: $f_1(x) = x$; функция f_2 — отрицание, для нее используют ряд обозначений: $\overline{x}$, $\neg x$, x', $\sim x$;

c) $n = 2$, $|\Lambda(2)| = 16$. Перечислим все 16 бинарных логических функций.

x_1	x_2	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
			$\wedge$	$\not\Rightarrow$		$\not\Leftarrow$		$\oplus$	$\vee$	$\downarrow$	$\Leftrightarrow$		$\Leftarrow$		$\Rightarrow$	$\mid$	

Прокомментируем таблицу. Функции f_0 и f_{15} суть константы 0 и 1. Далее,

$$f_3(x_1, x_2) = x_1,\ f_5(x_1, x_2) = x_2,\ f_{12}(x_1, x_2) = \neg x_1,\ f_{10}(x_1, x_2) = \neg x_2.$$

Остальные функции существенно зависят от обеих переменных:

$f_1(x_1, x_2)$ — *конъюнкция*, обозначается : $x_1 \cdot x_2,\ x_1 \wedge x_2,\ x_1 \,\&\, x_2$;
$f_7(x_1, x_2)$ — *дизъюнкция* : $x_1 + x_2,\ x_1 \vee x_2$;
$f_6(x_1, x_2)$ — *разделительная дизъюнкция*[1] : $x_1 \oplus x_2,\ x_1 \triangle x_2$;
$f_9(x_1, x_2)$ — *эквиваленция* : $x_1 \equiv x_2,\ x_1 \Leftrightarrow x_2$;
$f_{13}(x_1, x_2)$ — *импликация* : $x_1 \supset x_2,\ x_1 \Rightarrow x_2$;
$f_{11}(x_1, x_2)$ — обратная импликация («x_1 если x_2») : $x_1 \subset x_2,\ x_1 \Leftarrow x_2$;
$f_2(x_1, x_2)$ — коимпликация («x_1 не влечет x_2») : $x_1 \not\Rightarrow x_2$;
$f_4(x_1, x_2)$ — обратная коимпликация : $x_1 \not\Leftarrow x_2$;
$f_8(x_1, x_2)$ — *стрелка Пирса* («ни x_1, ни x_2») : $x_1 \downarrow x_2$;
$f_{14}(x_1, x_2)$ — *штрих Шеффера* («не x_1 или не x_2») : $x_1 \mid x_2$.

Упражнение 1. Как выразить $|x_1 \oplus x_2|$, $|x_1 \downarrow x_2|$, $|(x_1 \mid x_2)|$ через $|x_1|$ и $|x_2|$?

3. Функции и формулы

Для каждой из функций, рассмотренных в предыдущем пункте и существенно зависящих от всех своих переменных, мы ввели логическую связку. Рассматривая общий случай, предположим, что имеется некоторое множество связок, или функций $\Sigma = \{f_1, f_2, \ldots, f_m, \ldots\}$.

Определение. *Формулой над* Σ называется выражение, индуктивно конструируемое по следующим правилам[1] :

(1) константы 0, 1 и переменные $x_1, x_2, \ldots, x_n, \ldots$ — формулы над Σ;

(2) если $F_1, F_2, \ldots, F_n$ — формулы над Σ, а $f_i(x_1, x_2, \ldots, x_n)$ — функция от n переменных из Σ, то $F = f_i(F_1, F_2, \ldots, F_n)$ — формула над Σ.

В последнем случае $F_1, F_2, \ldots, F_n$ являются *подформулами* формулы F; кроме того, подформулы всех формул $F_1, F_2, \ldots, F_n$ являются также подформулами формулы F. Функция f_i называется *внешней операцией* формулы F. Результат применения функции $f(x_1, x_2, \ldots, x_n)$ к функциям $f_1(x_1, x_2, \ldots, x_k)$, $f_2(x_1, x_2, \ldots, x_k)$,..., $f_n(x_1, x_2, \ldots, x_k)$ называется *суперпозицией* функций f и $f_1, f_2, \ldots, f_n$.

[1] Другое название — *циклическое сложение*, или сложение по модулю 2; в программировании используется обозначение: x_1 `xor` x_2.

[1] Аналогично определению логической формулы в п.1.2.

Пример 2. Формула

$$F = f_2(\underline{f_1(\underline{x_1}, \underline{x_2})}, \underline{f_3(x_2, \underline{f_2(x_1, \underline{x_3})})})$$

имеет подформулы $f_1(x_1, x_2)$, $f_3(x_2, f_2(x_1, x_3))$, $f_2(x_1, x_3)$, x_1, x_2, x_3.

Часто вместо такой функциональной записи используется *инфиксная запись*, например, если f_1 — дизъюнкция, f_2 — циклическое сложение, f_3 — конъюнкция, то $F = (x_1 \vee x_2) \bigtriangleup (x_2 \wedge (x_1 \bigtriangleup x_3))$ или $(x_1 + x_2) \oplus (x_2 \cdot (x_1 \oplus x_3))$.

Каждая формула представляет определенную функцию, таблицу значений которой можно построить обычным образом. Однако представление функции формулой неединственно, например,

стрелку Пирса можно представить[1] через функции $+$, $\cdot$, $\neg$:

$$x_1 \downarrow x_2 = \overline{x_1 + x_2} = \overline{x}_1 \cdot \overline{x}_2;$$

штрих Шеффера — аналогично :

$$x_1 \mid x_2 = \overline{x_1 \cdot x_2} = \overline{x}_1 + \overline{x}_2;$$

отрицание, конъюнкцию и дизъюнкцию — наоборот, через $\downarrow$ или $\mid$:

$$\begin{gathered} \overline{x} = x \downarrow x = x \mid x, \\ x_1 \cdot x_2 = \overline{x}_1 \downarrow \overline{x}_2 = (x_1 \downarrow x_1) \downarrow (x_2 \downarrow x_2), \\ x_1 + x_2 = \overline{x_1 \downarrow x_2} = (x_1 \downarrow x_2) \downarrow (x_1 \downarrow x_2). \end{gathered}$$

4. Совершенная дизъюнктивная нормальная форма

Введем обозначения $x^0 = \overline{x}$, $x^1 = x$. Пусть α — параметр, равный 0 или 1. Тогда $x^\alpha = (x \Leftrightarrow \alpha)$. В частности, α^α=1.

Теорема 1. *Всякая логическая функция $f(x_1, x_2, \ldots, x_n)$ может быть представлена в виде*[2]

$$\begin{aligned} &f(x_1, \ldots, x_m, x_{m+1}, \ldots, x_n) = \\ &\qquad = \bigvee_{(\alpha_1, \ldots, \alpha_m)} x_1^{\alpha_1} \ldots x_m^{\alpha_m} f(\alpha_1, \ldots, \alpha_m, x_{m+1}, \ldots, x_n), \end{aligned} \tag{1}$$

где $m \leqslant n$, а дизъюнкция берется по всем 2^m наборам значений $(\alpha_1, \ldots, \alpha_m)$, $\alpha_i \in \mathbb{B}$.

[1] Формулы, представляющие одну и ту же функцию, мы связываем в настоящем параграфе знаком =.

[2] Далее в этом параграфе конъюнкция обозначается как умножение, а дизъюнкция как сложение.

(Это равенство называют разложением в дизъюнкцию по m первым переменным.)

$\lhd$ Покажем, что для любого набора значений переменных x_1, x_2,…, x_n значения левой и правой частей совпадают. Подставим в правую часть равенства (1) произвольный набор значений $\beta_1, \beta_2, \ldots, \beta_n$. Так как для каждого i $(1 \leqslant i \leqslant m)$ равенство $\beta_i^{\alpha_i} = 1$ выполняется только при $\alpha_i = \beta_i$, получим

$$\bigvee_{(\alpha_1,\ldots,\alpha_m)} \beta_1^{\alpha_1} \ldots \beta_m^{\alpha_m} f(\alpha_1, \ldots, \alpha_m, \beta_{m+1}, \ldots, \beta_n) =$$
$$= \beta_1^{\beta_1} \ldots \beta_m^{\beta_m} f(\beta_1, \ldots, \beta_n) = f(\beta_1, \ldots, \beta_n). \quad \rhd$$

Пример 3. При $m = 2, n = 3$ для произвольной логической функции f получим

$$f(x_1, x_2, x_3) =$$
$$= \overline{x}_1\overline{x}_2 f(0,0,x_3) + \overline{x}_1 x_2 f(0,1,x_3) + x_1\overline{x}_2 f(1,0,x_3) + x_1 x_2 f(1,1,x_3). \quad (2)$$

Упражнение 2. Примените формулу (2) к функции голосования, предварительно упростив $g(0,0,x_3)$, $g(0,1,x_3)$ и т.д.

Следствие 1. *Для любой логической функции имеет место* $f(x_1, x_2, \ldots, x_n) = \overline{x}_1 f(0, x_2, \ldots, x_n) + x_1 f(1, x_2, \ldots, x_n)$.

$\lhd$ Вытекает из теоремы 1 при $m = 1$. $\rhd$

Следствие 2. *Если функция f не совпадает с 0, то*

$$f(x_1, \ldots, x_n) = \bigvee_{f(\alpha_1,\ldots,\alpha_n)=1} x_1^{\alpha_1} \ldots x_n^{\alpha_n}, \quad (3)$$

где дизъюнкция берется по всем наборам $(\alpha_1, \ldots, \alpha_n)$, на которых значение функции f равно 1.

$\lhd$ Вытекает из теоремы 1 при $m = n$. $\rhd$

Разложение (3), в котором функция f представлена в виде дизъюнкции членов $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, называется *совершенной дизъюнктивной нормальной формой* (сокращенно *СДНФ*) функции f.

Формула, содержащая только функции дизъюнкции, конъюнкции и отрицания, называется *булевой формулой*.

Теорема 2. *Всякая логическая функция может быть представлена в виде булевой формулы (т.е. выражается через функции $\vee$, $\wedge$ и $\neg$).*

$\triangleleft$ Если функция f не равна тождественно 0, то, согласно следствию 2, она представима в виде СДНФ. Если же $f=0$, то $f = x\overline{x}$. $\triangleright$

Совершенная дизъюнктивная нормальная форма логической функции может быть получена из таблицы значений этой функции.

Для этого по каждому единичному набору запишем конъюнкцию переменных и их отрицаний по следующему правилу. Если в наборе значение переменной равно 0, то переменную возьмем с отрицанием, если равно 1, то без отрицания. Из получившихся конъюнкций построим дизъюнкцию.

Пример 4. Построим совершенную дизъюнктивную нормальную форму функции голосования. Таблица значений для нее построена в п.1. Наборы, на которых функция равна 1, — это (0,1,1), (1,0,1), (1,1,0), (1,1,1). Таким образом, СДНФ функции голосования будет иметь вид : $\overline{x}_1x_2x_3 + x_1\overline{x}_2x_3 + x_1x_2\overline{x}_3 + x_1x_2x_3$.

Упражнение 3. Найдите СДНФ функции, тождественно равной 1, т.е. $f(x_1,\ldots,x_n) = 1$.

5. Совершенная конъюнктивная нормальная форма

Во многом совершенно аналогично предыдущему определяется совершенная конъюнктивная нормальная форма.

Теорема 3. *Всякая логическая функция $f(x_1,x_2,\ldots,x_n)$ может быть представлена в виде*

$$f(x_1,\ldots,x_m,x_{m+1},\ldots,x_n) = \\ = \bigwedge_{(\alpha_1,\ldots,\alpha_m)} [\overline{x_1^{\alpha_1}} + \ldots + \overline{x_m^{\alpha_m}} + f(\alpha_1,\ldots,\alpha_m,x_{m+1},\ldots,x_n)], \qquad (4)$$

где $m \leqslant n$, а конъюнкция берется по всем 2^m наборам значений $(\alpha_1,\ldots,\alpha_m)$, $\alpha_i \in B$.

(Это равенство называют разложением в конъюнкцию по m первым переменным.)

$\triangleleft$ В правой части (4) каждый член конъюнкции представляет собой некоторую дизъюнкцию, и интерес представляют только те дизъюнкции, среди членов которых нет 1. Рассуждая аналогично доказательству теоремы 1, получим (так как равенство $\overline{\beta_i^{\alpha_i}} = 0$ выполняется только при $\alpha_i = \beta_i$) :

$$\bigwedge_{(\alpha_1,\ldots,\alpha_m)} [\overline{\beta_1^{\alpha_1}} + \ldots + \overline{\beta_m^{\alpha_m}} + f(\alpha_1,\ldots,\alpha_m,\beta_{m+1},\ldots,\beta_n)] = \\ = \overline{\beta_1^{\beta_1}} + \ldots + \overline{\beta_m^{\beta_m}} + f(\beta_1,\ldots,\beta_n) = f(\beta_1,\ldots,\beta_n). \quad \triangleright$$

Следствие 1. *Для любой логической функции имеет место* $f(x_1, x_2, \ldots, x_n) = (x_1 + f(0, x_2, \ldots, x_n))(\overline{x}_1 + f(1, x_2, \ldots, x_n))$.

Следствие 2. *Если функция f не совпадает с 1, то*

$$f(x_1, \ldots, x_n) = \bigwedge_{f(\alpha_1, \ldots, \alpha_n)=0} (\overline{x_1^{\alpha_1}} + \ldots + \overline{x_n^{\alpha_n}}), \tag{5}$$

где конъюнкция берется по всем наборам $(\alpha_1, \ldots, \alpha_n)$, на которых значение функции f равно 0.

Правая часть формулы (5), в которой функция f представлена в виде разложения в конъюнкцию по всем переменным, называется *совершенной конъюнктивной нормальной формой* (сокращенно *СКНФ*) функции f.

Совершенная конъюнктивная нормальная форма логической функции также может быть получена из таблицы значений этой функции.

Для этого по каждому нулевому набору запишем дизъюнкцию переменных и их отрицаний по следующему правилу. Если в наборе значение переменной равно 0, то переменную возьмем без отрицания, если равно 1, то с отрицанием. Из получившихся дизъюнкций построим конъюнкцию.

Пример 5. Вернемся к функции голосования (см. примеры 1 и 4). Наборы, на которых функция равна 0, — это (0,0,0), (0,0,1), (0,1,0), (1,0,0). В соответствии с правилом, СКНФ будет иметь вид : $(x_1 + x_2 + x_3)(x_1 + x_2 + \overline{x}_3)(x_1 + \overline{x}_2 + x_3)(\overline{x}_1 + x_2 + x_3)$.

Упражнение 4. Найдите СКНФ функции, тождественно равной 0, т.е. $f(x_1, \ldots, x_n) = 0$.

§3. Нормальные формы

1. Дизъюнктивная нормальная форма

Вновь обратимся к формулам логики высказываний для изучения, помимо совершенных дизъюнктивных и конъюнктивных нормальных форм, аналогичных, но более компактных видов представления логических функций.

Определение 1. *Литералом* называется атом или отрицание атома (т.е. A, $\neg B$, $\ldots$). *Конъюнктом* (или *элементарной конъюнкцией*) называется формула вида $L_1 \wedge \ldots \wedge L_n \quad (n \geqslant 1)$, где $L_1, \ldots, L_n$ — литералы (например, $A \wedge B$, $\neg A \wedge B \wedge \neg C$, $\neg B \wedge C$).

Говорят, что формула находится в *дизъюнктивной нормальной форме* (сокращенно *ДНФ*), если она имеет вид $K_1 \vee \ldots \vee K_m \quad (m \geqslant 1)$, где $K_1, \ldots, K_m$ — конъюнкты (например, $(A \wedge B) \vee (\neg A \wedge B \wedge \neg C) \vee$ $\vee (\neg B \wedge C)$).

Теорема 1. *Любая формула эквивалентна некоторой формуле в дизъюнктивной нормальной форме.*

$\triangleleft$ Пусть дана некоторая формула. Будем проводить эквивалентные преобразования в определенном порядке. Прежде всего, мы всегда можем

1) устранить двойные отрицания (с помощью закона двойного отрицания), т.е. заменить каждую часть формулы, имеющую вид $\neg \ldots \neg F$, где F — произвольная формула, с помощью эквивалентности:

$$\underbrace{\neg \ldots \neg}_{n} F \sim \begin{cases} F & \text{если } n \text{ четно,} \\ \neg F & \text{если } n \text{ нечетно;} \end{cases}$$

2) устранить все знаки, отличные от пяти стандартных логических связок $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$, т.е. $|$, $\downarrow$, $\oplus$, $\ldots$ и т.д. с помощью эквивалентностей:

$$A \mid B \sim \neg(A \wedge B), \quad A \downarrow B \sim \neg(A \vee B), \quad A \oplus B \sim \neg(A \Leftrightarrow B);$$

3) устранить все знаки эквиваленции и импликации (с помощью закона эквиваленции и закона импликации) — для удобства приведем их здесь вместе с некоторыми следствиями:

$$A \Rightarrow B \sim \neg A \vee B, \quad \neg(A \Rightarrow B) \sim A \wedge \neg B,$$
$$A \Leftrightarrow B \sim (A \Rightarrow B) \wedge (B \Rightarrow A) \sim$$
$$\sim (A \wedge B) \vee (\neg A \wedge \neg B) \sim (A \vee \neg B) \wedge (\neg A \vee B)$$

(заметим, что последние две формулы являются, соответственно, совершенной дизъюнктивной и совершенной конъюнктивной нормальными формами эквиваленции);

4) ввести знаки отрицания внутрь скобок (по законам Де Моргана):

$$\neg(A \vee B) \ \sim\ \neg B \wedge \neg A, \quad \neg(A \wedge B) \ \sim\ \neg B \vee \neg A,$$

причем продолжать их применение до тех пор, пока все отрицания не окажутся стоящими непосредственно перед атомами.

При проведении преобразований типа 2)–4) вновь может возникнуть необходимость неоднократного применения устранения двойного отрицания. В результате получится формула, составленная из литералов, соединенных знаками дизъюнкции и конъюнкции. Теперь нам остается

5) раскрыть скобки по закону дистрибутивности:

$$(A \vee B) \wedge C \ \sim\ (A \wedge C) \vee (B \wedge C).$$

Это преобразование напоминает процедуру перемножения многочленов в элементарной алгебре, если число членов дизъюнкции равно двум или более, например: $(A \vee B) \wedge (C \vee D) \ \sim\ (A \wedge C) \vee (B \wedge C) \vee$ $\vee (A \wedge D) \vee (B \wedge D)$.

В конце концов получится формула, представляющая собой дизъюнкцию элементарных конъюнкций. $\triangleright$

При приведении формул к ДНФ полезно иметь в виду, что из двух одинаковых членов в конъюнкции или в дизъюнкции один можно вычеркнуть (в силу законов идемпотентности $A \wedge A \ \sim\ A$, $A \vee A \ \sim\ A$). Кроме того, можно воспользоваться правилами поглощения и правилами оперирования с константами (см. эквивалентности (a)–(d) в конце § 1). Это позволяет упростить ДНФ и, в частности, избежать конъюнктов, содержащих литералы вида A и $\neg A$ (такие литералы называются *контрарными*).

Пример 1. $\neg(A \Leftrightarrow (A \Rightarrow B)) \ \sim\ \neg(A \Leftrightarrow (\neg A \vee B)) \ \sim\ \neg((A \vee$ $\vee \neg(\neg A \vee B)) \wedge (\neg A \vee \neg A \vee B)) \ \sim\ (\neg A \wedge \neg\neg(\neg A \vee B)) \vee (A \wedge A \wedge \neg B) \ \sim$ $\sim\ (\neg A \wedge (\neg A \vee B)) \vee (A \wedge \neg B) \ \sim\ \neg A \vee (A \wedge \neg B)$.

Заметим, что некоторые члены дизъюнкции могут оказаться не конъюнктами, а просто литералами: будем считать их в таком случае конъюнктами из одного литерала. Кроме того, вместо дизъюнкции конъюнктов может получиться один конъюнкт, и в этой ситуации мы будем говорить о дизъюнкции из одного конъюнкта.

При наличии в ДНФ контрарных литералов бывает полезно правила дистрибутивности и поглощения применять в обратном направлении.

Например, продолжая преобразование ДНФ из примера 1, мы можем получить более простое выражение: $\neg A \vee (A \wedge \neg B) \sim$ $\sim (\neg A \vee (\neg A \wedge \neg B)) \vee (A \wedge \neg B) \sim \neg A \vee ((\neg A \vee A) \wedge \neg B) \sim \neg A \vee \neg B$.

