# Майнор «Логика»
# НИУ ВШЭ, осень 2017 г.

Л.Д. Беклемишев

## 1 Логика высказываний

### 1.1 Алфавит, буква, слово

**Определение 1.1.** *Алфавитом* будем называть любое непустое множество. Его элементы называются *символами* (*буквами*).

**Определение 1.2.** *Словом* в алфавите $\Sigma$ называется конечная последовательность элементов $\Sigma$.

**Пример 1.3.** Рассмотрим алфавит $\Sigma = \{a, b, c\}$. Тогда $baaa$ является словом в алфавите $\Sigma$.

**Определение 1.4.** Слово, не содержащее ни одного символа (то есть последовательность длины 0), называется *пустым словом* и обозначается $\varepsilon$.

**Определение 1.5.** *Длина* слова $w$, обозначаемая $|w|$, есть число символов в $w$, причём каждый символ считается столько раз, сколько раз он встречается в $w$.

**Определение 1.6.** Если $x$ и $y$ — слова в алфавите $\Sigma$, то слово $xy$ (результат приписывания слова $y$ в конец слова $x$) называется *конкатенацией* слов $x$ и $y$.

**Определение 1.7.** Если $x$ — слово и $n \in \mathbb{N}$, то через $x^n$ обозначается слово

$$\underbrace{xx\dots x}_{n\text{ раз}}.$$

Положим $x^0 \rightleftharpoons \varepsilon$ (знак $\rightleftharpoons$ читается «равно по определению»).

**Пример 1.8.** По принятым соглашениям $ba^3 = baaa$ и $(ba)^3 = bababa$.

**Определение 1.9.** Множество всех слов в алфавите $\Sigma$ обозначается $\Sigma^*$.

**Определение 1.10.** Подмножества множества $\Sigma^*$ для некоторого алфавита $\Sigma$ называются *словарными множествами*. В лингвистике и информатике словарные множества также часто называют *языками*.

**Утверждение 1.11.** *Если алфавит $\Sigma$ конечен или счётен, то множество $\Sigma^*$ счётно.*

В самом деле, для любого конечного подмножества $\Sigma_0 \subseteq \Sigma$ множество всех слов фиксированной длины в алфавите $\Sigma_0$ конечно. Следовательно, $\Sigma_0^*$ является объединением счётного числа конечных множеств, а значит, таково и множество $\Sigma^* = \bigcup_{\Sigma_0 \subseteq \Sigma} \Sigma_0^*$.

## 1.2 Высказывания и логические операции

Логика высказываний формализует определённые представления о (реальных) высказываниях и логических операциях.

**Определение 1.12.** *Высказыванием* называется повествовательное предложение, для которого имеет смысл говорить о его истинности или ложности.

**Пример 1.13.** Предложение «Лиссабон — столица Испании» является высказыванием.

**Определение 1.14.** Существуют два *истинностных значения* — «истина» и «ложь». Мы будем обозначать их И и Л, соответственно; считаем 1 и 0 синонимами И и Л.

Некоторые сложные высказывания строятся из более простых с помощью *логических операций*, таких как отрицание «не», конъюнкция «и», дизъюнкция «или», импликация «если ..., то ...».

**Определение 1.15.** *Логическая операция* — это такой способ построения сложного высказывания из данных высказываний, при котором истинностное значение сложного высказывания полностью определяется истинностными значениями исходных высказываний.

**Пример 1.16.** Отрицание является логической операцией. Предложение «Неверно, что Лиссабон — столица Испании» построено из высказывания «Лиссабон — столица Испании» с помощью отрицания.

**Замечание 1.17.** Употребляемую в естественном языке импликацию «если $A$, то $B$» нельзя в полной мере считать логической операцией, поскольку она, среди прочего, указывает и на причинно-следственную связь между высказываниями $A$ и $B$, то есть не выражается только лишь через истинностные значения высказываний $A$ и $B$. Более того, высказывание «если $A$, то $B$» *полисемично*, то есть может пониматься по-разному в разных контекстах.

В математическом языке используется *материальная импликация*, которая является логической связкой. При этом высказывание «если $A$, то $B$» считается ложным в том и *только том* случае, если $A$ истинно и $B$ ложно.

## 1.3 Синтаксис логики высказываний

### 1.3.1 Переменные и связки

Пусть задан некоторый алфавит Var символов, называемых *пропозициональными*[1] *переменными*. Пропозициональные переменные будем обозначать буквами $P$, $Q$ и т. д. (возможно, с индексами). Интуитивно, пропозициональные переменные интерпретируются как высказывания.

Знаки $\neg$, $\wedge$, $\vee$, $\rightarrow$ (и аналогичные знаки, которые будут введены позже) называются *пропозициональными связками* или *булевыми связками*. Интуитивно, связки интерпретируются как логические операции (соответственно, как отрицание, конъюнкция, дизъюнкция, импликация).

### 1.3.2 Формулы

Формулы логики высказываний являются словами в алфавите, состоящем из пропозициональных переменных, пропозициональных связок и скобок: ( и ). Множество всех формул индуктивно определяется следующим образом.