Другой пример:

$$(\neg A \wedge \neg B) \vee (A \wedge \neg B) \sim (\neg A \vee A) \wedge \neg B \sim 1 \wedge \neg B \sim \neg B.$$

Вот тот случай, о котором мы говорили: ДНФ состоит из одного конъюнкта, в котором имеется лишь один литерал.

Очевидно, что представление в виде ДНФ не единственно, в отличие от СДНФ. Различные дизъюнктивные нормальные формы отличаются одна от другой по числу конъюнктов, числу литералов в конъюнктах, общему числу связок и т.д.

Упражнение 1. Найдите различные ДНФ для функции голосования, определенной в § 2.

2. Конъюнктивная нормальная форма

Определение 2. *Дизъюнктом* (или *элементарной дизъюнкцией*) называется формула вида $L_1 \vee \ldots \vee L_n \quad (n \geqslant 1)$, где $L_1, \ldots, L_n$ — литералы (например, $A \vee \neg B$, $B \vee \neg C \vee \neg A$).

Говорят, что формула находится в *конъюнктивной нормальной форме* (сокращенно *КНФ*), если она имеет вид $D_1 \wedge \ldots \wedge D_m \quad (m \geqslant 1)$, где $D_1, \ldots, D_m$ — дизъюнкты (например, $(A \vee \neg B) \wedge (B \vee \neg C \vee \neg A)$).

Теорема 2. *Любая формула эквивалентна некоторой формуле в конъюнктивной нормальной форме.*

$\triangleleft$ Процесс приведения к конъюнктивной нормальной форме аналогичен рассмотренному в теореме 1 — следует лишь использовать другой закон дистрибутивности

$$(A \wedge B) \vee C \sim (A \vee C) \wedge (B \vee C). \triangleright$$

Пример 2. $\neg(A \Leftrightarrow (B \Rightarrow C)) \sim$
$\sim \neg((A \wedge (B \Rightarrow C)) \vee (\neg A \wedge \neg(B \Rightarrow C))) \sim$
$\sim (\neg A \vee \neg(B \Rightarrow C)) \wedge (A \vee (B \Rightarrow C)) \sim$
$\sim (\neg A \vee (B \wedge \neg C)) \wedge (A \vee \neg B \vee C) \sim$
$\sim (\neg A \vee B) \wedge (\neg A \vee \neg C) \wedge (A \vee \neg B \vee C)$.

Рассмотрим другой способ получения КНФ.

Предложение 1. *Пусть F — формула, составленная из литералов с применением $\wedge$ и $\vee$. Пусть F' — формула, полученная из F заменой $\wedge$ на $\vee$, $\vee$ на $\wedge$ и каждого литерала на контрарный ему (т.е. A на $\neg A$ и наоборот). Тогда $F' \sim \neg F$.*

$\lhd$ Достаточно проследить за применением к $\neg F$ преобразований вида 1) и 4) из доказательства теоремы 1. $\rhd$

Теорема 3. *Если F — дизъюнктивная нормальная форма формулы G, то F' — конъюнктивная нормальная форма формулы $\neg G$.*

$\lhd$ Очевидно, что из $F \sim G$ следует $\neg F \sim \neg G$. Тогда в силу предложения 1 $F' \sim \neg G$. Если при этом F находится в ДНФ, то F' окажется в КНФ. $\rhd$

Из теоремы 3 вытекает следующее правило: чтобы получить КНФ некоторой формулы, найдем ДНФ отрицания этой формулы, а затем совершим преобразование, описанное в предложении 1.

Пример 3. Найдем КНФ формулы $A \Rightarrow B \wedge C$. Имеем $\neg(A \Rightarrow B \wedge C) \sim A \wedge \neg(B \wedge C) \sim A \wedge (\neg B \vee \neg C) \sim (A \wedge \neg B) \vee (A \wedge \neg C)$.

Таким образом, КНФ исходной формулы: $(\neg A \vee B) \wedge (\neg A \vee C)$.

Иногда ДНФ и КНФ могут совпадать, в этом случае отыскание одной из этих форм сразу приводит и к другой. Например, в п.1 мы, преобразовывая формулу $\neg(A \Leftrightarrow (A \Rightarrow B))$, нашли одну из ее ДНФ $\neg A \vee \neg B$ (дизъюнкция двух конъюнктов, каждый из которых состоит из одного литерала), одновременно являющуюся и КНФ (конъюнкция одного дизъюнкта, состоящего из двух литералов).

Упражнение 2. Найдите различные КНФ для функции голосования.

3. Приведение нормальных форм к совершенным нормальным формам

Совершенная ДНФ может быть получена из ДНФ, а совершенная КНФ — из КНФ путем добавления в конъюнкты (дизъюнкты) недостающих атомов с помощью эквивалентностей

$$A \sim A \wedge (B \vee \neg B), \quad A \sim A \vee (B \wedge \neg B).$$

Пример 4. $A \vee (\neg A \wedge B)$ (в первом члене дизъюнкции отсутствует атом B)
$\sim (A \wedge (B \vee \neg B)) \vee (\neg A \wedge B) \sim (A \wedge B) \vee (A \wedge \neg B) \vee (\neg A \wedge B)$.

Пример 5. $A \wedge B$ (Будьте внимательны — это не СКНФ!)
$\sim (A \vee (B \wedge \neg B)) \wedge (B \vee (A \wedge \neg A)) \sim$

$\sim\ (A \vee B) \wedge (A \vee \neg B) \wedge (B \vee A) \wedge (B \vee \neg A)\ \sim$
$\sim\ (A \vee B) \wedge (A \vee \neg B) \wedge (\neg A \vee B)$.

Упражнение 3. Что можно сказать относительно формулы $A \wedge B$ — находится ли она в ДНФ, КНФ, СДНФ? Почему это не СКНФ?

4. Логическое следование

Рассмотрим приложения совершенных нормальных форм к понятию логического следования.

Пусть $F_1, \ldots, F_n$, G — логические формулы. Будем говорить, что G *логически следует* из $F_1, \ldots, F_n$, если в любой интерпретации, при которой истинны все формулы $F_1, \ldots, F_n$, формула G также истинна. Для логического следования будем использовать обозначение $F_1, \ldots, F_n \models G$. Это согласуется с обозначением $\models G$, которое мы приняли для тождественно истинной формулы. Формулы $F_1, \ldots, F_n$ называются *посылками* следствия G.

Всегда можно проверить, является ли G следствием из $F_1, \ldots, F_n$, составив общую таблицу значений.

Пример 6. Проверим, что $A \Rightarrow B,\ A \Rightarrow C \models A \Rightarrow B \wedge C$:

				F_1	F_2	G
A	B	C	$B \wedge C$	$A \Rightarrow B$	$A \Rightarrow C$	$A \Rightarrow B \wedge C$
0	0	0	0	1	1	1
0	0	1	0	1	1	1
0	1	0	0	1	1	1
0	1	1	1	1	1	1
1	0	0	0	0	0	0
1	0	1	0	0	1	0
1	1	0	0	1	0	0
1	1	1	1	1	1	1

Действительно, во всех строках, в которых на пересечении со столбцами, соответствующими F_1 и F_2, стоят 1 (первые четыре строки и последняя строка), на пересечении с последним столбцом тоже стоит 1.

Теорема 4. *Логическое следование $F_1, \ldots, F_n \models G$ имеет место тогда и только тогда, когда $\models F_1 \wedge \ldots \wedge F_n \Rightarrow G$.*

$\triangleleft$ Согласно определению, $F_1, \ldots, F_n \models G$ означает, что для каждой интерпретации I имеет место следующее:

$$\text{если } |F_1| = \ldots = |F_n| = 1, \text{ то } |G| = 1.$$

Это можно записать как $|F_1|, \ldots, |F_n| \leqslant |G|$, или $|F_1 \wedge \ldots \wedge F_n| \leqslant |G|$, что равносильно общезначимости формулы $F_1 \wedge \ldots \wedge F_n \Rightarrow G$. $\triangleright$

Еще один способ проверки логического следования заключается в рассуждении от противного.

Теорема 5. *$F_1, \ldots, F_n \models G$ тогда и только тогда, когда формула $F_1 \wedge \ldots \wedge F_n \wedge \neg G$ тождественно ложна.*

$\triangleleft$ Действительно, $\neg(F_1 \wedge \ldots \wedge F_n \wedge \neg G) \sim \neg(F_1 \wedge \ldots \wedge F_n) \vee G \sim$ $\sim F_1 \wedge \ldots \wedge F_n \Rightarrow G$. $\triangleright$

Пример 7. Проверим логическое следование

$$A \Rightarrow (B \Rightarrow C),\ \neg A \Rightarrow \neg D \models B \wedge D \Rightarrow C.$$

Предположим, что конъюнкция формул $A \Rightarrow (B \Rightarrow C)$, $\neg A \Rightarrow \neg D$ и отрицания формулы $B \wedge D \Rightarrow C$ выполнима. Тогда должно быть $|A \Rightarrow (B \Rightarrow C)| = 1$, $|\neg A \Rightarrow \neg D| = 1$ и $|B \wedge D \Rightarrow C| = 0$. Из последнего равенства заключаем, что $|C| = 0$, $|B| = |D| = 1$, а из первого равенства (поскольку теперь ясно, что $|B \Rightarrow C| = 0$) следует $|A| = 0$. Подставляя найденные значения во второе равенство, получим противоречие: $|\neg A \Rightarrow \neg D| = 0$.

Теорема 6. *$F \sim G$ тогда и только тогда, когда $F \models G$ и $G \models F$.*

$\triangleleft$ Вытекает из закона эквивалентности. $\triangleright$

Логическое следование допускает ясное описание с помощью совершенных нормальных форм.

Теорема 7. *Если F и G — формулы в СДНФ от одних и тех же переменных, то $F \models G$ тогда и только тогда, когда множество дизъюнктивных членов F содержится в множестве дизъюнктивных членов G.*

$\triangleleft$ Согласно следствию 2 из теоремы 1 § 2, каждый дизъюнктивный член в СДНФ соответствует некоторому единичному набору для F. По определению логического следования, каждый единичный набор для F должен быть единичным набором и для G. Отсюда вытекает заключение теоремы. $\triangleright$

Теорема 8. *Если F и G — формулы в СКНФ от одних и тех же переменных, то $F \models G$ тогда и только тогда, когда множество конъюнктивных членов F содержит множество конъюнктивных членов G.*

$\triangleleft$ Согласно следствию 2 из теоремы 3 § 2, каждый конъюнктивный член в СКНФ соответствует некоторому нулевому набору для F. Из определения логического следования можно заключить, что каждый нулевой набор для G должен быть нулевым набором и для F. Но это равносильно тому, что множество конъюнктивных членов G содержится в множестве конъюнктивных членов F. $\triangleright$

Пример 8. Найдем все логические следствия формулы $A \Rightarrow B \wedge C$. По таблице значений (см. пример 6) составим СКНФ :

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

Отсюда заключаем, что логическими следствиями данной формулы являются отдельные конъюнктивные члены[1]:

$$\neg A \vee B \vee C \;\sim\; A \Rightarrow B \vee C, \neg A \vee B \vee \neg C \;\sim\; A \wedge C \Rightarrow B,$$
$$\neg A \vee \neg B \vee C \;\sim\; A \wedge B \Rightarrow C,$$

а также их попарные конъюнкции[2]:

$$\neg A \vee B \;\sim\; A \Rightarrow B, \neg A \vee C \;\sim\; A \Rightarrow C,$$
$$\neg A \vee ((B \vee \neg C) \wedge (\neg B \vee C)) \;\sim\; A \Rightarrow (B \Leftrightarrow C).$$

В полный перечень логических следствий входят также исходная формула и тождественно истинная формула.

§4. Функциональная полнота и замкнутость

1. Функционально полные системы функций

Существует два существенно различных способа задания логических функций — табличный и формульный. Таблица задает непосредственное соответствие между значениями аргумента и функции. Формула — более компактный способ задания функции, однако он задает функцию через другие функции.

Пусть Σ — некоторая система логических функций, $\Sigma \subset \Lambda$ (Λ — множество всех логических функций). Нас будут интересовать следующие два вопроса: *Всякая ли логическая функция может быть представлена формулой над* Σ ? И если нет, то *какие логические функции могут быть представлены формулами над* Σ ?

[1] С помощью эквивалентностей записываем их в виде импликаций.

[2] Записанные сразу в упрощенном виде.

Определение 1. *Замыканием* системы функций Σ называется множество всех логических функций, представимых формулами над Σ.

Замыкание Σ обозначается $[\Sigma]$.

Пример 1. Если $\Sigma = \Lambda$, то $[\Sigma] = \Lambda$.

Для $\Sigma = \{1, \oplus\}$ замыканием служит множество $[\Sigma] = \{c_0 \oplus \oplus\ x_{i_1} \oplus x_{i_2} \oplus \ldots \oplus x_{i_k} |\ 1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n,\ c_0 = 0 \text{ или } 1\} = = \{f(x_1, x_2, \ldots, x_n)\ |\ f(x_1, x_2, \ldots, x_n) = c_0 \oplus c_1x_1 \oplus c_2x_2 \oplus \ldots \oplus c_nx_n,$ где $c_i \in \{0,\ 1\}\ \}$.

Функции из $[\Sigma]$ в последнем примере называются *линейными* функциями. Обоснованием такого названия служит то обстоятельство, что операция $\oplus$ является сложением по модулю 2, а сами функции действительно линейны в арифметике вычетов по модулю 2.

Упражнение 1. Докажите свойства замыкания:
1) $\Sigma \subset [\Sigma]$; 2) $[[\Sigma]] = [\Sigma]$;
3) если $\Sigma_1 \subset \Sigma_2$, то $[\Sigma_1] \subset [\Sigma_2]$;
4) $[\Sigma_1] \cup [\Sigma_2] \subset [\Sigma_1 \cup \Sigma_2]$.

Определение 2. Система функций Σ называется *функционально полной*, если $[\Sigma] = \Lambda$, т.е. если любая логическая функция представима формулой над Σ.

Иными словами, система функций $\{f_1, f_2, \ldots\}$ полна (слово «функционально» часто опускается), если любая логическая функция является результатом суперпозиций функций этой системы.

Полная система функций Σ называется *(функциональным) базисом*, если никакое собственное подмножество $\Sigma_1 \subset \Sigma,\ \Sigma_1 \neq \Sigma$ не является полной системой.

Пример 2. $\Sigma_{(1)} = \Lambda$ — полная система (это тривиальный факт).

$\Sigma_{(2)} = \{\neg, \wedge, \vee\}$ — полная система (ввиду существования для каждой логической функции ДНФ или КНФ).

Следующее утверждение позволит нам расширить круг полных систем.

Теорема 1. *Если Σ' — функционально полная система и все функции из Σ' представимы формулами над системой Σ, то Σ также функционально полна.*

$\triangleleft$ Пусть h — произвольная логическая функция. По предположению, она представима формулой над Σ'. Запишем это следующим образом: $h = F[f_1, f_2, \ldots]$, $(f_i \in \Sigma')$. В силу другого условия $f_i = = G_i[g_1, g_2, \ldots]$, $(g_i \in \Sigma)$ для любого $f_i \in \Sigma'$. Подставляя эти выражения в формулу F, получим

$$h = F[G_1[g_1, g_2, \ldots], G_2[g_1, g_2, \ldots], \ldots] = H[g_1, g_2, \ldots],$$

т.е. h представима формулой над Σ. $\triangleright$

Пример 3. Рассмотрим еще несколько полных систем.

$\Sigma_{(3)} = \{\neg, \wedge\}$, так как функции из полной системы $\Sigma_{(2)}$ представимы формулами над $\Sigma_{(3)}$: $x_1 \vee x_2 = \overline{\overline{x}_1 \wedge \overline{x}_2}$.

$\Sigma_{(4)} = \{|\}$, так как $\overline{x} = x|x$, $x_1 \wedge x_2 = \overline{x_1|x_2} = (x_1|x_2)|(x_1|x_2)$.

$\Sigma_{(5)} = \{1, \wedge, \oplus\}$, так как $\overline{x} = x \oplus 1$.

Упражнение 2. Проверить, что системы функций $\Sigma_{(3)}$–$\Sigma_{(5)}$ являются базисами, а $\Sigma_{(1)}$, $\Sigma_{(2)}$ — нет.

2. Многочлены Жегалкина

Остановимся подробнее на базисе $\Sigma_{(5)}$. Выпишем ряд эквивалентностей (конъюнкцию будем обозначать как умножение):

$$\begin{aligned} &x_1 \oplus x_2 = x_2 \oplus x_1, && x \oplus x = 0, \\ &x_1 \oplus (x_2 \oplus x_3) = (x_1 \oplus x_2) \oplus x_3, && x \oplus 0 = x, \\ &x_1(x_2 \oplus x_3) = x_1x_2 \oplus x_1x_3, && x \oplus 1 = \overline{x}. \end{aligned} \tag{1}$$

Эти тождества легко проверяются с помощью таблиц значений или применением эквивалентных преобразований, если использовать СДНФ для $x_1 \oplus x_2 = \overline{x}_1x_2 \vee x_1\overline{x}_2$.

Упражнение 3. Произведите проверку тождеств (1) указанными способами.

Определение 3. *Многочленом Жегалкина* от n переменных $x_1, \ldots, x_n$ называется формула вида

$$c_0 \oplus \bigoplus_{i_1, i_2, \ldots, i_s} c_{i_1, i_2, \ldots, i_s} x_{i_1} x_{i_2} \ldots x_{i_s}, \tag{2}$$

где $c_0,\ c_{i_1,i_2,\ldots,i_s} \in \{0, 1\}$, а суммирование ведется по всем различным строго возрастающим наборам индексов: $1 \leqslant i_1 < i_2 < \ldots < i_s \leqslant n$ $(1 \leqslant s \leqslant n)$.

Менее формально можно сказать, что многочлен Жегалкина имеет вид $K_1 \oplus K_2 \oplus \ldots \oplus K_m$, где K_i — конъюнкция неповторяемых переменных или 1 $(1 \leqslant i \leqslant m)$.

Пример 4. 1, $\overline{x} = 1 \oplus x$, $x_1 \Leftrightarrow x_2 = 1 \oplus x_1 \oplus x_2$ (проверьте!), и вообще все линейные функции представлены в форме многочлена Жегалкина; $x_1 \oplus x_1x_2 \oplus x_2x_3$ — многочлен Жегалкина нелинейной функции.

В выражении (2) зафиксирован порядок, в котором записываются одночлены и в каждом одночлене переменные. Желая подчеркнуть это, будем говорить, что многочлен Жегалкина (2) имеет стандартный вид.

Теорема 2. *Каждая логическая функция может быть единственным образом представлена в виде многочлена Жегалкина стандартного вида.*

$\triangleleft$ Так как система функций $\Sigma_{(5)}$ полна, то любую логическую функцию можно представить формулой над $\{1, \wedge, \oplus\}$. Далее, в силу коммутативности и ассоциативности $\wedge, \oplus$ и дистрибутивности $\wedge$ относительно $\oplus$, эту формулу можно преобразовать к виду (2).

Для доказательства единственности покажем, что число всех логических функций от n аргументов и число многочленов Жегалкина с n аргументами совпадают между собой. Во-первых, $|\Lambda(n)| = 2^{2^n}$ (предложение 1 § 2). С другой стороны, число возможных циклических слагаемых в выражении (2) равно количеству подмножеств $\{i_1, \ldots, i_s\}$ из n чисел $\{1, \ldots, n\}$, включая пустое подмножество $\varnothing$, которому соответствует первое слагаемое. Поскольку каждый коэффициент $c_{i_1,\ldots,i_s}$ равен 0 или 1, искомое число многочленов Жегалкина равно 2^{2^n}. $\triangleright$

Существует ряд способов построения многочлена Жегалкина для заданной логической функции.

Пример 5. Найдем многочлен Жегалкина для $x_1 \vee x_2$ методом неопределенных коэффициентов. Запишем

$$x_1 \vee x_2 = \alpha_0 \oplus \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \alpha_3 x_1 x_2,$$

где $\alpha_i \in \{0, 1\}$ $(0 \leqslant i \leqslant 3)$ — неопределенные коэффициенты.

При $x_1 = x_2 = 0$ имеем $x_1 \vee x_2 = 0 = \alpha_0$. При $x_1 = 0,\ x_2 = 1$ имеем $x_1 \vee x_2 = 1 = \alpha_0 \oplus \alpha_2$, т.е. $\alpha_2 = 1$. При $x_1 = 1,\ x_2 = 0$ имеем $x_1 \vee x_2 = 1 = \alpha_0 \oplus \alpha_1$, т.е. $\alpha_1 = 1$. При $x_1 = x_2 = 1$ имеем $x_1 \vee x_2 = 1 = \alpha_0 \oplus \alpha_1 \oplus \alpha_2 \oplus \alpha_3$, откуда $\alpha_3 = 1$.

В результате получаем

$$x_1 \vee x_2 = x_1 \oplus x_2 \oplus x_1 x_2.$$

Пример 6. Используем предыдущий пример, чтобы найти многочлен Жегалкина для импликации: $x_1 \Rightarrow x_2 = \overline{x}_1 \vee x_2 = \overline{x}_1 \oplus x_2 \oplus \overline{x}_1 x_2 = (x_1 \oplus 1) \oplus x_2 \oplus (x_1 \oplus 1) x_2 = x_1 \oplus 1 \oplus x_2 \oplus x_1 x_2 \oplus x_2 = 1 \oplus x_1 \oplus x_1 x_2$ (так как два одинаковых циклических слагаемых взаимно уничтожаются).

Пример 7. Поскольку при $xy = 0$ справедливо $x \vee y = x \oplus y$, то для совершенной дизъюнктивной нормальной формы имеет место $K_1 \vee K_2 \vee \ldots \vee K_n = K_1 \oplus K_2 \oplus \ldots \oplus K_n$. Применим это замечание к $x_1 x_2 x_3 \vee \overline{x}_1 \overline{x}_2 x_3 \vee \overline{x}_1 x_2 \overline{x}_3 = x_1 x_2 x_3 \oplus \overline{x}_1 \overline{x}_2 x_3 \oplus \overline{x}_1 x_2 \overline{x}_3 = x_1 x_2 x_3 \oplus (x_1 \oplus 1)(x_2 \oplus 1) x_3 \oplus (x_1 \oplus 1) x_2 (x_3 \oplus 1) = x_1 x_2 x_3 \oplus x_1 x_2 \oplus x_1 x_3 \oplus x_2 \oplus x_3$ (проверьте!).

3. Двойственность

Определение 4. Логическая функция

$$f^*(x_1, \ldots, x_n) = \neg f(\overline{x}_1, \ldots, \overline{x}_n)$$

называется *двойственной* функцией к функции $f(x_1, \ldots, x_n)$.

Очевидно, что таблица значений для двойственной функции f^* получается из таблицы значений функции f инвертированием (т.е. заменой 0 на 1 и 1 на 0) столбца функции и его переворачиванием, или же только инвертированием, но всех столбцов — и функции, и аргументов.

x_1	x_2	x_3	$f(x_1, x_2, x_3)$	$f^*(x_1, x_2, x_3)$
0	0	0	1	0
0	0	1	1	0
0	1	0	0	1
0	1	1	1	1
1	0	0	0	0
1	0	1	0	1
1	1	0	1	0
1	1	1	1	0

Двойственность обладает свойством взаимности.

Предложение 1. *Функция f является двойственной к f^*, т.е. $f^{**} = f$.*

Упражнение 4. Докажите предложение 1.

Пример 8. $\vee^* = \wedge$, $\wedge^* = \vee$; $0^* = 1$, $1^* = 0$; $\oplus^* = \Leftrightarrow$, $\Leftrightarrow^* = \oplus$.

Если $f^* = f$, то функция f называется *самодвойственной*. Такова, например, функция $\neg = \neg^*$.

Теорема 3. *Если $F(x_1, \ldots, x_n) = f(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$, то $F^*(x_1, \ldots, x_n) = f^*(f_1^*(x_1, \ldots, x_n), \ldots, f_m^*(x_1, \ldots, x_n))$.*

$\triangleleft$ Имеем равенства

$$\begin{aligned}
&F^*(x_1, \ldots, x_n) = \neg F(\overline{x}_1, \ldots, \overline{x}_n) = \\
&= \neg f(f_1(\overline{x}_1, \ldots, \overline{x}_n), \ldots, f_m(\overline{x}_1, \ldots, \overline{x}_n)) = \\
&= \neg f(\neg\neg f_1(\overline{x}_1, \ldots, \overline{x}_n), \ldots, \neg\neg f_m(\overline{x}_1, \ldots, \overline{x}_n)) = \\
&\qquad = \neg f(\neg f_1^*(x_1, \ldots, x_n), \ldots, \neg f_m^*(x_1, \ldots, x_n)) = \\
&\qquad = f^*(f_1^*(x_1, \ldots, x_n), \ldots, f_m^*(x_1, \ldots, x_n)). \quad \triangleright
\end{aligned}$$

Следствие 1. *Если функция $f(x_1, \ldots, x_n)$ представлена формулой F над $\{\neg, \wedge, \vee\}$, то для получения двойственной формулы F^*, представляющей функцию $f^*(x_1, \ldots, x_n)$, нужно в формуле F всюду заменить $\wedge$ на $\vee$ и $\vee$ на $\wedge$.*

Пример 9. Двойственной к $f(x_1, x_2) = (x_1 \wedge x_2) \vee \overline{x}_1$ является $f^*(x_1, x_2) = (x_1 \vee x_2) \wedge \overline{x}_1$.

Следствие 2. *Если формулы F и G представляют одну и ту же логическую функцию: $F = G$, то $F^* = G^*$.*

Объединение этих двух следствий, называемое *принципом двойственности*, позволяет почти вдвое сокращать усилия на вывод логических тождеств.

Пример 10. Отметим несколько пар двойственных тождеств:

1) $\neg(x_1 \wedge x_2) = \overline{x}_1 \vee \overline{x}_2$ и $\neg(x_1 \vee x_2) = \overline{x}_1 \wedge \overline{x}_2$;
2) $x_1 \vee (x_1 \wedge x_2) = x_1$ и $x_1 \wedge (x_1 \vee x_2) = x_1$;
3) $\overline{x} = (x \oplus 1)$ и $\overline{x} = (x \Leftrightarrow 0)$.

4. Замкнутые классы

Определение 5. Множество Σ логических функций называется *(функционально) замкнутым классом*, если $[\Sigma] = \Sigma$.

Пример 11. $\Sigma = \Lambda$ является замкнутым классом, в то время как $\Sigma = \{1, \oplus\}$ — незамкнутый класс.

Замыкание $[\Sigma]$ любого множества Σ логических функций является замкнутым классом.

Рассмотрим важнейшие замкнутые классы.

T_0 — класс всех логических функций, сохраняющих константу 0, т.е. функций $f(x_1, \ldots, x_n)$, для которых выполнено равенство $f(0, \ldots, 0) = 0$. Классу T_0 принадлежат функции 0, x, $x_1 \wedge x_2$, $x_1 \vee x_2$, $x_1 \oplus x_2$, и не принадлежат функции 1, $\overline{x}$. Таблицы значений функций класса T_0 характеризуются тем, что в первой строке они содержат 0. Число всех функций этого класса равно $|T_0| = \frac{1}{2} \cdot 2^{2^n}$. Класс T_0 замкнут, поскольку если $f, f_1, \ldots, f_m \in T_0$, то $F = f(f_1, \ldots, f_m) \in T_0$:

$$F(0, \ldots, 0) = f(f_1(0, \ldots, 0), \ldots, f_m(0, \ldots, 0)) = f(0, \ldots, 0) = 0.$$

T_1 — класс всех логических функций, сохраняющих константу 1, т.е. функций $f(x_1, \ldots, x_n)$, для которых выполнено равенство $f(1, \ldots, 1) = 1$. Классу T_1 принадлежат функции 1, x, $x_1 \wedge x_2$, $x_1 \vee x_2$, $x_1 \Leftrightarrow x_2$, и не принадлежат функции 0, $\overline{x}$. Таблицы значений функций класса T_1 характеризуются тем, что в последней строке они содержат 1. Класс T_1 состоит из функций, двойственных функциям из T_0. Отсюда сразу можно сделать вывод о замкнутости класса T_1.

L — класс всех линейных функций. Ему принадлежат константы 0, 1, тождественная функция x, функции $\overline{x}$, $x_1 \oplus x_2$ и не принадлежат функции $x_1 \wedge x_2$ и $x_1 \vee x_2$. Класс L замкнут, так как является замыканием системы функций $\{1, \oplus\}$.

S — класс всех самодвойственных функций, т.е. функций $f \in \Lambda$, удовлетворяющих условию $f^* = f$. Мы уже рассматривали такие функции в п.3. Примерами самодвойственных функций могут служить x, $\overline{x}$, а также функция голосования.

Упражнение 5. Докажите, что функция голосования, определенная в п.1 § 2: $g(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$, является самодвойственной.

На противоположных наборах $(\alpha_1, \ldots, \alpha_n)$ и $(\overline{\alpha}_1, \ldots, \overline{\alpha}_n)$ самодвойственная функция принимает противоположные значения. Отсюда следует, что самодвойственная функция полностью определяется первой половиной строк таблицы значений (или же, наоборот, второй). Поэтому число самодвойственных функций от n переменных равно $2^{2^{n-1}} = \sqrt{2^{2^n}}$. Замкнутость класса S следует из теоремы 3.

M — класс всех монотонных функций, т.е. функций $f \in \Lambda$, удовлетворяющих условию

$$\alpha_1 \leqslant \beta_1, \ldots, \alpha_n \leqslant \beta_n \Rightarrow f(\alpha_1, \ldots, \alpha_n) \leqslant f(\beta_1, \ldots, \beta_n).$$

Монотонными функциями, очевидно, являются $0,\ 1,\ x,\ x_1 \wedge x_2,\ x_1 \vee x_2$ и не являются $\overline{x},\ x_1 \oplus x_2$.

Для доказательства замкнутости класса M покажем, что если f, $f_1, \ldots, f_m \in M$, то $F = f(f_1, \ldots, f_m) \in M$. Пусть $\alpha_i \leqslant \beta_i \quad (1 \leqslant i \leqslant n)$. Тогда $f_i(\alpha_1, \ldots, \alpha_n) \leqslant f_i(\beta_1, \ldots, \beta_n) \quad (1 \leqslant i \leqslant n)$ и

$$\begin{aligned} F(\alpha_1, \ldots, \alpha_n) = f(f_1(\alpha_1, \ldots, \alpha_n), \ldots, f_m(\alpha_1, \ldots, \alpha_n)) \leqslant \\ \leqslant f(f_1(\beta_1, \ldots, \beta_n), \ldots, f_m(\beta_1, \ldots, \beta_n)) = F(\beta_1, \ldots, \beta_n). \end{aligned}$$

Замкнутые классы T_0, T_1, S, M, L попарно различны, что видно из следующей таблицы, в которой знак «+» означает принадлежность функции, стоящей в первой колонке, указанному классу, а знак «−» — противоположную ситуацию.

	T_0	T_1	S	M	L
0	+	−	−	+	+
1	−	+	−	+	+
$\neg$	−	−	+	−	+

5. Теорема о функциональной полноте

Теорема 4. *Для того чтобы система логических функций Σ была функционально полной, необходимо и достаточно, чтобы она целиком не содержалась ни в одном из пяти замкнутых классов T_0, T_1, S, M и L.*

Иными словами, критерием функциональной полноты системы функций является наличие в ней:

1) функции, не сохраняющей 0;
2) функции, не сохраняющей 1;
3) несамодвойственной функции;
4) немонотонной функции;
5) нелинейной функции.

Доказательство основывается на следующих трех леммах.

Лемма 1. *Если f — несамодвойственная функция, то из нее путем подстановки функций x и $\overline{x}$ можно получить константу.*

$\triangleleft$ Так как $f \notin S$, то найдется набор $(\alpha_1, \ldots, \alpha_n)$ такой, что $f(\overline{\alpha}_1, \ldots, \overline{\alpha}_n) = f(\alpha_1, \ldots, \alpha_n)$. Подставим в f на место i-го аргумента функцию $f_i(x) = x^{\alpha_i}$ $(1 \leqslant i \leqslant n)$: $F(x) = f(x^{\alpha_1}, \ldots, x^{\alpha_n})$. Эта функция — константа, так как

$$F(0) = f(0^{\alpha_1}, \ldots, 0^{\alpha_n}) = f(\overline{\alpha}_1, \ldots, \overline{\alpha}_n) = \\ = f(\alpha_1, \ldots, \alpha_n) = f(1^{\alpha_1}, \ldots, 1^{\alpha_n}) = F(1). \quad \triangleright$$

Лемма 2. *Если f — немонотонная функция, то из нее путем подстановки констант 0 и 1 и тождественной функции x можно получить функцию $\overline{x}$.*

$\triangleleft$ Пусть $f \notin M$. Тогда найдутся наборы $(\alpha_1, \ldots, \alpha_n) < (\beta_1, \ldots, \beta_n)$[1] такие, что $f(\alpha_1, \ldots, \alpha_n) = 1 > f(\beta_1, \ldots, \beta_n) = 0$. Построим цепочку наборов

$$(\alpha_1, \ldots, \alpha_n) = (\alpha_1^0, \ldots, \alpha_n^0) < (\alpha_1^1, \ldots, \alpha_n^1) < \ldots \\ \ldots < (\alpha_1^k, \ldots, \alpha_n^k) = (\beta_1, \ldots, \beta_n),$$

в которой каждая пара соседних наборов различается только в одной компоненте. Очевидно, найдется такая пара соседних наборов, для которых $f(\alpha_1^i, \ldots, \alpha_n^i) = 1$, $f(\alpha_1^{i+1}, \ldots, \alpha_n^{i+1}) = 0$, причем отличие заключено лишь в компоненте j:

[1] Это означает, что $\alpha_1 \leqslant \beta_1, \ldots, \alpha_n \leqslant \beta_n$, и хотя бы в одном случае неравенство строгое.

$$\alpha_1^i = \alpha_1^{i+1}, \ldots, \alpha_{j-1}^i = \alpha_{j-1}^{i+1}, \alpha_j^i = 0 < \alpha_j^{i+1} = 1,$$
$$\alpha_{j+1}^i = \alpha_{j+1}^{i+1}, \ldots, \alpha_n^i = \alpha_n^{i+1}.$$

Положим $F(x) = f(\alpha_1^i, \ldots, \alpha_{j-1}^i, x, \alpha_{j+1}^i, \ldots, \alpha_n^i)$. Тогда $F(0) = f(\alpha_1^i, \ldots, \alpha_n^i) = 1$, $F(1) = f(\alpha_1^{i+1}, \ldots, \alpha_n^{i+1}) = 0$, т.е. $F(x) = \overline{x}$. $\triangleright$

Лемма 3. *Если f — нелинейная функция, то из нее путем подстановки констант 0 и 1 и функций вида x и $\overline{x}$, а также, быть может, путем применения к ней $\neg$ можно получить функцию $x_1 \wedge x_2$.*

$\triangleleft$ Пусть $f \notin L$. Если представить f в форме многочлена Жегалкина, то в нем непременно найдется циклическое слагаемое вида $x_{i_1}x_{i_2}\ldots x_{i_k}$ $(k \geqslant 2)$. Без ограничения общности можно считать, что $i_1 = 1, i_2 = 2$. Положим $x = x_1, y = x_2$ и представим функцию f в виде $xyf_1(x_3, \ldots, x_n) \oplus xf_2(x_3, \ldots, x_n) \oplus yf_3(x_3, \ldots, x_n) \oplus f_4(x_3, \ldots, x_n)$, причем $f_1 \not\equiv 0$. Выберем $\alpha_3, \ldots, \alpha_n$ так, чтобы $f_1(\alpha_3, \ldots, \alpha_n) = 1$. Рассмотрим функцию $h(x, y) = f(x, y, \alpha_3, \ldots, \alpha_n) = xy \oplus \alpha x \oplus \beta y \oplus \gamma$, где $\alpha, \beta, \gamma \in \{0, 1\}$. В зависимости от значений α, β и γ возможны 8 случаев:

α	β	γ	$h(x,y)$	Эквив.булева ф-ла	Реализация $x \wedge y$
0	0	0	xy	$x \wedge y$	$x \wedge y = h(x,y)$
0	0	1	$xy \oplus 1$	$\neg(x \wedge y)$	$x \wedge y = \neg h(x,y)$
0	1	0	$xy \oplus y$	$\neg x \wedge y$	$x \wedge y = h(\neg x, y)$
0	1	1	$xy \oplus y \oplus 1$	$x \vee \neg y$	$x \wedge y = \neg h(\neg x, y)$
1	0	0	$xy \oplus x$	$x \wedge \neg y$	$x \wedge y = h(x, \neg y)$
1	0	1	$xy \oplus x \oplus 1$	$\neg x \vee y$	$x \wedge y = \neg h(x, \neg y)$
1	1	0	$xy \oplus x \oplus y$	$x \vee y$	$x \wedge y = \neg h(\neg x, \neg y)$
1	1	1	$xy \oplus x \oplus y \oplus 1$	$\neg(x \vee y)$	$x \wedge y = h(\neg x, \neg y)$

В каждом случае можно получить функцию $x \wedge y$. $\triangleright$

Доказательство теоремы.

$\triangleleft$ Необходимость. Пусть система Σ функционально полна. Тогда $[\Sigma] = \Lambda$, но если бы Σ содержалась в одном из указанных замкнутых классов (обозначим его Σ_0), то в силу свойств замыкания $[\Sigma] \subset [\Sigma_0] = \Sigma_0 \neq \Lambda$.

Достаточность. Пусть система Σ целиком не содержится ни в одном из пяти указанных замкнутых классов. Тогда в Σ найдется функция f_1, не сохраняющая 0, функция f_2, не сохраняющая 1, несамодвойственная функция f_3, немонотонная функция f_4, нелинейная функция f_5. Без ограничения общности можно считать, что все эти функции зависят от одних и тех же переменных $x_1, \ldots, x_n$.

Докажем, что из этих функций можно получить константы 0 и 1, отрицание и конъюнкцию.

I. Построим константы.

Рассмотрим функцию $\varphi(x) = f_1(x, \ldots, x)$. Поскольку f_1 не сохраняет 0, $\varphi(0) = f_1(0, \ldots, 0) = 1$. Если $\varphi(1) = 1$, то $\varphi(x)$ есть константа 1, а так как f_2 не сохраняет 1, то $f_2(1, \ldots, 1) = 0$ и $\psi(x) = f_2(\varphi(x), \ldots, \varphi(x))$ есть константа 0.

Если же $\varphi(1) = 0$, то $\varphi(x) = \overline{x}$. Так как теперь $\overline{x}$ находится в нашем распоряжении, в силу леммы 1 из несамодвойственной функции f_3 можно получить константу, а затем также с помощью $\overline{x}$ и другую константу.

II. Построим при помощи констант 0, 1 и немонотонной функции f_4 функцию $\overline{x}$, используя лемму 2.

III. Построим при помощи констант 0, 1, функции $\overline{x}$ и нелинейной функции f_5 функцию $x_1 \wedge x_2$, используя лемму 3.

Таким образом, мы реализовали функции $\overline{x}$ и $x_1 \wedge x_2$ при помощи формул над Σ. Но $\{\neg, \wedge\}$ — полная система, следовательно, и система Σ полна. ▹

Пример 12. Система $\{1, 0, m, \wedge\}$, где функция m задана формулой $m(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$, функционально полна. Действительно, имеем: $1 \notin T_0, 0 \notin T_1, 0 \notin S, m \notin M, \wedge \notin L$. Удаление любой из функций приводит к неполной системе, так как $\{0, m, \wedge\} \subset T_1$, $\{1, m, \wedge\} \subset T_0$, $\{1, 0, \wedge\} \subset M$, $\{1, 0, m\} \subset L$.

Упражнение 6. Покажите, что $\{d\}$, где $d(x_1, x_2, x_3, x_4) = \overline{x}_1\overline{x}_4 \vee x_2\overline{x}_3$, — полная система. Проверьте выполнение условий критерия полноты и выразите основные логические связки через функцию d.

§5. Исчисление высказываний

1. Аксиомы и правила вывода

Исчисление, или *формальная теория*, строится следующим образом:

1) определяется множество *формул*, или *правильно построенных выражений*, образующее *язык* теории;

2) выделяется подмножество формул, называемых *аксиомами* теории;

3) задаются *правила вывода* теории. Правило вывода — это отношение $R(F_1, F_2, \ldots, F_n, G)$ на множестве формул. Говорят, что формула G *непосредственно выводима* из формул $F_1, F_2, \ldots, F_n$ по правилу R. Часто правило вывода обозначается $\frac{F_1, F_2, \ldots, F_n}{G}$. Формулы $F_1, F_2, \ldots, F_n$ называются *посылками*, а G — *следствием*, или *заключением*.

Исчисление высказываний включает в себя множество логических формул, построенных с помощью атомов $P, Q, R, \ldots$ и логических связок $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$. Множество аксиом определяется следующими схемами:

1) $A \Rightarrow (B \Rightarrow A)$;
2) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$;
3) $A \wedge B \Rightarrow A$;
4) $A \wedge B \Rightarrow B$;
5) $A \Rightarrow (B \Rightarrow (A \wedge B))$;
6) $A \Rightarrow (A \vee B)$;
7) $B \Rightarrow (A \vee B)$;
8) $(A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \vee B \Rightarrow C))$;
9) $(A \Rightarrow B) \Rightarrow ((A \Rightarrow \neg B) \Rightarrow \neg A)$;
10) $\neg\neg A \Rightarrow A$;
11) $(A \Rightarrow B) \Rightarrow ((B \Rightarrow A) \Rightarrow (A \Leftrightarrow B))$;
12) $(A \Leftrightarrow B) \Rightarrow (A \Rightarrow B)$;
13) $(A \Leftrightarrow B) \Rightarrow (B \Rightarrow A)$.

Эти тринадцать формул называются схемами аксиом, потому что аксиомы получаются из них подстановкой вместо букв A, B, C конкретных формул.

В качестве единственного правила вывода принимаем правило

$$\frac{A, A \Rightarrow B}{B} \qquad \text{(MP — modus ponens, или \textit{правило отделения})}.$$

Пример 1. Аксиомами, получаемыми из схемы 1, т.е. из $A \Rightarrow (B \Rightarrow A)$, являются: $P \Rightarrow (P \Rightarrow P)$, $P \Rightarrow ((Q \Rightarrow R) \Rightarrow P)$, $Q \Rightarrow (P \Rightarrow Q)$, $\neg P \Rightarrow (P \wedge Q \Rightarrow \neg P)$ и т.д.

Согласно правилу отделения, из формул $P \wedge Q$, $P \wedge Q \Rightarrow P$ непосредственно выводима формула P.

2. Выводимость

Определение 1. *(Формальным) выводом* формулы B из списка формул $\Gamma = \{A_1, A_2, \ldots, A_n\}$ называется последовательность $B_1, B_2, \ldots, B_m$, в которой каждая формула B_i $(1 \leqslant i \leqslant m)$ является:

– либо одной из формул списка Γ,

– либо одной из аксиом,

– либо получена по правилу МР из двух формул, расположенных в этой последовательности раньше нее;

последняя формула B_m совпадает с B.

Говорят, что формула B *выводима* из $\Gamma = \{A_1, A_2, \ldots, A_n\}$, если существует вывод формулы B из списка Γ. Для выводимости используют обозначение $A_1, A_2, \ldots, A_n \vdash B$ или $\Gamma \vdash B$. Формулы A_i из списка Γ называются *гипотезами*, или *допущениями* вывода. Выражение $\Gamma \vdash B$ называется *секвенцией*. Последовательность гипотез в списке не играет роли, поэтому мы будем обращаться с Γ как с множеством, хотя для удобства будем ссылаться на порядковые номера гипотез и опускать фигурные скобки при перечислении гипотез.

Пример 2. Покажем, что $P \Rightarrow (Q \Rightarrow R)$, $P \wedge Q \vdash R$. Будем строить вывод, нумеруя последовательные шаги вывода и объясняя их.

1.	$P \wedge Q$	(гипотеза 2).
2.	$P \wedge Q \Rightarrow P$	(аксиома 3).
3.	P	(МР, 1, 2).
4.	$P \Rightarrow (Q \Rightarrow R)$	(гипотеза 1).
5.	$Q \Rightarrow R$	(МР, 3, 4).
6.	$P \wedge Q \Rightarrow Q$	(аксиома 4).
7.	Q	(МР, 1, 6).
8.	R	(МР, 7, 5).

Определение 2. *(Формальным) доказательством* формулы B называется вывод этой формулы из пустого списка формул, т.е. последовательность формул $B_1, B_2, \ldots, B_m$, в которой каждая формула

B_i $(1 \leqslant i \leqslant m)$ — либо аксиома, либо получается из предыдущих формул последовательности по правилу MP.

Формула B называется *доказуемой* формулой, или *теоремой*, если существует ее доказательство; этот факт обозначается $\vdash B$.

Пример 3. Построим доказательство для $A \Rightarrow A$.

1. $A \Rightarrow ((A \Rightarrow A) \Rightarrow A)$ (аксиома 1).
2. $(A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$(акс.2).
3. $(A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)$ (MP, 1, 2).
4. $A \Rightarrow (A \Rightarrow A)$ (аксиома 1).
5. $A \Rightarrow A$ (MP, 4, 3).

Теорема 1. *$\vdash A \Rightarrow A$ для любой формулы A.*

$\triangleleft$ Действительно, в приведенном выше выводе A может быть заменена на любую формулу. $\triangleright$

Сделаем несколько замечаний.

I. Выводы и доказательства в формальной теории проводятся не на языке этой теории, а на так называемом *метаязыке*: если символами формальной теории являются атомы P, Q, R, связки $\Rightarrow, \neg, \wedge, \vee$, и т.д., то в метаязыке используются *метапеременные* A, B, C, обозначающие произвольную формулу, Γ, Δ, обозначающие списки формул, символ $\vdash$, обозначающий выводимость и т.д. Термин «теорема» (а также «доказательство», «вывод» и т.д.) имеет двоякое значение: в формальной теории это — доказуемая логическая формула, при изучении формальной теории это — утверждение об объектах формальной теории, формулируемое и обосновываемое на метаязыке.

II. В определенном нами исчислении высказываний имеется бесконечное число аксиом, получаемых путем подстановок различных формул в конечное множество схем аксиом.

Иногда задают другие множества аксиом: например, считают, что в языке исчисления имеются только связки $\Rightarrow, \neg, \wedge, \vee$, и удаляют последние три схемы аксиом. Если же вновь потребуется связка $\Leftrightarrow$, то запись $A \Leftrightarrow B$ обычно вводят как сокращение для формулы $(A \Rightarrow B) \wedge (B \Rightarrow A)$.

III. Следует различать запись $\models A$ («формула A общезначима», т.е. истинна при любой интерпретации входящих в нее атомов — это проверяется с помощью таблиц истинности или проведением эквивалентных преобразований) и $\vdash A$ («формула A доказуема»— это можно проверить, только построив доказательство). Интересен вопрос: как связаны между собой отношения общезначимости и доказуемости на множестве всех логических формул?

Отметим некоторые свойства понятия выводимости.

Теорема 2. *Пусть A, B — произвольные формулы, Γ, Δ — множества формул. Тогда*

1) если $A \in \Gamma$, то $\Gamma \vdash A$ (рефлексивность);

2) если $\Gamma \subset \Delta$ и $\Gamma \vdash A$, то $\Delta \vdash A$ (утончение);

3) если $\Gamma \vdash A_i$ для всех $A_i \in \Delta$ и $\Delta \vdash B$, то $\Gamma \vdash B$ (транзитивность).

$\triangleleft$ Свойство 1) означает, что $A_1, \ldots, A_n \ \vdash \ A_i \quad (1 \leqslant i \leqslant n)$, что, очевидно, верно.

Далее, 2) означает, что можно добавить к списку гипотез совершенно произвольные формулы. Вывод при этом останется прежним, просто новые гипотезы в нем не будут участвовать.

Транзитивность доказывается реконструкцией выводов. В выводе B из списка гипотез Δ: $B_1, B_2, \ldots, B_m\ (= B)$ содержатся аксиомы, гипотезы $A_i \in \Delta$ и формулы, полученные по правилу MP. Заменим в нем гипотезы A_i на их вывод из Γ, т.е. вместо $B_1, \ldots, A_i, \ldots, B_m$ запишем $B_1, \ldots, \underbrace{A_{1i}, \ldots, A_{ki}(= A_i)}_{A_i \quad \Gamma}, \ldots, B_m(= B)$, в результате построим вывод B из Γ. $\triangleright$

Теорема 3. *Если* $\Gamma \ \vdash \ A \Rightarrow B$, *то* $\Gamma, A \ \vdash \ B$.

$\triangleleft$ Пусть $C_1, \ldots, C_m(= (A \Rightarrow B)\ )$ — вывод из Γ. Добавим к нему еще два шага вывода:

1.	C_1	
$\vdots$	$\vdots$	
m.	$A \Rightarrow B$	
m+1.	A	(гипотеза)
m+2.	B	(MP, m+1, m)

В результате мы построили требуемый вывод. $\triangleright$

В качестве следствия получаем, что если $\vdash \ A \Rightarrow B$, то $A \vdash B$.

Пример 4. Покажем, что $A,\ B,\ A \Rightarrow (B \Rightarrow C) \ \vdash \ C$. Согласно теореме 2(1), $A \Rightarrow (B \Rightarrow C) \ \vdash \ A \Rightarrow (B \Rightarrow C)$. Применим теорему 3: $A \Rightarrow (B \Rightarrow C),\ A \ \vdash \ B \Rightarrow C$; еще раз: $A \Rightarrow (B \Rightarrow C),\ A,\ B \vdash \ C$.

Упражнение 1. Постройте вывод непосредственно, не обращаясь к теоремам 2 и 3.

3. Теорема дедукции

Утверждение теоремы 3 допускает обращение, которое дает хорошо известный метод рассуждения: «Чтобы установить импликацию $A \Rightarrow B$, введем допущение A и докажем B».

Теорема 4. *Если* $\Gamma, A \ \vdash \ B$, *то* $\Gamma \ \vdash \ A \Rightarrow B$.

$\triangleleft$ Пусть $B_1, \ldots, B_n(= \ B)$ — вывод B из $\Gamma \cup \{A\}$. Построим вывод $A \Rightarrow B$ из Γ. Таким выводом была бы последовательность $A \Rightarrow B_1, \ldots, A \Rightarrow B_n$, но каждую формулу $A \Rightarrow B_i$ нужно еще вывести.

Построим выводы формул $A \Rightarrow B_i\ \ (1 \leqslant i \leqslant n)$ индукцией по i.

I. Пусть $i = 1$. Формула B_1 — либо аксиома, либо принадлежит Γ, либо совпадает с A.

Если B_1 — аксиома, то цепочка B_1, $B_1 \Rightarrow (A \Rightarrow B_1)$, $A \Rightarrow B_1$ является нужным выводом.

Если $B_1 \in \Gamma$, вывод такой же, как в предыдущем случае.

Если $B_1 = A$, необходимый вывод формулы $A \Rightarrow A$ можно взять из примера 3.

II. Пусть построены цепочки выводов

$$\ldots, A \Rightarrow B_1; \ldots; \ldots, A \Rightarrow B_{i-1} \quad (i > 1).$$

Построим вывод формулы $A \Rightarrow B_i$. Проведем и здесь анализ случаев. Возможны четыре случая: формула B_i — либо аксиома, либо принадлежит Γ, либо совпадает с A, либо непосредственно выводится по правилу MP из формул, предшествующих ей в исходном выводе. Первые три случая совершенно аналогичны случаям, разобранным выше, а четвертый необходимо рассмотреть отдельно.

Пусть B_i получается применением правила MP к формулам B_j и B_k $(j, k < i)$, причем B_k имеет вид $B_j \Rightarrow B_i$. По предположению индукции, уже имеются выводы из Γ формул $A \Rightarrow B_j$ и $A \Rightarrow (B_j \Rightarrow B_i)$. Искомая цепочка теперь строится так:

$$\begin{array}{ll}
(A \Rightarrow (B_j \Rightarrow B_i)) \Rightarrow ((A \Rightarrow B_j) \Rightarrow (A \Rightarrow B_i)) & \text{(аксиома 2).}\\
(A \Rightarrow B_j) \Rightarrow (A \Rightarrow B_i) & \text{(MP).}\\
A \Rightarrow B_i & \text{(MP).}
\end{array}$$

Таким образом, существует вывод

$$\ldots, A \Rightarrow B_1, \ldots, A \Rightarrow B_i, \ldots, A \Rightarrow B. \quad \triangleright$$

Пример 5. Имеем $A \Rightarrow (B \Rightarrow C), B, A \vdash C$. Построим вывод для $A \Rightarrow (B \Rightarrow C), B \vdash A \Rightarrow C$.

1. B (гип.2)	$1'$. $B \Rightarrow (A \Rightarrow B)$	(акс.1).
	$2'$. B	(гип.2).
	$3'$. $A \Rightarrow B$	(MP,$2'$,$3'$).
2. A (гип.3)	$4'$. …	5 шагов вывода $A \Rightarrow A$.
	…	
	$8'$. $A \Rightarrow A$	
3. $A \Rightarrow (B \Rightarrow C)$	$9'$. $(A \Rightarrow (B \Rightarrow C)) \Rightarrow (A \Rightarrow (A \Rightarrow (B \Rightarrow C)))$	(акс.1).
(гип.1)	$10'$. $A \Rightarrow (B \Rightarrow C)$	(гип.1).
	$11'$. $A \Rightarrow (A \Rightarrow (B \Rightarrow C))$	(MP,$2'$,$3'$).
4. $B \Rightarrow C$	$12'$. …	эти шаги необязательны,
(MP,2,3)	$13'$. …	т.к. $14'$ совп. с гип.1.
	$14'$. $A \Rightarrow (B \Rightarrow C)$	
5. C (MP,1,4)	$15'$. $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$	(акс.2).
	$16'$. $(A \Rightarrow B) \Rightarrow (A \Rightarrow C)$	(MP,$14'$,$15'$).
	$17'$. $A \Rightarrow C$	(MP,$3'$,$16'$).

Пользуясь теоремой дедукции, можно сразу без проведенного выше громоздкого построения вывода из $A \Rightarrow (B \Rightarrow C), B, A \vdash C$ заключить о выводимости $A \Rightarrow (B \Rightarrow C), B \vdash A \Rightarrow C$.

Заметим, что, применяя теорему дедукции еще раз, мы получим $A \Rightarrow (B \Rightarrow C) \vdash B \Rightarrow (A \Rightarrow C)$ (*правило перестановки посылок*).

Пример 6. Докажем *правило контрапозиции*: $A \Rightarrow B \vdash \vdash \neg B \Rightarrow \neg A$. Согласно теореме дедукции, для этого достаточно построить вывод $A \Rightarrow B, \neg B \vdash \neg A$:

1.	$\neg B$	(гипотеза 2).
2.	$\neg B \Rightarrow (A \Rightarrow \neg B)$	(аксиома 1).
3.	$A \Rightarrow \neg B$	(MP, 1, 2).
4.	$A \Rightarrow B$	(гипотеза 1).
5.	$(A \Rightarrow B) \Rightarrow ((A \Rightarrow \neg B) \Rightarrow \neg A)$	(аксиома 9).
6.	$(A \Rightarrow \neg B) \Rightarrow \neg A$	(MP, 4, 5).
7.	$\neg A$	(MP, 3, 6).

Упражнение 2. Постройте полный вывод правила контрапозиции аналогично примеру 5, пользуясь конструкциями из доказательства теоремы дедукции.

§6. Полнота и непротиворечивость

1. Непротиворечивость и корректность

Мы рассмотрели один пример формальной теории — исчисление высказываний. Наша цель теперь — показать, что доказуемость ($\vdash A$) и общезначимость ($\models A$) равносильны. Тогда мы будем уверены, что два метода — вывод и таблицы истинности — в исчислении высказываний всегда приводят к одним и тем же результатам.

Пусть S — некоторое свойство формул. Говорят, что формальная теория *корректна* (или *непротиворечива*) относительно свойства S, если все теоремы теории обладают свойством S; формальная теория *полна* относительно свойства S, если все формулы теории, обладающие свойством S, суть теоремы. Обычно корректность и полнота рассматриваются относительно свойства общезначимости (тождественной истинности). В этом случае свойство корректности формулируется так: если $\vdash A$, то $\models A$, а свойство полноты — если $\models A$, то $\vdash A$.

Теорема 1. *(Теорема о корректности). Всякая доказуемая формула исчисления высказываний общезначима.*

$\triangleleft$ Все аксиомы исчисления высказываний — общезначимые формулы. Это доказывается путем построения таблиц истинности или какими-либо другими способами, рассмотренными ранее. Например, покажем тождественную истинность аксиомы 1: $A \Rightarrow (B \Rightarrow A)$.

A	B	$B \Rightarrow A$	$A \Rightarrow (B \Rightarrow A)$
0	0	1	1
0	1	0	1
1	0	1	1
1	1	1	1

Вместо построения таблицы истинности можно было произвести эквивалентные преобразования:

$$A \Rightarrow (B \Rightarrow A) \sim \neg A \vee (\neg B \vee A) \sim 1\ .$$

Общезначимость всех остальных аксиом доказывается аналогично. Таким образом, для любой аксиомы A имеет место $\models A$.

По теореме 2 из § 1, если $\models A$ и $\models A \Rightarrow C$, то $\models C$. Отсюда следует, что если из общезначимых формул A и B по правилу отделения получается формула C, то C также общезначима. Действительно, чтобы правило отделения было применимо, формула B должна иметь вид $A \Rightarrow C$.

Рассмотрим формальное доказательство $B_1, B_2, \ldots, B_n$ формулы $B = B_n$. В нем каждая формула B_i — либо аксиома, либо получается по правилу отделения из предыдущих. В обоих случаях $\models B_i$; в частности, $\models B$, т.е. теорема B общезначима. $\triangleright$

Упражнение 1. Докажите тождественную истинность всех аксиом исчисления высказываний.

Следствие. *(Абсолютная непротиворечивость). Не существует формулы B такой, что доказуемы формулы B и $\neg B$.*

$\triangleleft$ Пусть для некоторой формулы B одновременно справедливы секвенции $\vdash B$ и $\vdash \neg B$. По теореме 1 тогда $\models B$ и $\models \neg B$, т.е. при любой интерпретации I значения $|B| = |\neg B| = 1$. Но это невозможно, так как если B имеет значение 1, то $\neg B$ должно иметь значение 0. $\triangleright$

Абсолютно непротиворечивой называется формальная теория, в которой не все формулы доказуемы, т.е. не все формулы суть теоремы. Следствие теоремы 1 как раз утверждает это для исчисления высказываний. Можно привести конкретный пример: поскольку известно, что $A \Rightarrow A$ — теорема (теорема 1 § 5), то $\neg(A \Rightarrow A)$ не есть теорема. Вообще говоря, в абсолютно непротиворечивой теории отношение доказуемости разбивает множество всех формул теории на два класса: теоремы и нетеоремы. Согласно свойству корректности, все теоремы общезначимы. Существуют ли общезначимые формулы, не являющиеся теоремами?

2. Правила введения и удаления логических связок

Использование дополнительных свойств выводимости, а также известных теорем облегчает процесс построения вывода, как мы уже могли убедиться в предыдущем параграфе. Добавим еще ряд *производных* правил вывода — ими можно пользоваться наравне с правилом отделения, но их предварительно нужно обосновать. Производное правило 1-го рода записывается как $F_1, F_2 \vdash G$ и означает, что из формул F_1 и F_2 выводится формула G. Производное правило 2-го рода записывается как $\frac{S_1;\, S_2}{S}$ и означает, что из справедливости секвенций S_1 и S_2 вытекает справедливость секвенции S.

Теорема 2. *Для любых формул A, B, C и списка формул Γ имеют место следующие правила вывода*[1] *:*

$\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}$	*(введ.$\Rightarrow$)*	$A, A \Rightarrow B \vdash B$	*(удал.$\Rightarrow$, или MP)*
$A, B \vdash A \wedge B$	*(введ.$\wedge$)*	$A \wedge B \vdash A$ $A \wedge B \vdash B$	*(удал.$\wedge$)*
$A \vdash A \vee B$ $B \vdash A \vee B$	*(введ.$\vee$)*	$\dfrac{\Gamma, A \vdash C; \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}$	*(удал.$\vee$, или разбор случаев)*
$\dfrac{\Gamma, A \vdash B; \quad \Gamma, A \vdash \neg B}{\Gamma \vdash \neg A}$	*(введ.$\neg$, или приведение к абсурду)*	$\neg\neg A \vdash A$	*(удал.$\neg\neg$)*
		$A, \neg A \vdash B$	*(удал.$\neg$)*
$A \Rightarrow B, B \Rightarrow A \vdash A \Leftrightarrow B$	*(введ.$\Leftrightarrow$)*	$A \Leftrightarrow B \vdash A \Rightarrow B$ $A \Leftrightarrow B \vdash B \Rightarrow A$	*(удал.$\Leftrightarrow$)*

$\triangleleft$ Введение $\Rightarrow$ имеет место в силу теоремы дедукции. Удаление $\Rightarrow$ выражает собой правило отделения. Введение $\wedge, \vee, \Leftrightarrow$ и удаление $\wedge, \neg\neg, \Leftrightarrow$ непосредственно вытекают из аксиом и теоремы 3 § 5.

Докажем, например, введение $\wedge$:

1. $\vdash A \Rightarrow (B \Rightarrow A \wedge B)$ (аксиома 5).
2. $A \vdash B \Rightarrow A \wedge B$ (теорема 3 § 5, 1).
3. $A,\ B \vdash A \wedge B$ (теорема 3 § 5, 2).

Докажем введение $\vee$:

1. $\vdash A \Rightarrow A \vee B$ (аксиома 6).
2. $A \vdash A \vee B$ (теорема 3 § 5, 1).

Упражнение 2. Докажите введение $\Leftrightarrow$ и удаление $\wedge, \neg\neg, \Leftrightarrow$.

Докажем удаление $\vee$ (правило разбора случаев):

1. $\Gamma, A \vdash C$ (гипотеза 1).
2. $\Gamma, B \vdash C$ (гипотеза 2).
3. $\Gamma \vdash A \Rightarrow C$ (введ.$\Rightarrow$, 1).
4. $\Gamma \vdash B \Rightarrow C$ (введ.$\Rightarrow$, 2).
5. $A \Rightarrow C, B \Rightarrow C, A \vee B \vdash C$ (по аксиоме 8, см. ниже).
6. $\Gamma, A \vee B \vdash C$ (транзитивность, 3,4,5).

Вывод формулы 5 произведем отдельно:

[1] Названия правил поясняются следующим. Введение связки означает, что она появляется в заключении секвенции; удаление — связка присутствовала в одной из гипотез, но пропала в заключении.

1′.	$A \Rightarrow C$	(гипотеза 1).
2′.	$B \Rightarrow C$	(гипотеза 2).
3′.	$A \vee B$	(гипотеза 3).
4′.	$(A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \vee B \Rightarrow C))$	(аксиома 8).
5′.	$(B \Rightarrow C) \Rightarrow (A \vee B \Rightarrow C)$	(MP, $1'$,$4'$).
6′.	$A \vee B \Rightarrow C$	(MP, $2'$,$5'$).
7′.	C	(MP, $3'$,$6'$).

Совершенно аналогично доказывается введение $\neg$ (правило приведения к абсурду):

1.	$\Gamma, A \vdash B$	(гипотеза 1).
2.	$\Gamma, A \vdash \neg B$	(гипотеза 2).
3.	$\Gamma \vdash A \Rightarrow B$	(введ.$\Rightarrow$, 1).
4.	$\Gamma \vdash A \Rightarrow \neg B$	(введ.$\Rightarrow$, 2).
5.	$A \Rightarrow B, A \Rightarrow \neg B \vdash \neg A$	(по аксиоме 9).
6.	$\Gamma \vdash \neg A$	(транзитивность, 3,4,5).

Докажем удаление $\neg$ (правило противоречия):

1.	$A, \neg A, \neg B \vdash A$	(рефлексивность).
2.	$A, \neg A, \neg B \vdash \neg A$	(рефлексивность).
3.	$A, \neg A \vdash \neg\neg B$	(прив. к абсурду, 1, 2).
4.	$\neg\neg B \vdash B$	(удал.$\neg\neg$).
5.	$A, \neg A \vdash B$	(транзитивность, 3, 4). ▷

В дальнейшем выводы, аналогичные последнему, будем записывать в более компактной форме:

$$\left.\begin{array}{l} A, \neg A, \neg B \vdash A \\ A, \neg A, \neg B \vdash \neg A \end{array}\right\} \quad A, \neg A \vdash \neg\neg B \vdash B.$$

Пример 1. Докажем секвенцию $A \vee B \vdash \neg A \Rightarrow B$:

1.	$A, \neg A \vdash B$	(удал.$\neg$).
2.	$A \vdash \neg A \Rightarrow B$	(введ.$\Rightarrow$).
3.	$B, \neg A \vdash B$	(рефлексивность).
4.	$B \vdash \neg A \Rightarrow B$	(введ.$\Rightarrow$, 3).
5.	$A \vee B \vdash \neg A \Rightarrow B$	(разбор случаев, 2, 4).

3. Полнота исчисления высказываний

При доказательстве теоремы о полноте исчисления высказываний нам потребуется ряд лемм.

Лемма 1. *Для любой формулы A имеет место секвенция $A \vdash \neg\neg A$.*

$$\triangleleft \qquad \left.\begin{array}{l} A, \neg A \vdash A \\ A, \neg A \vdash \neg A \end{array}\right\} \quad A \vdash \neg\neg A. \quad \triangleright$$

Лемма 2. *Для любых формул A и B имеет место секвенция $A \Rightarrow B, \neg A \Rightarrow B \vdash B$.*

$\triangleleft$ Пусть $\Gamma = \{A \Rightarrow B, \neg A \Rightarrow B\}$; тогда

$$\begin{array}{l} \left.\begin{array}{r} \Gamma, \neg B, A \vdash B \ \ (\text{MP}) \\ \Gamma, \neg B, A \vdash \neg B \quad\quad\ \end{array}\right\} \quad \Gamma, \neg B \vdash \neg A \quad (\text{прив. к абсурду}), \\ \left.\begin{array}{r} \Gamma, \neg B, \neg A \vdash B \ \ (\text{MP}) \\ \Gamma, \neg B, \neg A \vdash \neg B \quad\quad\ \end{array}\right\} \quad \Gamma, \neg B \vdash \neg\neg A \quad (\text{прив. к абсурду}). \end{array}$$

Еще раз применяя правило приведения к абсурду, получим:

$$\Gamma \vdash \neg\neg B \vdash B. \quad \triangleright$$

Лемма 3. *Пусть A — формула; $L_1, \ldots, L_k$ — атомы, входящие в A; I — интерпретация этих атомов. Пусть*

$$L_i' = \begin{cases} L_i & \text{при } |L_i| = 1, \\ \neg L_i & \text{при } |L_i| = 0, \end{cases} \quad \text{и точно так же} \quad A' = \begin{cases} A & \text{при } |A| = 1, \\ \neg A & \text{при } |A| = 0. \end{cases}.$$

Тогда $L_1', \ldots, L_k' \vdash A'$.

Поскольку формулировка этой леммы не простая, проиллюстрируем ее на примере. Для формулы $A = (\neg L_1 \Rightarrow L_2)$ таблица значений имеет вид:

L_1	L_2	A
0	0	0
0	1	1
1	0	1
1	1	1

Каждая строка таблицы задает некоторую интерпретацию; первой строке соответствует секвенция $\neg L_1, \neg L_2 \vdash \neg(\neg L_1 \Rightarrow L_2)$, второй строке — секвенция $\neg L_1, L_2 \vdash (\neg L_1 \Rightarrow L_2)$ и т.д.

$\triangleleft$ Доказательство проведем индукцией по числу связок n, входящих в состав формулы A.

Пусть $n = 0$. Тогда A состоит из одного атома: $A = L_1$, и доказательство леммы сводится к проверке секвенции $L_1 \vdash L_1$ при $|L_1| = 1$ и $\neg L_1 \vdash \neg L_1$ при $|L_1| = 0$.

Пусть утверждение леммы верно для любой формулы с числом связок $m < n$. Внешней связкой формулы A может являться либо $\neg$, либо одна из бинарных связок.

I. Рассмотрим случай, когда $A = \neg B$. Так как B содержит на одну связку меньше, чем A, по предположению индукции справедливо $L'_1, \dots, L'_k \vdash B'$. Проверим, что $B' \vdash A'$. Возможны два варианта:

$|B| = 0$, тогда $|A| = 1, B' = \neg B, A' = A = \neg B$, и нужно проверить $\neg B \vdash \neg B$;

$|B| = 1$, тогда $|A| = 0, B' = B, A' = \neg A = \neg\neg B$, и нужно проверить $B \vdash \neg\neg B$.

Обе проверяемые секвенции верны; первая в силу рефлексивности, вторая — согласно лемме 1.

II. Для каждого из случаев $A = (B \wedge C)$, $A = (B \vee C)$, $A = (B \Rightarrow C)$, $A = (B \Leftrightarrow C)$ по предположению индукции справедливо $L'_1, \dots, L'_k \vdash B'$ и $L'_1, \dots, L'_k \vdash C'$ (так как и B, и C содержат меньше связок, чем A). Поэтому проверке подлежат следующие секвенции[1] (учитываем здесь различные значения B и C):

B	C	$A = (B \wedge C)$	$A = (B \vee C)$	$A = (B \Rightarrow C)$
0	0	$\neg B, \neg C \vdash \neg(B \wedge C)$	$\neg B, \neg C \vdash \neg(B \vee C)$	$\neg B, \neg C \vdash B \Rightarrow C$
0	1	$\neg B, C \vdash \neg(B \wedge C)$	$\neg B, C \vdash B \vee C$	$\neg B, C \vdash B \Rightarrow C$
1	0	$B, \neg C \vdash \neg(B \wedge C)$	$B, \neg C \vdash B \vee C$	$B, \neg C \vdash \neg(B \Rightarrow C)$
1	1	$B, C \vdash B \wedge C$	$B, C \vdash B \vee C$	$B, C \vdash B \Rightarrow C$

Проверка каждой из 16 секвенций проводится с помощью свойств выводимости и правил введения и удаления логических связок. Например, докажем $\neg B, \neg C \vdash \neg(B \wedge C)$:

$$\left.\begin{array}{l} \neg B, \neg C, B \wedge C \vdash B \wedge C \vdash B \\ \neg B, \neg C, B \wedge C \vdash \neg B \end{array}\right\} \quad \neg B, \neg C \vdash \neg(B \wedge C).$$

Докажем еще $\neg B, \neg C \vdash \neg(B \vee C)$, пользуясь неоднократно правилом приведения к абсурду и один раз правилом разбора случаев:

$$\left.\begin{array}{r} \left.\begin{array}{l} \neg B, \neg C, B, B \vee C \vdash B \\ \neg B, \neg C, B, B \vee C \vdash \neg B \end{array}\right\} \quad \neg B, \neg C, B \vdash \neg(B \vee C) \\ \text{аналогично} \quad \neg B, \neg C, C \vdash \neg(B \vee C) \end{array}\right\},$$

$$\left.\begin{array}{ll} \text{добавим к} & \neg B, \neg C, B \vee C \vdash \neg(B \vee C) \\ \text{секвенцию} & \neg B, \neg C, B \vee C \vdash B \vee C \end{array}\right\} \quad \neg B, \neg C \vdash \neg(B \vee C).$$

Проверка остальных секвенций не представляет сложностей. $\triangleright$

Упражнение 3. Докажите все секвенции, выписанные в приведенной выше таблице, а также секвенции, относящиеся к случаю $A = (B \Leftrightarrow C)$.

[1] А также 4 секвенции для $A = (B \Leftrightarrow C)$, не уместившиеся в таблице.

Теорема 3. *Всякая общезначимая формула исчисления высказываний доказуема.*

$\triangleleft$ Предположим, что $\models A$. Пусть $L_1, \ldots, L_k$ — атомы, входящие в A. При любой интерпретации I имеем $|A|_I = 1$; тогда $A' = A$ и в силу леммы 3 $L'_1, \ldots, L'_k \ \vdash \ A$. В качестве L'_k можно выбрать и L_k, и $\neg L_k$; следовательно, справедливо и $L'_1, \ldots, L_k \ \vdash \ A$, и $L'_1, \ldots, \neg L_k \ \vdash \ A$. По правилу введения $\Rightarrow$ отсюда следует $L'_1, \ldots, L'_{k-1} \ \vdash \ L_k \Rightarrow A$, и $L'_1, \ldots, L'_{k-1} \ \vdash \ \neg L_k \Rightarrow A$, но в силу леммы 2 $L_k \Rightarrow A, \ \neg L_k \Rightarrow A \ \vdash \ A$; поэтому по свойству транзитивности $L'_1, \ldots, L'_{k-1} \vdash A$. Число гипотез уменьшилось; повторение этого рассуждения последовательно приводит к секвенциям $L'_1, \ldots, L'_{k-2} \ \vdash \ A; \ldots; L'_1 \ \vdash \ A$; и, наконец, $\vdash A$. $\triangleright$

Пример 2. Мы знаем, что $\models A \vee \neg A$. Чтобы доказать формулу $A \vee \neg A$, будем исходить из атома A и секвенций $A \ \vdash \ A \vee \neg A$ и $\neg A \ \vdash \ A \vee \neg A$, очевидно, верных по правилу введения $\vee$. Можно взять теперь $\vdash \ A \Rightarrow A \vee \neg A$ и $\vdash \ \neg A \Rightarrow A \vee \neg A$ (в данном случае это даже аксиомы, получаемые из схем аксиом 6 и 7) и применить лемму 2, что даст $\vdash \ A \vee \neg A$.

Другой способ основан на применении правила приведения к абсурду:

$$\left.\begin{array}{r} \neg(A \vee \neg A), A \ \vdash \ A \ \vdash \ A \vee \neg A \\ \neg(A \vee \neg A), A \ \vdash \quad \neg(A \vee \neg A) \end{array}\right\} \quad \neg(A \vee \neg A) \ \vdash \ \neg A,$$

$$\left.\begin{array}{r} \neg(A \vee \neg A), \neg A \ \vdash \ \neg A \ \vdash \ A \vee \neg A \\ \neg(A \vee \neg A), \neg A \ \vdash \quad \neg(A \vee \neg A) \end{array}\right\} \quad \neg(A \vee \neg A) \ \vdash \ \neg\neg A.$$

Следовательно, $\vdash \ \neg\neg(A \vee \neg A)$, и после удаления $\neg\neg$ получим $\vdash A \vee \neg A$.

§7. Исчисление секвенций

1. Аксиомы и правила вывода

Познакомимся с другой теорией, формализующей логику высказываний, — исчислением секвенций. Основной конструкцией здесь является *секвенция* — выражение вида $\Gamma \vdash F$, где Γ — список формул, возможно, пустой; F — формула или символ $\Box$[1]. Таким образом, допустимы секвенции $\vdash F$ (такие секвенции мы уже рассматривали; они используются для выражения того факта, что F есть теорема) и $\Gamma \vdash$ (что означает противоречивость посылок Γ). Смысл секвенции $\Gamma \vdash F$ состоит в том, что формула F выводится из гипотез Γ. Список Γ называется *антецедентом* секвенции, F — *консеквентом*, или *заключением*.

Определение формулы практически не отличается от принятого в логике высказываний. Однако мы воспользуемся возможностью сужения набора основных логических связок, о которой говорили в замечании II § 5, и исключим эквиваленцию из числа основных связок. Выражение $A \Leftrightarrow B$ определим как сокращение для формулы $(A \Rightarrow B) \wedge (B \Rightarrow A)$.

Множество аксиом задается с помощью одной-единственной схемы. Правил вывода значительно больше — к ним относятся 10 правил введения и удаления логических связок и одно структурное правило — правило утончения.

Схема аксиом: $F \vdash F$.

Правила вывода:

Правила введения — Правила удаления

$$\frac{\Gamma \vdash A;\ \Gamma \vdash B}{\Gamma \vdash A \wedge B} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \quad \text{(вв. и уд. } \wedge\text{).}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \qquad \frac{\Gamma, A \vdash C;\ \Gamma, B \vdash C;\ \Gamma \vdash A \vee B}{\Gamma \vdash C} \quad \text{(вв. и уд. } \vee\text{).}$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \qquad \frac{\Gamma \vdash A;\ \Gamma \vdash A \Rightarrow B}{\Gamma \vdash B} \quad \text{(вв. и уд. } \Rightarrow\text{).}$$

[1] Впрочем, в секвенции $\Gamma \vdash \Box$ символ противоречия $\Box$ часто опускают: $\Gamma \vdash$.

$$\frac{\Gamma \vdash A;\ \Gamma \vdash \neg A}{\Gamma \vdash} \qquad\qquad \frac{\Gamma, \neg A \vdash}{\Gamma \vdash A} \quad \text{(вв. и уд. }\Box\text{).}$$

$$\frac{\Gamma \vdash A}{\Gamma, B \vdash A} \qquad\qquad \text{(утончение).}$$

Отметим, что имеется два правила удаления $\wedge$ и два правила введения $\vee$.

2. Дерево доказательства

Вместо линейного вывода в исчислении секвенций по традиции используется древовидный вывод, или дерево доказательства.

Определение. *Деревом доказательства* называется конструкция, построенная при помощи следующих правил:

(1) аксиома является деревом доказательства, состоящим только из корня — самой этой аксиомы;

(2) если $T_1, \ldots, T_k$ — деревья доказательства с корнями $R_1, \ldots, R_k$ и $\dfrac{R_1, \ldots, R_k}{\Sigma}$ — правило вывода, где Σ — некоторая секвенция, то $\dfrac{T_1, \ldots, T_k}{\Sigma}$ — дерево доказательства с корнем Σ.

Секвенция Σ называется *доказуемой*, если существует дерево доказательства с корнем Σ. Формула F называется доказуемой, если доказуема секвенция $\vdash F$.

Пример 1. Докажем секвенцию $A \wedge B \vdash B \wedge A$.

$$\cfrac{\cfrac{A \wedge B \vdash A \wedge B}{A \wedge B \vdash B}(\text{уд.}\wedge_2) \qquad \cfrac{A \wedge B \vdash A \wedge B}{A \wedge B \vdash A}(\text{уд.}\wedge_1)}{A \wedge B \vdash B \wedge A}(\text{вв.}\wedge).$$

Пример 2. Еще проще выводится секвенция $A, B \vdash A \wedge B$:

$$\cfrac{\cfrac{A \vdash A}{A, B \vdash A}(\text{ут.}) \qquad \cfrac{B \vdash B}{A, B \vdash B}(\text{ут.})}{A, B \vdash A \wedge B}(\text{вв.}\wedge).$$

Справа от черты мы указываем на применяемое правило. Однако ввиду частого использования правила утончения не будем указывать на его применение.

Пример 3. Докажем секвенцию $A \Rightarrow B,\ B \Rightarrow C \vdash A \Rightarrow C$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A}{A \Rightarrow B, A \vdash A} \quad \dfrac{A \Rightarrow B \vdash A \Rightarrow B}{A \Rightarrow B, A \vdash A \Rightarrow B}}{A \Rightarrow B, A \vdash B}\text{(уд. }\Rightarrow\text{)}}{A \Rightarrow B, B \Rightarrow C, A \vdash B} \qquad \dfrac{B \Rightarrow C \vdash B \Rightarrow C}{A \Rightarrow B, B \Rightarrow C, A \vdash B \Rightarrow C}}{A \Rightarrow B, B \Rightarrow C, A \vdash C}\text{(уд. }\Rightarrow\text{).}}{A \Rightarrow B, B \Rightarrow C \vdash A \Rightarrow C}\text{(вв. }\Rightarrow\text{)}$$

Мы рекомендуем строить деревья доказательств снизу вверх, начиная с корней (т.е. с секвенций, которые требуется доказать) и постепенно наращивая дерево так, чтобы конечными секвенциями были аксиомы. При этом следует пользоваться следующими эвристиками:

— если доказываемая секвенция имеет вид $\Gamma \vdash A \wedge B$, причем Γ не содержит формулы $A \wedge B$, то нужно применить правило введения $\wedge$ и далее строить две ветви доказательства $\Gamma \vdash A$ и $\Gamma \vdash B$;

— если доказываемая секвенция имеет вид $\Gamma \vdash A \Rightarrow B$, причем Γ не содержит формулы $A \Rightarrow B$, то нужно применить правило введения $\Rightarrow$ и далее доказывать $\Gamma, A \vdash B$;

— если доказываемая секвенция имеет вид $\Gamma \vdash A \vee B$, причем Γ не содержит формулы $A \vee B$, то можно применить правило введения $\vee$, но только в том случае, если можно вывести $\Gamma \vdash A$ или $\Gamma \vdash B$;

— если формула $A \wedge B$ содержится в антецеденте, но не содержится в консеквенте доказываемой секвенции, то можно попытаться дойти до секвенций, в которых консеквент есть A или B, и применить правило удаления $\wedge$;

— если формула $A \Rightarrow B$ содержится в антецеденте, но не содержится в консеквенте доказываемой секвенции, то можно попытаться дойти до секвенции, в которой консеквент есть B, и, применив правило удаления $\Rightarrow$, перейти к доказательству секвенции с консеквентом A;

— если формула $A \vee B$ содержится в антецеденте, но не содержится в консеквенте доказываемой секвенции, то можно, применив правило удаления $\vee$, далее строить две ветви доказательства секвенций, в которых $A \vee B$ заменено на A и B соответственно;

— если вышеперечисленные приемы ничего не дают, надо обратиться к доказательству от противного, т.е. применить правило удаления противоречия, а затем (для вывода секвенции вида $\Gamma \vdash \ $) — правило введения противоречия.

Таким образом, при построении дерева доказательства правила введения позволяют разбирать на части консеквент, а правила удаления — антецедент секвенции.

Применяя правило введения противоречия, важно правильно подобрать формулу A.

Часто значительное упрощение доказательства дают допустимые правила вывода (см. следующий пункт).

Чтобы не пойти по тупиковому пути при построении доказательства, следует постоянно проверять, можно ли вообще вывести те секвенции, к которым мы пришли. Если речь идет о секвенции вида $\Gamma \vdash A$, то в силу полноты исчисления секвенций (см. п. 4) для этого достаточно проверить, имеет ли место логическое следование $\Gamma \models A$.

3. Эквивалентность и допустимые правила вывода

Говорят, что формулы F и G *эквивалентны* в смысле исчисления секвенций, если доказуемы секвенции $F \vdash G$ и $G \vdash F$. Будем записывать в таком случае $F \equiv G$.

Пример 4. Докажем эквивалентность $A \equiv \neg\neg A$.

$$\cfrac{\cfrac{\cfrac{\neg A \vdash \neg A}{\neg\neg A, \neg A \vdash \neg A} \qquad \cfrac{\neg\neg A \vdash \neg\neg A}{\neg\neg A, \neg A \vdash \neg\neg A}}{\neg\neg A, \neg A \vdash}\,(\text{вв.}\square)}{\neg\neg A \vdash A}\,(\text{уд.}\square).$$

Из построенного доказательства секвенции $\neg\neg A \vdash A$ ясно, что и секвенция $\neg\neg\neg A \vdash \neg A$ является доказуемой. Используем это:

$$\cfrac{\cfrac{\cfrac{A \vdash A}{A, \neg\neg\neg A \vdash A} \qquad \cfrac{\neg\neg\neg A \vdash \neg A}{A, \neg\neg\neg A \vdash \neg A}}{A, \neg\neg\neg A \vdash}\,(\text{вв.}\square)}{A \vdash \neg\neg A}\,(\text{уд.}\square).$$

Чтобы не иметь дело с длинными цепочками отрицаний, можно ввести правила введения отрицания и удаления двойного отрицания:

$$\frac{\Gamma, A \vdash}{\Gamma \vdash \neg A} \qquad\qquad \frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A} \qquad\qquad (\text{вв. } \neg \text{ и уд. } \neg\neg).$$

Правило называется *допустимым*, если его добавление к списку правил вывода не расширяет множество доказуемых секвенций.

Теорема 1. *Следующие правила являются допустимыми:*

1) $\dfrac{\Gamma \vdash A}{\Delta \vdash A}$ (где $\Gamma \subset \Delta$);   2) $\dfrac{\Gamma \vdash}{\Delta \vdash}$ (где $\Gamma \subset \Delta$);

3) $\dfrac{\Gamma \vdash A;\ \Gamma, A \vdash B}{\Gamma \vdash B}$;   4) $\dfrac{\Gamma, A, B, \Delta \vdash C}{\Gamma, A \wedge B, \Delta \vdash C}$;

5) $\dfrac{\Gamma \vdash A \wedge \neg A}{\Gamma \vdash}$;   6) $\dfrac{\Gamma \vdash}{\Gamma \vdash A}$;

7) $\dfrac{\Gamma, A \vdash}{\Gamma \vdash \neg A}$;   8) $\dfrac{\Gamma \vdash A}{\Gamma, \neg A \vdash}$;   9) $\dfrac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}$;

10) $\dfrac{\Gamma, A \vdash B}{\Gamma, \neg B \vdash \neg A}$;   11) $\dfrac{\Gamma, \neg A \vdash \neg B}{\Gamma, B \vdash A}$.

$\triangleleft$ Допустимость правила 1) следует из правила утончения; 2) — из 1), 5) и 6). Докажем правило 3):

$$\cfrac{\Gamma \vdash A \qquad \cfrac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}}{\Gamma \vdash B}.$$

Допустимость правила 4) следует из правила 3), правила удаления $\wedge$ и правила утончения. Докажем правила 5) и 6):

$$\cfrac{\cfrac{\Gamma \vdash A \wedge \neg A}{\Gamma \vdash A} \qquad \cfrac{\Gamma \vdash A \wedge \neg A}{\Gamma \vdash \neg A}}{\Gamma \vdash}; \qquad\qquad \cfrac{\cfrac{\Gamma \vdash}{\Gamma, \neg A \vdash}}{\Gamma \vdash A}.$$

Чтобы доказать допустимость правила 7), покажем, что секвенция $A, \neg A \vdash$ доказуема; для этого применим правило 5) и пример 2:

$$\frac{A, \neg A \vdash A \wedge \neg A}{A, \neg A \vdash}.$$

Тогда, разумеется, и секвенция $\neg A, \neg\neg A \vdash$ доказуема. Используем это в следующем дереве доказательства:

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\neg\neg A, \neg A \vdash}{\Gamma, \neg\neg A, \neg A \vdash}}{\Gamma, \neg\neg A \vdash A} \qquad \cfrac{\cfrac{\cfrac{\Gamma, A \vdash}{\Gamma, A \vdash A \wedge \neg A}}{\Gamma, \neg\neg A, A \vdash A \wedge \neg A}}{\Gamma, \neg\neg A \vdash A \Rightarrow A \wedge \neg A}}{\Gamma, \neg\neg A \vdash A \wedge \neg A}}{\Gamma, \neg\neg A \vdash}}{\Gamma \vdash \neg A}.$$

Доказательства допустимости остальных правил не представляет трудностей. $\triangleright$

Упражнение 1. Докажите допустимость правил 4), 8)–11).

4. Равносильность исчисления секвенций и исчисления высказываний

Сравнивая две формальные теории, будем использовать их сокращенные названия: ИС — исчисление секвенций, ИВ — исчисление высказываний.

Лемма 1. *Доказуемость в ИС секвенции $A_1, \ldots, A_n \vdash B$ равносильна доказуемости в ИС формулы*

$$A_1 \Rightarrow (A_2 \Rightarrow (\ldots \Rightarrow (A_n \Rightarrow B)\ldots)).$$

$\triangleleft$ В одну сторону проверяется применением правила введения $\Rightarrow$, в другую — применением правила удаления $\Rightarrow$. $\triangleright$

Лемма 2. *Все аксиомы ИВ являются доказуемыми формулами ИС.*

$\triangleleft$ В силу леммы 1, очевидно, достаточно доказать секвенции:

1) $A, B \vdash A$;
2) $A \Rightarrow (B \Rightarrow C), A \Rightarrow B, A \vdash C$;
3) $A \wedge B \vdash A$;
4) $A \wedge B \vdash B$;
5) $A, B \vdash A \wedge B$;
6) $A \vdash A \vee B$;
7) $B \vdash A \vee B$;
8) $A \Rightarrow C, B \Rightarrow C, A \vee B \vdash C$;
9) $A \Rightarrow B, A \Rightarrow \neg B \vdash \neg A$;
10) $\neg\neg A \vdash A$.

Аксиомы 11–13 в силу соглашения о смысле эквиваленции в ИС попадают под действие аксиом 3–5.

Докажем, для примера, секвенцию 8. Введем обозначение $\Gamma = \{A \Rightarrow C, B \Rightarrow C, A \vee B\}$.

$$\cfrac{\cfrac{A \Rightarrow C, A \vdash C}{\Gamma, A \vdash C} \quad \cfrac{B \Rightarrow C, B \vdash C}{\Gamma, B \vdash C} \quad \cfrac{A \vee B \vdash A \vee B}{\Gamma \vdash A \vee B}}{A \Rightarrow C, B \Rightarrow C, A \vee B \vdash C}.$$

Вывод секвенций $A \Rightarrow B, A \vdash B$ (а именно такой вид имеют оставшиеся секвенции наверху первой и второй ветви) проведен в левой ветви доказательства в примере 3. $\triangleright$

Теорема 2. *1) Секвенция $\Gamma \vdash A$ тогда и только тогда доказуема в ИС, когда A выводима из Γ в ИВ.*

2) Секвенция $\Gamma \vdash$ тогда и только тогда доказуема в ИС, когда формула $P \wedge \neg P$ выводима из Γ в ИВ.

$\triangleleft$ Очевидно, что вторая часть теоремы вытекает из первой в силу возможности применить допустимые правила вывода 5) и 6).

I. Пусть $\Gamma \vdash A$ в ИВ. Докажем, что секвенция $\Gamma \vdash A$ доказуема в ИС, используя индукцию по длине вывода в ИВ.

Пусть вывод в ИВ состоит из единственной формулы A. Тогда A — аксиома или гипотеза. В первом случае, согласно лемме 2 и допустимому правилу 1), доказуемы секвенции $\vdash A$ и $\Gamma \vdash A$. Во втором случае применение того же допустимого правила к аксиоме ИС $A \vdash A$ доказывает секвенцию $\Gamma \vdash A$.

Рассмотрим теперь вывод в ИВ $B_1, \ldots, B_n (= A)$, имеющий произвольную длину $n > 1$. Тогда формула A должна получаться по правилу отделения из B_j, B_k, $(j, k < n)$, причем по предположению индукции секвенции $\Gamma \vdash B_j$ и $\Gamma \vdash B_k$ доказуемы, так как вывод каждой из формул B_j, B_k имеет длину, меньшую n. Формула B_k должна иметь вид $B_j \Rightarrow A$, и секвенция выводится по правилу удаления $\Rightarrow$.

II. Пусть секвенция $\Gamma \vdash A$ доказуема в ИС. Докажем, что существует вывод формулы A из Γ в ИВ.

В силу свойств выводимости в ИВ (теорема 2 § 5, рефлексивность и транзитивность), достаточно показать, что все правила вывода ИС сохраняют выводимость в ИВ (при этом секвенцию $\Gamma \vdash$ будем заменять на $\Gamma \vdash P \wedge \neg P$).

Сохранение выводимости для правил введения и удаления $\wedge$, $\vee$ и $\Rightarrow$ можно доказать, используя одноименные правила ИВ (теорема 2 § 6) и транзитивность отношения выводимости в ИВ. Сохранение выводимости для правила утончения имеет место в силу свойства утончения (теорема 2(2) § 5).

Докажем сохранение выводимости правилом удаления противоречия, т.е. докажем в ИВ производное правило вывода

$$\frac{\Gamma, \neg A \vdash P \wedge \neg P}{\Gamma \vdash A}:$$

1. $\Gamma, \neg A \vdash P \wedge \neg P$ (исходная посылка).
2. $\Gamma, \neg A \vdash P$ и $\Gamma, \neg A \vdash \neg P$ (удаление $\wedge$).
3. $\Gamma \vdash \neg\neg A$ (приведение к абсурду).
4. $\Gamma \vdash A$ (удаление $\neg\neg$).

Рассмотрим правило введения противоречия. Оно соответствует производному правилу ИВ

$$\frac{\Gamma \vdash A;\ \Gamma \vdash \neg A}{\Gamma \vdash P \wedge \neg P},$$

которое доказывается аналогично предыдущему. Из $\Gamma \vdash A$ и $\Gamma \vdash \neg A$ по свойству утончения получаем соответственно $\Gamma, P \wedge \neg P \vdash A$ и $\Gamma, P \wedge \neg P \vdash \neg A$. Отсюда, пользуясь правилами приведения к абсурду и удаления $\neg\neg$, получим:

$$\Gamma \vdash \neg\neg(P \wedge \neg P) \vdash P \wedge \neg P. \quad \triangleright$$

В качестве следствия получаем утверждение о полноте и корректности ИС.

Следствие 1. *Для того чтобы формула A была доказуема в ИС, необходимо и достаточно, чтобы A была общезначимой.*

$\triangleleft$ Согласно теореме 2, доказуемость формулы A в ИС равносильна доказуемости в ИВ, а это, в свою очередь, равносильно по теоремам 1 и 3 § 6 общезначимости A. $\triangleright$

Следствие 2. *Для того чтобы секвенция $\Gamma \vdash A$ была доказуема в ИС, необходимо и достаточно, чтобы имело место логическое следование $\Gamma \models A$.*

Упражнение 2. Докажите следствие 2.

§8. Логика первого порядка

В логике высказываний исходными элементами являются атомы. Из атомов составляются формулы, сами же атомы рассматриваются как единое целое. Однако существуют типы логических рассуждений, которые не могут рассматриваться таким простым способом. Например, «Все люди смертны. Конфуций — человек. Следовательно, Конфуций смертен.» Чтобы выявить связь между высказанными предложениями, необходимо детализировать строение атомов, составляющих эти предложения. Это делается в логике первого порядка, которая по сравнению с логикой высказываний имеет еще три логических понятия (*термы*, *предикаты* и *кванторы*).

Пусть $P(x)$ означает, что x обладает свойством P. Запись $\forall x P(x)$ обозначает утверждение: «для всех x свойство P выполнено». Запись $\exists x P(x)$ будет означать, что «существует x, обладающий свойством P». Символ $\forall$ называется *квантором всеобщности*, $\exists$ — *квантором существования*. Например, при обозначениях $H(x)$: «x есть человек», $S(x)$: «x смертен», k: «Конфуций» приведенное выше умозаключение примет вид:

$$\forall x(H(x) \Rightarrow S(x)),\ H(k)\ \models\ S(k).$$

Определим язык логики первого порядка — для этого последовательно введем алфавит логики первого порядка и понятия терма и формулы.

1. Язык логики первого порядка

Алфавит логики первого порядка состоит из:

1) предметных символов, или констант (т.е. имен предметов: `1, 2, Jane, John, Петербург, Шанхай`). Абстрагируясь от смысла предметов, будем их обозначать $a_1, a_2, a_3, \ldots, a, b, c, \ldots$;

2) символов предметных переменных $(x_1, x_2, x_3, \ldots, x, y, z, \ldots)$;

3) функциональных символов $(f_1, f_2, f_3, \ldots, f, g, h, \ldots)$;

4) предикатных символов $(P_1, P_2, P_3, \ldots, P, Q, R, \ldots)$;

5) логических связок $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$;

6) кванторов $\forall$, $\exists$;

7) синтаксических символов — скобок и запятой.

Каждый функциональный и предикатный символ имеет свою арность (количество аргументов). Разделение на функциональные и предикатные символы до некоторой степени условно. Например, выражение $\mathtt{sum}(x, y, z)$ может иметь тот же смысл, что и $\mathtt{sum}(x, y) = z$.

Функцией арности n будем называть отображение, ставящее в соответствие списку из n констант некоторую константу. Совершенно аналогично *предикат* — это отображение, ставящее в соответствие списку констант истинностное значение $\{\texttt{истина}, \texttt{ложь}\}$.

Пример 1. $E(x)$, «x — четное число» — унарный (одноместный) предикат; $P(x, y)$, «прямые x и y параллельны» — бинарный (двуместный) предикат; $S(x, y, z)$, «$z = x + y$ » — тернарный (трехместный) предикат.

Определение 1. *Терм* определяется рекурсивно следующим образом:

1) всякая предметная константа есть терм;

2) всякая предметная переменная есть терм;

3) если f — n-арный функциональный символ и $t_1, t_2, \ldots, t_n$ — термы, то $f(t_1, t_2, \ldots, t_n)$ — терм.

Определение 2. Если P — n-арный предикатный символ и $t_1, t_2, \ldots, t_n$ — термы, то $P(t_1, t_2, \ldots, t_n)$ — *атом* (*элементарная формула*).

Определение 3. *Формула* определяется рекурсивно следующим образом:

1) всякий атом есть формула;

2) если G и H — формулы, то $(\neg G)$, $(G \wedge H)$, $(G \vee H)$, $(G \Rightarrow H)$, $(G \Leftrightarrow H)$ — формулы;

3) если F — формула и x — предметная переменная, то $(\forall x F)$ и $(\exists x F)$ — формулы.

Пример 2. Пусть g, h, f — соответственно унарный, бинарный и тернарный функциональные символы; Q и P — унарный и бинарный предикатные символы. Тогда $f(g(x), h(a, g(y)), z)$ — терм, $P(x, h(a, g(y)))$ — атом, $\forall x(\exists y P(x, y) \Rightarrow Q(x))$ — формула.

Для опускания избыточных скобок в формулах будем пользоваться соглашением, что кванторы обладают наивысшим приоритетом в связывании выражений. Например, запись $\forall x F \vee G$ в полной форме выглядит как $((\forall x F) \vee G)$.

В формулах $\forall x F$ и $\exists x F$ подформула F называется *областью действия* квантора $\forall$ ($\exists$). Вхождение переменной x в формулу называется *связанным*, если оно является вхождением в кванторный комплекс $\forall x$ или $\exists x$ или находится в области действия квантора; в противном случае вхождение переменной называется *свободным*.

Переменная x *свободна* в формуле F, если хотя бы одно вхождение x в F свободно. Переменная x *связана* в формуле F, если хотя бы одно вхождение x в F связано.

Пример 3. В формуле $\forall x P(x, y) \wedge \forall y Q(y, z)$ переменная x связана, переменная y одновременно свободна и связана, переменная z свободна.

Будем считать, что любая переменная, содержащаяся в терме, свободна в этом терме, и любое ее вхождение в терм свободно.

Выражением называется терм или формула. Для выражений будем использовать обозначение E или $E(x_1, \ldots, x_n)$, где $x_1, \ldots, x_n$ — переменные, входящие в выражение. Выражение, не содержащее переменных, называется *основным* выражением. Выражение, не содержащее свободных переменных, называется *замкнутым* выражением. Замкнутая формула называется *предложением*.

Терм t называется *свободным для переменной* x_i в выражении E, если никакое свободное вхождение x_i в E не лежит в области действия $\forall x_j$ или $\exists x_j$, где x_j — переменная, входящая в t.

Пример 4. Терм $f(z)$ свободен для переменной y в формуле $\forall x(P(x, y) \Rightarrow Q(x, z))$, а терм $f(x)$ не свободен для y.

Если термы $t_1, \ldots, t_n$ свободны для переменных $x_1, \ldots, x_n$ соответственно в выражении E, то правомерна подстановка термов t_i вместо x_i $(1 \leqslant i \leqslant n)$ в выражении E, результат которой будем обозначать $E(t_1/x_1, \ldots, t_n/x_n)$ или $E(t_1, \ldots, t_n)$, если ясно, вместо каких переменных подставляются термы $t_1, \ldots, t_n$.

Упражнение 1. Докажите следующие утверждения:

1) всякий терм свободен для любой переменной в любом терме;

2) всякий основный терм свободен для любой переменной в любой формуле;

3) терм t свободен для любой переменной в формуле F, если никакая переменная терма t не является связанной в F;

4) переменная x свободна для x в любой формуле;

5) всякий терм свободен для переменной x в формуле F, если F не содержит свободных вхождений x.

2. Интерпретация формул

Выражения, т.е. термы и формулы в логике первого порядка имеют смысл только тогда, когда задана интерпретация входящих в них символов.

Определение 4. *Интерпретация* I в логике первого порядка состоит из непустого множества (предметной области) D и отображения оценки, которое будем обозначать $|\cdot|_I$ и которое ставит в соответствие:

1) каждой константе a — некоторый элемент $|a|_I$ из D;

2) каждому n-арному функциональному символу f — некоторую n-арную функцию (операцию) $|f|_I$ из D^n в D;

3) каждому n-арному предикатному символу P — некоторый n-арный предикат (отношение) $|P|_I$ на D^n.

При заданной интерпретации предметные переменные мыслятся пробегающими предметную область D, а связкам и кванторам придается их обычный смысл. Тогда всякий основный терм имеет определенное значение в предметной области D, всякая замкнутая формула имеет определенное истинностное значение; если же терм или формула содержат свободные переменные, то они выражают собой соответственно функцию или предикат предметной области.

Формализуем утверждения последнего абзаца.

Пусть Σ — множество всех счетных последовательностей $s = (s_1, s_2, \ldots)$ элементов из D. *Расширением* интерпретации I при помощи $s \in \Sigma$ будем называть продолжение отображения оценки $|\cdot|_I$ путем включения в него соответствия

4) каждой переменной x_j элемента $|x_j|_I^s = s_j \in D$.

Продолжим расширенную интерпретацию I^s на произвольные выражения (обычную интерпретацию можно было бы распространить только на основные выражения):

a) если выражение E есть терм $f(t_1, \ldots, t_n)$, то

$$|E|_I^s = |f|_I(|t_1|_I^s, \ldots, |t_n|_I^s);$$

b) если выражение E есть атом $P(t_1, \ldots, t_n)$, то

$$|E|_I^s = |P|_I(|t_1|_I^s, \ldots, |t_n|_I^s);$$

c) если выражение E есть формула $\neg G$, $G \wedge H$, $G \vee H$, $G \Rightarrow H$ или $G \Leftrightarrow H$, то $|E|_I^s$ определяется по истинностным значениям $|G|_I^s$ и $|H|_I^s$ как в логике высказываний;

d) если выражение E есть формула $\forall x_j F$, то $|E|_I^s = 1$ (`истина`) при условии, что $|F|_I^{s'} = 1$ для всех последовательностей $s' \in \Sigma$, отличающихся от s разве что j-й компонентой;

e) если выражение E есть формула $\exists x_j F$, то $|E|_I^s = 1$ при условии, что $|F|_I^{s'} = 1$ для некоторой последовательности $s' \in \Sigma$, отличающейся от s разве что j-й компонентой.

Будем говорить, что формула F:

— *выполнена* в расширенной интерпретации I^s, если $|F|_I^s = 1$;

— *истинна* в интерпретации I, если она выполнена в любом расширении этой интерпретации;

— *ложна* в интерпретации I, если она не выполнена ни в одном расширении этой интерпретации.

Пример 5. Рассмотрим формулу $F = \forall x(P(x) \Rightarrow Q(f(x), a))$. В этой формуле имеется одна константа a, одна связанная переменная

x, один унарный функциональный символ f, один унарный предикатный символ P и один бинарный предикатный символ Q. В качестве предметной области D возьмем множество из двух элементов $\{\alpha, \beta\}$. Зададим интерпретацию I таблицами

a
α

x	$f(x)$
α	β
β	α

x	$P(x)$
α	0
β	1

x	y	$Q(x,y)$
α	α	1
α	β	1
β	α	0
β	β	1

Рассмотрим подформулу $F_1 = \ (P(x) \Rightarrow Q(f(x), a))$ и расширение интерпретации I при помощи присваивания значений переменной x.

Если $|x| = \alpha$, то $|F_1| = |P(\alpha) \Rightarrow Q(f(\alpha), \alpha)| = |\ 0 \Rightarrow Q(\beta, \alpha)| = 1$.

Если $|x| = \beta$, то $|F_1| = |P(\beta) \Rightarrow Q(f(\beta), \beta)| = |\,1 \Rightarrow Q(\alpha, \beta)| = 1$.

Так как F_1 истинно для всех расширений I, затрагивающих x, то формула F истинна в интерпретации I.

Упражнение 2. Докажите следующие утверждения:

1) никакая формула не может быть одновременно истинной и ложной в одной и той же интерпретации;

2) формула F истинна в данной интерпретации тогда и только тогда, когда в этой интерпретации истинно $\forall x_1 \ldots \forall x_n F$, где $x_1, \ldots, x_n$ — все свободные переменные формулы F (формула $\forall x_1 \ldots \forall x_n F$ называется *замыканием* формулы F);

3) формула F, полученная из тавтологии логики высказываний подстановкой вместо ее атомов произвольных формул, истинна в любой интерпретации;

4) если свободные переменные формулы F содержатся среди переменных $x_{i_1}, \ldots, x_{i_n}$ и у последовательностей s и s' компоненты с номерами $i_1, \ldots, i_n$ совпадают, то формула F выполнена на I^s тогда и только тогда, когда она выполнена на $I^{s'}$;

5) если формула F замкнута, то в любой интерпретации F либо истинна, либо ложна.

Замкнутая формула хотя и принимает в любой интерпретации определенное истинностное значение, но в одних интерпретациях может быть истинной, а в других — ложной. Незамкнутая формула может в некоторой интерпретации быть не истинной и не ложной.

Формула F называется:

— *общезначимой*, если она истинна в каждой интерпретации ($\models F$);

— *противоречивой*, если $\neg F$ является общезначимой или, что то же самое, если F ложна в каждой интерпретации;

— *выполнимой*, если существует расширенная интерпретация, в которой она выполнена;

— *опровержимой*, если существует расширенная интерпретация, в которой выполнено $\neg F$.

Очевидно, что формула общезначима тогда и только тогда, когда она не опровержима, и выполнима тогда и только тогда, когда она не противоречива.

Если формула F истинна в интерпретации I, то говорят, что I есть *модель* формулы F $(\models_I F)$. Формула G называется *логическим следствием* формул $F_1, \ldots, F_n$, если для всякой расширенной интерпретации, в которой выполнены $F_1, \ldots, F_n$, выполнена и G $(F_1, \ldots, F_n \models G)$. Формулы F и G называются *(логически) эквивалентными*, если каждая из них является логическим следствием другой $(F \sim G)$.

Пример 6. Докажем общезначимость формулы

$$F = P(f(x)) \Rightarrow \exists x P(x).$$

Рассмотрим произвольную интерпретацию I. Формула F в ней будет истинна, если в каждом ее расширении либо не выполнено $P(f(x))$, либо выполнено $\exists x P(x)$. Но, если $P(f(x))$ выполнено при некотором значении $|x|$ переменной x, то существует элемент предметной области, равный $|f(|x|)|$, который обладает свойством P, и, следовательно, выполнено $\exists x P(x)$.

Пример 7. Пусть $F_1 = \forall x(P(x) \Rightarrow Q(x))$ и $F_2 = P(a)$. Докажем логическое следование $F_1, F_2 \models Q(a)$.

Рассмотрим любую расширенную интерпретацию, в которой выполнены формулы F_1 и F_2. В ней, очевидно, $|P(a)| = 1$. Из $|F_1| = 1$ вытекает, что $|P(x) \Rightarrow Q(x)| = 1$, каким бы ни было значение x. Выбирая $|x| = |a|$, получим $|P(a) \Rightarrow Q(a)| = 1$ и, следовательно, $|Q(a)| = 1$.

Пример 8. Составим таблицу значений формулы $F = P(a)\vee \vee\forall x(P(x) \Rightarrow Q)$ на предметной области $D = \{\alpha, \beta\}$. При этом нам надо исходить из некоторой интерпретации предиката P — логической функции одной переменной, заданной на D. Таких логических функций может быть четыре, как в п. 2, b § 2:

x	$l_1(x)$	$l_2(x)$	$l_3(x)$	$l_4(x)$
α	0	0	1	1
β	0	1	0	1

Помимо выбора $|P|$ из $\{l_1, l_2, l_3, l_4\}$, необходимо также выбрать истинностное значение Q и предметное значение a. (Для экономии места вместо таблицы с 16 строками, каждая из которых отвечает отдельной интерпретации, составим таблицу 4×4 с двумя входами.)

Q	a	l_1	l_2	l_3	l_4	$(= P)$
0	α	1	0	1	1	
0	β	1	1	0	1	
1	α	1	1	1	1	
1	β	1	1	1	1	

Так как в логике первого порядка число интерпретаций бесконечно, метод таблиц значений в общем случае неприменим для проверки формул на общезначимость (или противоречивость). В отдельных случаях применяются другие средства анализа формул.

3. Свойства кванторов и префиксная нормальная форма

Помимо основных логических законов (п. 3 § 1), которые сохраняют силу в логике первого порядка, эффективным является использование свойств кванторов, основные из которых мы сейчас рассмотрим.

Теорема 1. *Имеют место следующие логические эквивалентности:*

(1) $\forall x\forall yF(x,y) \sim \forall y\forall xF(x,y)$ *(перестановка одно-*
$\exists x\exists yF(x,y) \sim \exists y\exists xF(x,y)$ *именных кванторов),*

(2) $\forall xF(x) \sim \forall yF(y)$ *(переименование*
$\exists xF(x) \sim \exists yF(y)$ *связанных переменных),*

(3) $\neg\forall xF(x) \sim \exists x\neg F(x)$
$\neg\exists xF(x) \sim \forall x\neg F(x)$ *(отрицание кванторов),*

$$
\begin{array}{llll}
(4) & G \wedge \forall x F(x) \sim \forall x(G \wedge F(x)) & & \\
& G \vee \forall x F(x) \sim \forall x(G \vee F(x)) & & \\
& G \wedge \exists x F(x) \sim \exists x(G \wedge F(x)) & & \textit{(вынесение кванторов} \\
& G \vee \exists x F(x) \sim \exists x(G \vee F(x)) & & \textit{за скобки),} \\
(5) & \forall x F(x) \wedge \forall x G(x) \sim \forall x(F(x) \wedge G(x)) & & \textit{(группирование} \\
& \exists x F(x) \vee \exists x G(x) \sim \exists x(F(x) \vee G(x)) & & \textit{кванторов)}
\end{array}
$$

для произвольных формул F и G при условии, что в формулах (4) G не содержит свободных вхождений переменной x, а в формулах (2) y не свободна в $F(x)$, но свободна для x в $F(x)$.

$\lhd$ Согласно определению логической эквивалентности, нам необходимо показать, что во всякой расширенной интерпретации, в которой выполнена одна из частей эквивалентности, выполнена и другая.

Для доказательства эквивалентностей (1) достаточно заметить, что их левая и правая части одновременно выполнены в расширенной интерпретации, в которой $F(x, y)$ выполнено при всех возможных значениях x и y — для случая $\forall$ (при некоторых значениях x и y — для случая $\exists$).

Соотношения (2) следуют из того, что процедура проверки выполнения $\forall x F(x)$ относится к переменной x в $F(x)$, а $\forall y F(y)$ — к переменной y в $F(y)$, что дает один и тот же результат. То же справедливо для случая $\exists$.

Докажем первую из эквивалентностей (3). Выполнение $\neg\forall x F(x)$ означает, что не при всех возможных значениях x выполнено $F(x)$, т.е. при некотором $|x| \in D$ имеет место $|F(|x|)| = 0$. Но то же самое выражает выполнение $\exists x \neg F(x)$: при некотором $|x| \in D$ имеет место $|\neg F(|x|)| = 1$.

Вторая эквивалентность следует из первой и из закона двойного отрицания: $\neg\exists x F(x) \sim \neg\underline{\exists x \neg}\neg F(x) \sim \neg\underline{\neg\forall x}\neg F(x) \sim \forall x \neg F(x)$. $\rhd$

Упражнение 3. Докажите эквивалентности (4) и (5).

Заметим, что если унарный предикат $P(x)$ определен на конечном множестве $D = \{a_1, \ldots, a_n\}$, то $\forall x P(x) \sim P(a_1) \wedge \ldots \wedge P(a_n)$, а $\exists x P(x) \sim P(a_1) \vee \ldots \vee P(a_n)$. В общем случае кванторы общности и существования можно понимать как «бесконечную конъюнкцию» и «бесконечную дизъюнкцию». Тогда соотношения (3) оказываются обобщениями законов Де Моргана, а соотношения (5) — обобщениями свойства произвольного группирования членов конъюнкции (дизъюнкции).

Упражнение 4. Покажите, что $\forall x F(x) \vee \forall x G(x) \nsim \forall x(F(x) \vee G(x))$ и $\exists x F(x) \wedge \wedge \exists x G(x) \nsim \exists x(F(x) \wedge G(x))$.

Пользуясь соотношениями (1)–(5), мы можем производить эквивалентные преобразования над формулами логики первого порядка, в частности, с целью получить равносильную формулу, имеющую особенно простой вид.

Определение 5. Говорят, что формула F находится в *префиксной нормальной форме* (сокращенно *ПНФ*), если она имеет вид $\mathrm{Q}_1x_1\dots\mathrm{Q}_nx_nM$, где каждое Q_ix_i $(1 \leqslant i \leqslant n)$ есть $\forall x_i$ или $\exists x_i$, а M — формула, не содержащая кванторов. $\mathrm{Q}_1x_1\dots\mathrm{Q}_nx_n$ называется *префиксом*, а формула M — *матрицей* формулы F.

Теорема 2. *Всякая формула логики первого порядка эквивалентна некоторой формуле в префиксной нормальной форме.*

$\lhd$ Для преобразования формулы к ПНФ:

1) используем законы эквивалентности и импликации, чтобы исключить логические связки $\Rightarrow$ и $\Leftrightarrow$;

2) повторно используем закон двойного отрицания, законы Де Моргана и свойство (3), чтобы внести символы отрицания внутрь формулы, до атомов;

3) переименовываем связанные переменные (свойство (2)), если это необходимо;

4) выносим кванторы за скобки путем применения свойства (4), а также свойств (5) и (1), они могут дать некоторую экономию кванторов.

Очевидно, что описанная процедура всегда за конечное число шагов приводит к эквивалентной формуле, находящейся в ПНФ. $\rhd$

Пример 9. Приведем формулу $\forall xP(x) \Rightarrow \exists xQ(x)$ к ПНФ:
$\forall xP(x) \Rightarrow \exists xQ(x) \;\sim\; \neg\forall xP(x) \vee \exists xQ(x) \;\sim\; \exists x\neg P(x) \vee \exists xQ(x) \;\sim$
$\sim\; \exists x(\neg P(x) \vee Q(x))$.

Вот еще один пример:
$\exists xP(x,y) \Rightarrow \exists zQ(x,z) \;\sim\; \neg\exists xP(x,y) \vee \exists zQ(x,z) \;\sim\; \forall x\neg P(x,y)\vee$
$\vee\exists zQ(x,z) \;\sim\; \forall t\neg P(t,y) \vee \exists zQ(x,z) \;\sim\; \forall t(\neg P(t,y) \vee \exists zQ(x,z)) \;\sim$
$\sim\; \forall t\exists z(\neg P(t,y) \vee Q(x,z))$.

Здесь потребовалось переименовать связанную переменную x, поскольку она в данной формуле имела, помимо связанного, также и свободное вхождение — чтобы после вынесения квантора за скобку это свободное вхождение не превратилось бы в связанное.

§9. Формальные теории

Различают:

— формальные теории нулевого порядка (исчисление высказываний и исчисление секвенций);

— формальные теории первого порядка (исчисление предикатов и их расширения, о которых речь пойдет в настоящем параграфе);

— формальные теории второго и более высоких порядков.

1. Исчисление предикатов

Алфавит и правила построения формул исчисления предикатов (первого порядка) мы уже определили, изучая логику первого порядка.

Возможны различные подходы к заданию схем аксиом и правил вывода (ср. § 5 и § 7). Будем придерживаться первого варианта.

Схемы аксиом исчисления предикатов включают в себя схемы аксиом 1)–13) исчисления высказываний (п.1 § 5) и четыре дополнительные схемы аксиом для кванторов:

Q1) $\forall x A(x) \Rightarrow A(t)$;

Q2) $A(t) \Rightarrow \exists x A(x)$;

Q3) $\forall x (A \Rightarrow B) \Rightarrow (A \Rightarrow \forall x B)$;

Q4) $\forall x (A \Rightarrow B) \Rightarrow (\exists x A \Rightarrow B)$;

причем в схемах аксиом Q1), Q2) терм t свободен для x в $A(x)$, в схеме Q3) переменная x не свободна в A, в схеме Q4) x не свободна в B.

Множество правил вывода состоит из двух правил: знакомого нам правила отделения (MP) и *правила обобщения*, или *генерализации* (Gen):

$$\frac{A,\ A \Rightarrow B}{B} \quad (\mathrm{MP}), \qquad\qquad \frac{A}{\forall x A} \quad (\mathrm{Gen}).$$

Очевидно, что аксиомы Q1)–Q4) суть общезначимые формулы логики предикатов. Однако правило обобщения не удовлетворяет определению логического следования, но удовлетворяет слабому логическому следованию: для всякой интерпретации (не расширенной), в которой истинна формула A, истинна формула $\forall x A$. Поэтому, определяя понятие вывода, необходимо учесть особую роль правила обобщения.

Определение 1. *Выводом* формулы B из списка гипотез Γ называется последовательность формул $B_1, B_2, \ldots, B_m = B$, каждая из которых есть либо гипотеза, либо аксиома, либо получена по правилу вывода из предшествующих формул последовательности; причем выполняется следующее *структурное условие*: если формула $\forall x A$ получена из формулы A по правилу обобщения, то переменная x не является свободной в гипотезах, предшествующих формуле $\forall x A$ в этой последовательности.

Выводимость и доказуемость в исчислении предикатов определяется так же, как и в исчислении высказываний.

Пример 1. Построим доказательство формулы $\forall x A(x) \Rightarrow \Rightarrow \forall y A(y)$:

1.	$\forall x A(x) \Rightarrow A(y)$	(аксиома Q1).
2.	$\forall y(\forall x A(x) \Rightarrow A(y))$	(Gen, 1).
3.	$\forall y(\forall x A(x) \Rightarrow A(y)) \Rightarrow (\forall x A(x) \Rightarrow \forall y A(y))$	(аксиома Q3).
4.	$\forall x A(x) \Rightarrow \forall y A(y)$	(MP, 2, 3).

Здесь структурное условие выполнено, так как правило обобщения применяется на шаге 2, а перед ним стоит только аксиома (гипотез нет вообще).

Так же, как в исчислении высказываний, выводы даже простых формул получаются очень громоздкими. Поэтому практически для построения доказательств пользуются производными правилами вывода, среди которых ключевую роль играет теорема дедукции.

Теорема 1. *Если* $\Gamma, A \vdash B$*, то* $\Gamma \vdash A \Rightarrow B$.

$\lhd$ В доказательстве разберем только случай применения правила обобщения, так как все остальное дословно повторяет доказательство аналогичной теоремы исчисления высказываний (теорема 4 § 5).

Пусть формула B_i получена из формулы B_j $(j < i)$ по правилу обобщения, и, таким образом, имеет вид $\forall x B_j$. Без ограничения общности можно предполагать, что формула B_i в выводе непосредственно следует за B_j, т.е. $i = j + 1$. Предположим, что имеется вывод $\Gamma \vdash A \Rightarrow B_j$ и построим вывод $\Gamma \vdash A \Rightarrow \forall x B_j$.

Если в последовательности формул $B_1, \ldots, B_j$ встречается A, то в силу структурного условия переменная x не является свободной в A. Тогда допустима аксиома Q3: $\forall x(A \Rightarrow B_j) \Rightarrow (A \Rightarrow \forall x B_j)$ и возможно применение правила обобщения к формуле $A \Rightarrow B_j$, что дает $\forall x(A \Rightarrow B_j)$ и, после применения правила MP, $A \Rightarrow \forall x B_j$.

Если среди формул $B_1, \ldots, B_j$ нет A, то вывод формулы B_j и следующей за ней формулы $\forall x B_j$ не зависит от A, т.е. существует вывод формулы $\forall x B_j$ только из гипотез Γ. Остается воспользоваться аксиомой 1 в виде $\forall x B_j \Rightarrow (A \Rightarrow \forall x B_j)$ и правилом MP, чтобы вновь получить $A \Rightarrow \forall x B_j$. $\rhd$

Теорема 2. *Для любых формул A, B и любого множества формул Γ, если переменная y не является свободной в Γ и B, а терм t свободен для x в A, то имеют место следующие правила вывода:*

$$\frac{\Gamma \vdash A(y)}{\Gamma \vdash \forall y A(y)} \quad \text{(введ.}\forall\text{);} \qquad\qquad \frac{\Gamma \vdash \forall x A(x)}{\Gamma \vdash A(t)} \quad \text{(удал.}\forall\text{);}$$

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x A(x)} \quad \text{(введ.}\exists\text{);} \qquad\qquad \frac{\Gamma,\ A(y) \vdash B}{\Gamma,\ \exists y A(y) \vdash B} \quad \text{(удал.}\exists\text{).}$$

$\lhd$ Докажем, для примера, правило удаления $\exists$:

1.	$\Gamma,\ A(y) \vdash B$	(исходная посылка).
2.	$\Gamma \vdash A(y) \Rightarrow B$	(теорема дедукции).
3.	$\Gamma \vdash \forall y(A(y) \Rightarrow B)$	(Gen, 2 — т.к. y не своб. в Γ).
4.	$\forall y(A(y) \Rightarrow B) \Rightarrow (\exists y A(y) \Rightarrow B)$	(акс. Q4 — т.к. y не своб. в B).
5.	$\Gamma \vdash \exists y A(y) \Rightarrow B$	(MP, 3, 4).
6.	$\Gamma,\ \exists y A(y) \vdash B$	(теор.3, § 5). $\rhd$

Пример 2. Докажем $\vdash \exists x A(x) \Rightarrow \neg\forall x \neg A(x)$:

1.	$A(x),\ \forall x \neg A(x) \ \vdash\ A(x)$	(рефлексивность).
2.	$A(x),\ \forall x \neg A(x) \ \vdash\ \forall x \neg A(x)$	(рефлексивность).
3.	$A(x),\ \forall x \neg A(x) \ \vdash\ \neg A(x)$	(удал.$\forall$, 2).
4.	$A(x) \ \vdash\ \neg\forall x \neg A(x)$	(прив. к абсурду, 1, 3).
5.	$\exists x A(x) \ \vdash\ \neg\forall x \neg A(x)$	(удал.$\exists$, 4).

2. Эквациональные теории

Ограниченное исчисление предикатов определяется так же, как обычное исчисление предикатов, за исключением того, что ограничивается его алфавит: требуется, чтобы множества предметных, функциональных и предикатных символов были не более чем счетны (в частности, конечны или пусты), но должен быть хотя бы один предикатный символ.

Формальная теория (или *исчисление*) *первого порядка* представляет собой расширение ограниченного исчисления предикатов, при котором к аксиомам исчисления предикатов (называемых *логическими* аксиомами) добавляются *специальные* (или *нелогические*) аксиомы. Как правило, в формальной теории фиксируется ряд предметных, функциональных и предикатных символов, называемых *специальными*. *Моделью* теории называется интерпретация множества ее формул, в которой истинны все теоремы этой теории.

Формальная теория первого порядка называется *эквациональной теорией* (или *теорией с равенством*), если в ней присутствует специальный функциональный символ $=$ и следующие специальные схемы аксиом:

E1) $x = x$ (рефлексивность равенства);
E2) $x = y \ \Rightarrow \ (A(x/z) \Rightarrow A(y/z))$ (подстановочность равенства).

В аксиоме E2) под $A(z)$ понимается произвольная формула, выразимая над заданным алфавитом; переменные x и y свободны для z в $A(z)$. Выражения $A(x/z)$, $A(y/z)$, напомним, обозначают результат подстановки в $A(z)$ переменной x и, соответственно, y вместо z.

Теорема 3. *Во всякой эквациональной теории:*
1) $\vdash \forall x(x = x)$;
2) $\vdash \forall x \forall y(x = y \ \Rightarrow \ y = x)$;
3) $\vdash \forall x \forall y \forall z(x = y \wedge y = z \ \Rightarrow \ x = z)$.

$\lhd$ Утверждение 1) получается из E1) по правилу обобщения.

Для доказательства 2) возьмем в качестве $A(z)$ формулу $z = x$. Тогда из E2) получим $x = y \ \Rightarrow \ (x = x \Rightarrow y = x)$. Легко доказываемое правило перестановки посылок $A \Rightarrow (B \Rightarrow C) \ \vdash \ B \Rightarrow (A \Rightarrow C)$ приводит к $x = x \ \Rightarrow \ (x = y \Rightarrow y = x)$. Остается применить аксиому E1) и правила MP и Gen.

Для доказательства 3) возьмем в качестве $A(z)$ формулу $v = z$. Из E2) получим $x = y \ \Rightarrow \ (v = x \Rightarrow v = y)$. Пользуясь легко доказываемым правилом объединения посылок $A \Rightarrow (B \Rightarrow C) \ \vdash \ B \wedge A \Rightarrow C$, получим $v = x \wedge x = y \Rightarrow v = y$. Остается теперь применить правило Gen и правило переименования связанных переменных $\forall x A(x) \vdash \forall y A(y)$ (ср. пример 1). $\rhd$

Следствие 1. *Во всякой эквациональной теории для любых термов* t, t_1, t_2:
1) $\vdash (t = t)$;
2) $\vdash (t = t_1 \ \Rightarrow \ t_1 = t)$;
3) $\vdash (t = t_1 \wedge t_1 = t_2 \ \Rightarrow \ t = t_2)$.

Следствие 2. *Во всякой модели эквациональной теории предикат, соответствующий символу $=$, есть отношение эквивалентности.*

Если в модели эквациональной теории символу $=$ соответствует предикат тождественного равенства, то эта модель называется *нормальной*.

Теорема 4. *Во всякой эквациональной теории:*
1) $\vdash x_1 = y_1 \wedge \ldots \wedge x_n = y_n \;\Rightarrow\; t(x_1/z_1, \ldots, x_n/z_n) = t(y_1/z_1, \ldots, y_n/z_n)$*;*
2) $\vdash x_1 = y_1 \wedge \ldots \wedge x_n = y_n \;\Rightarrow$
$$\Rightarrow\; (A(x_1/z_1, \ldots, x_n/z_n) \Rightarrow A(y_1/z_1, \ldots, y_n/z_n));$$
где t *— произвольный терм,* A *— произвольная формула, а переменные* x_i, y_i *свободны для* z_i $(1 \leqslant i \leqslant n)$ *в* $t(z_1, \ldots, z_n)$ *и* $A(z_1, \ldots, z_n)$*.*

$\lhd$ Утверждение 1) докажем в случае $n = 1$: $x = y \;\Rightarrow\; t(x) = t(y)$, где $t(x)$ — это, конечно, $t(x/z)$. В качестве $A(z)$ в схеме аксиом E2) возьмем формулу $t(x) = t(z)$ и воспользуемся правилом перестановки посылок, следствием 1(1) и правилом MP.

Утверждение 2) в случае $n = 1$ совпадает с E2), а при $n = 2$ имеет вид: $x_1 = y_1 \wedge x_2 = y_2 \;\Rightarrow\; A(x_1, x_2) \Rightarrow A(y_1, y_2)$ и выводится из двух частных случаев схемы аксиом E2):

$$x_1 = y_1 \;\Rightarrow\; (A(x_1, x_2) \Rightarrow A(y_1, x_2)),$$
$$x_2 = y_2 \;\Rightarrow\; (A(y_1, x_2) \Rightarrow A(y_1, y_2))$$

путем применения правил

$$A_1 \Rightarrow B_1, A_2 \Rightarrow B_2 \;\vdash\; A_1 \wedge A_2 \Rightarrow B_1 \wedge B_2,$$
$$(A \Rightarrow B) \wedge (B \Rightarrow C) \;\vdash\; A \Rightarrow C$$

и транзитивности отношения выводимости.

Аналогично проводится доказательство для произвольного n. $\rhd$

Теорема 5. *Если эквациональная теория имеет модель, то она имеет и нормальную модель.*

$\lhd$ Пусть M — модель эквациональной теории, D — предметное множество, R — предикат, соответствующий символу «=» (т.е. $R = \;|=|_M$). Согласно следствию 2, R есть отношение эквивалентности на D, поэтому можно определить фактор-множество D/R, состоящее из классов эквивалентности $[\alpha]$ $(\alpha \in D)$. Определим новую интерпретацию M^* с предметным множеством D/R и отображением оценки $|\cdot|^*$, заданным для любой константы a, любого функционального символа f, любого предикатного символа P и символа «=» следующим образом:

1) $|=|^*$ есть предикат тождественного равенства;

2) если $|a| = \alpha \in D$, то $|a|^* = [\alpha]$;

3) если $|f| = \varphi$ — функция из D^n в D, то $|f|^* = \varphi^*$ — функция, определенная на классах эквивалентности следующим образом: $\varphi^*([\alpha_1], \ldots, [\alpha_n]) = [\varphi(\alpha_1, \ldots, \alpha_n)]$. Это определение не зависит от выбора представителей в классах, поскольку, согласно теореме 4(1), доказуема формула

$$x_1 = y_1 \wedge \ldots \wedge x_n = y_n \;\Rightarrow\; f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n),$$

что означает истинность на множестве D импликации

$$\alpha_1 R\beta_1 \wedge \ldots \wedge \alpha_n R\beta_n \Rightarrow \varphi(\alpha_1 \ldots \alpha_n) R\varphi(\beta_1 \ldots \beta_n);$$

4) если $|P| = \Phi$ — предикат на D^n, то $|P|^* = \Phi^*$ — предикат, определенный на классах эквивалентности следующим образом: $\Phi^*([\alpha_1], \ldots, [\alpha_n]) = \Phi(\alpha_1, \ldots, \alpha_n)$. Истинностное значение предиката Φ^* не зависит от выбора представителей в классах, поскольку, согласно теореме 4(2), доказуема формула

$$x_1 = y_1 \wedge \ldots \wedge x_n = y_n \;\Rightarrow\; (P(x_1, \ldots, x_n) \Rightarrow P(y_1, \ldots, y_n)),$$

что означает истинность на множестве D импликации

$$\alpha_1 R\beta_1 \wedge \ldots \wedge \alpha_n R\beta_n \Rightarrow (\Phi(\alpha_1 \ldots \alpha_n) \Leftrightarrow \Phi(\beta_1 \ldots \beta_n)).$$

Следующая лемма легко может быть доказана путем рассмотрения всех конструкций из определения терма и формулы логики первого порядка с учетом определенной выше интерпретации M^*.

Лемма. *Пусть M^s — расширение M при помощи последовательности $s = (s_1, s_2, \ldots)$, M^{*s} — расширение M^* при помощи последовательности $s^* = ([s_1], [s_2], \ldots)$. Тогда произвольная формула F выполнена в M^s тогда и только тогда, когда F выполнена в M^{*s}.*

Из леммы немедленно следует, что любая формула F истинна в M тогда и только тогда, когда она истинна в M^*; а так как M — модель нашей эквациональной теории, то, следовательно, M^* — ее нормальная модель. ▷

Описанная в доказательстве теоремы 5 процедура построения нормальной модели по произвольной модели называется *нормализацией*. Эта конструкция часто применяется в алгебре, геометрии и анализе, когда необходимо рассматривать фактор-объекты (примеры — модульная арифметика, тензорное произведение векторных пространств, проективные пространства, функциональные пространства L_p и т.д.).

3. Элементарные теории

Элементарной теорией некоторого класса математических систем называется формальная теория первого порядка, множество теорем которой совпадает с множеством истинных в системах этого класса формул, выразимых в этой теории. Во всех последующих примерах предполагается, что алфавит элементарной теории содержит символ

«=», а формулы E1), E2) являются схемами (эквациональных) аксиом этой теории; поэтому задание элементарной теории будет состоять в перечислении остальных символов и специальных аксиом.

I. *Элементарная теория групп* **G**. Содержит константу 1, бинарный функциональный символ $\cdot$ и аксиомы

$$\begin{array}{ll} \text{G1)} & x \cdot (y \cdot z) = (x \cdot y) \cdot z; \\ \text{G2)} & x \cdot 1 = x; \\ \text{G3)} & \forall x \exists y (x \cdot y = 1). \end{array}$$

Добавив аксиому

$$\text{G4)} \quad x \cdot y = y \cdot x,$$

получим элементарную теорию абелевых групп.

II. *Элементарная теория полей* **F**. Содержит константы 0 и 1, бинарные функциональные символы $+$ и $\cdot$ и аксиомы

$$\begin{array}{llll} \text{F1)} & x + (y + z) = (x + y) + z; & \text{F5)} & x \cdot (y \cdot z) = (x \cdot y) \cdot z; \\ \text{F2)} & x + 0 = x; & \text{F6)} & x \cdot 1 = x; \\ \text{F3)} & \forall x \exists y (x + y = 0); & \text{F7)} & x \cdot (y + z) = x \cdot y + x \cdot z; \\ \text{F4)} & x + y = y + x; & \text{F8)} & x \cdot y = y \cdot x; \\ & & \text{F9)} & x \neq 0 \Rightarrow \exists y (x \cdot y = 1). \end{array}$$

Заметим, что, если действовать строго в соответствии с определениями, то надо использовать предметные символы a_1 и a_2, функциональные символы f_1, f_2, предикатный символ P_1 и записывать аксиому F2), например, так: $P_1(f_1(x, a_1), x)$, а аксиому F9) следующим образом: $\neg P_1(x, a_1) \Rightarrow \exists y (P_1(f_2(x, y), a_2))$.

Удобно использовать, кроме общепринятых основных символов, некоторые символы сокращений: например, формула $t_1 \neq t_2$ есть сокращение для $\neg(t_1 = t_2)$.

III. *Элементарная теория частично упорядоченных множеств* **O**. Содержит бинарный предикатный символ $<$ и аксиомы

$$\begin{array}{ll} \text{O1)} & \neg(x < x); \\ \text{O2)} & x < y \wedge y < z \Rightarrow x < z. \end{array}$$

В этой теории приняты сокращения:

$$\begin{array}{l} t_1 \leqslant t_2 \text{ для } t_1 < t_2 \vee t_1 = t_2; \\ t_1 > t_2 \text{ для } t_2 < t_1; \\ t_1 \geqslant t_2 \text{ для } t_2 < t_1 \vee t_1 = t_2, \end{array}$$

с помощью которых можно записать теорему теории **O**:

$$x \leqslant y \Rightarrow \neg(x > y).$$

Формула $\forall y(x \leqslant y)$ выражает предикат «наименьший элемент». Приняв для этой формулы сокращенное обозначение $M(x)$, можно записать еще одну теорему теории **O**:

$$M(x) \wedge M(y) \Rightarrow x = y.$$

Нормальными моделями теорий $\mathbf{G}, \mathbf{F}, \mathbf{O}$ в точности являются все группы, все поля, все частично упорядоченные множества. Существуют и ненормальные модели.

Пример 3. Рассмотрим следующую интерпретацию множества формул теории **F**: в качестве предметного множества возьмем множество целых чисел, символам 0, 1, $+$, $\cdot$ припишем их обычный смысл, а символу «$=$» назначим предикат сравнимости по некоторому фиксированному модулю $m > 1$. Нетрудно показать, что в этой интерпретации истинны все формулы E1) и E2) (для любой формулы A, выразимой в теории **F**), формулы F1)–F8), а при простом m также и F9). Таким образом, если m — простое число, эта интерпретация является ненормальной моделью теории **F**; нормализация приводит к полю классов вычетов по модулю m.

IV. *Элементарная арифметика* **A**. Содержит константу 0, унарный функциональный символ $'$, бинарные функциональные символы $+$ и $\cdot$ и аксиомы

A1) $x' \neq 0$;
A2) $x' = y' \Rightarrow x = y$;
A3) $x + 0 = x$;
A4) $x + y' = (x + y)'$;
A5) $x \cdot 0 = 0$;
A6) $x \cdot y' = x \cdot y + x$;
A7) $A(0) \wedge \forall x(A(x) \Rightarrow A(x')) \Rightarrow \forall x A(x)$,

причем последняя определяет не аксиому, а схему аксиом с произвольной формулой $A(x)$ теории **A** (схему аксиом *индукции*).

Рассмотрим интерпретацию ω множества формул теории **A**, в которой предметным множеством является множество натуральных чисел, а символам $=$, 0, $'$, $+$, $\cdot$ отвечают соответственно равенство, нуль, прибавление единицы, сложение и умножение. Все аксиомы теории **A**, включая эквациональные, в интерпретации ω оказываются истинными, и, в силу очевидного свойства выводимости сохранять истинность, все теоремы теории **A** истинны в интерпретации ω. Поэтому ω является (нормальной) моделью элементарной арифметики. Аксиомы A1)–A7) выбраны так, чтобы все обычные факты, истинные в ω и выразимые в теории **A**, были бы доказуемы в **A**. Это объясняет принятое для ω название — *стандартная* модель элементарной арифметики.

Пример 4. Докажем $\vdash\ 0 + x = x$. Используем схему аксиом индукции, выбрав в качестве $A(x)$ формулу $0 + x = x$.

1. $0 + 0 = 0$ (из A3) с помощью Gen и Q1) при $t = 0$).
2. $0 + x' = (0 + x)'$ (аналогично из A4).
3. $0 + x = x \Rightarrow 0 + x' = x'$ (аналогично из 2 и E2).
4. $0 + 0 = 0 \wedge \forall x(0 + x = x \Rightarrow 0 + x' = x')$ (1 и Gen, 3).
5. $\forall x(0 + x = x)$ (1, 4 и A7).
6. $0 + x = x$ (Q1 и MP).

Упражнение 1. Пусть 1 обозначает терм $0'$, 2 — $0''$, 4 — $0''''$. Докажите в элементарной арифметике:

1) $2 \neq 4$; 3) $x' = x + 1$;
2) $x' \neq x$; 4) $(x + y) + z = x + (y + z)$.

Формальная теория T называется *полной*, если для всякого предложения F, выразимого в этой теории, справедливо $T \vdash F$ или $T \vdash \neg F$. Формальная теория T называется *разрешимой*, если существует алгоритм, позволяющий для любого предложения F определить, верно $T \vdash F$ или нет. Формальная теория T называется *категоричной*, если она имеет единственную с точностью до изоморфизма модель.

Элементарная арифметика является неполной, неразрешимой и некатегоричной теорией.

Хотя очень не просто привести пример истинного в ω, но не доказуемого в **A** утверждения, такие примеры существуют.

В заключение приведем пример формальной теории второго порядка. В логике второго порядка, помимо предметных переменных, допускаются функциональные и предикатные переменные и кванторы по таким переменным.

V. *Формальная арифметика второго порядка* $\mathbf{A}_2$. Содержит:

1) два сорта переменных: переменные для натуральных чисел $x, y, z, \ldots$ (сорт 0) и переменные для подмножеств множества ω натуральных чисел $X, Y, Z, \ldots$ (сорт 1);

2) символы элементарной арифметики $=$, 0, $'$, $+$, $\cdot$, а также новый предикатный символ $\in$, связывающий объекты сорта 0 и сорта 1;

3) все аксиомы элементарной арифметики с той лишь разницей, что в схеме аксиом индукции в качестве формулы $A(x)$ можно брать

теперь любую формулу, выразимую в $\mathbf{A}_2$; а также новую схему аксиом *свертывания*:

$$\text{A8)} \quad \exists X\, \forall x\, (x \in X \Leftrightarrow A(x)),$$

где X не входит свободно в $A(x)$.

Некоторые сокращенные обозначения теории $\mathbf{A}_2$:

$$\begin{array}{lll} X \subset Y & \text{есть} & \forall x\,(x \in X \Rightarrow x \in Y); \\ X = Y & \text{есть} & \forall x\,(X \subset Y \wedge Y \subset X); \\ X = \{x|A(x)\} & \text{есть} & \forall x\,(x \in X \Leftrightarrow A(x)). \end{array}$$

Таким образом, в арифметике второго порядка появляется возможность выражать в виде формул и доказывать утверждения о множествах натуральных чисел.

Список литературы

Учебники

1. Гильберт Д., Аккерман В. Основы теоретической логики. М.: Иностр. лит., 1947.

2. Гладкий А.В. Математическая логика. М.: Изд-во Рос. гос. гум. ун-та, 1998.

3. Гудстейн Р.Л. Математическая логика. М.: Иностр. лит., 1961.

4. Ершов Ю.Л., Палютин Е.А. Математическая логика. М.: Наука, 1979.

5. Клини С.К. Математическая логика. М.: Мир, 1973.

6. Колмогоров А.Н., Драгалин А.Г. Введение в математическую логику. М.: МГУ, 1982.

7. Колмогоров А.Н., Драгалин А.Г. Математическая логика. Дополнительные главы. М.: МГУ, 1984.

8. Мендельсон Э. Введение в математическую логику. М.: Наука, 1976.

9. Новиков П.С. Элементы математической логики. М.: Наука, 1973.

10. Черч А. Введение в математическую логику. Т.I. М.: Иностр. лит., 1960.

11. Шенфилд Дж. Математическая логика. М.: Наука, 1975.

Задачники

12. Гиндикин С.Г. Алгебра логики в задачах. М.: Наука, 1972.

13. Лавров И.А., Максимова Л.Л. Задачи по теории множеств, математической логике и теории алгоритмов. М.: Наука, 1984.

Содержание