**Определение 1.18.** *Множество формул* Fm логики высказываний порождается из множества Var по следующим правилам:

1. Если $P \in \mathrm{Var}$, то $P$ — формула.

[1] Propositio (лат.) = предложение.

2. Если $A$ — формула, то $\neg A$ — формула.

3. Если $A$ и $B$ — формулы, то $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ — формулы.

Другими словами, множество формул есть наименьшее множество, замкнутое относительно этих трёх правил.

**Определение 1.19.** *Построением* формулы $A$ называем последовательность формул, каждый элемент которой есть либо переменная, либо получается из предыдущих по правилам 2 или 3, и последний элемент которой есть $A$.

Смысл определения 1.18 состоит в том, что формулами считаются те и только те слова, которые имеют построение. Определение множества объектов как наименьшего множества, замкнутого относительно некоторых правил образования, называется *индуктивным.* Такого рода определения часто используются в алгебре и логике.

**Пример 1.20.** Последовательность $P$, $Q$, $(P \to Q)$, $(Q \wedge (P \to Q))$ есть построение формулы $(Q \wedge (P \to Q))$.

Формулы логики высказываний будем обозначать буквами $A$, $B$ и т. д. (возможно, с индексами).

**Определение 1.21.** *Подформулами* формулы $A$ называются все те формулы, которые входят в любое построение $A$. Подформула формулы $A$, отличная от самой формулы $A$, называется *собственной подформулой* формулы $A$.

**Замечание 1.22.** Не следует путать подформулы с их *вхождениями* в формулу. Одна и та же подформула может иметь несколько вхождений, например подформула $P$ входит три раза в формулу $(P \to (P \wedge P))$.

**Предложение 1.23 (однозначность разбора,** без доказательства**).**
*Каждая пропозициональная формула, не являющаяся переменной, может быть представлена единственным образом как* $\neg A$, $(A \wedge B)$, $(A \vee B)$ *или* $(A \to B)$.

Доказательство этого утверждения основывается на соображениях баланса скобок в формуле. Следствием является, например, тот факт, что множество подформул данной формулы не зависит от её построения и совпадает с множеством всех подслов данной формулы, являющихся формулами.

### 1.3.3 Сокращённая запись формул

Для удобства записи формул принято использовать некоторые сокращения. С формальной точки зрения, такие сокращения являются приёмами изложения, а не элементами языка логики высказываний. Мы рассмотрим два важных вида сокращений.

А. *Соглашения о скобках.*

Во-первых, можно опустить внешнюю пару скобок. Например, запись $P \to (Q \to P)$ обозначает формулу $(P \to (Q \to P))$.

Во-вторых, если в сокращённой записи рядом находятся две операции $\wedge$, то при отсутствии скобок внутренней считается та, которая находится левее. Другими словами, связка $\wedge$ считается *левоассоциативной*. Например, $P \wedge Q \wedge R$ и $(P \wedge Q) \wedge R$ обозначают одну и ту же формулу (длина этой формулы — 9 символов). Однако в записи $P \wedge (Q \wedge R)$ ни одной скобки опустить нельзя. Связка $\vee$ тоже является левоассоциативной, но связка $\to$ не является ни левоассоциативной, ни правоассоциативной (в этом курсе).

В-третьих, если в сокращённой записи рядом находятся разные связки, то при отсутствии скобок внутренней считается та, которая имеет более высокий приоритет согласно следующему списку, составленному в порядке убывания приоритетов: $\neg$, $\wedge$, $\vee$, $\to$. Иными словами, связки с более высоким приоритетом связывают сильнее.

Разрешается также добавить внешнюю пару скобок. Например, запись $(\neg P)$ обозначает формулу $\neg P$. Добавление скобок пригодится, например, в определении 1.44.

Б. *Введение новых логических связок.*

Логическую связку *эквивалентности* $\leftrightarrow$ часто определяют как сокращение. При этом для любых формул $A, B$ запись $A \leftrightarrow B$ понимается как обозначение для формулы $(A \to B) \wedge (B \to A)$. Аналогичным образом можно ввести и другие логические связки, в частности:

$$
\begin{aligned}
\bot &\rightleftharpoons (P_0 \wedge \neg P_0), \quad \text{где } P_0 \text{ — фиксированная переменная;} \\
\top &\rightleftharpoons \neg\bot; \\
\bigwedge_{i=1}^{n} A_i &\rightleftharpoons (A_1 \wedge A_2 \wedge \cdots \wedge A_n); \\
\bigvee_{i=1}^{n} A_i &\rightleftharpoons (A_1 \vee A_2 \vee \cdots \vee A_n).
\end{aligned}
$$

### 1.3.4 Другие варианты синтаксиса

Помимо стандартного, изложенного выше, способа записи формул логики высказываний существуют и другие варианты. Отметим три важных способа представления формул.

А. *Польская запись.* Логические связки (как унарные, так и бинарные) записываются префиксным образом, например, вместо $(A \wedge B)$ пишем $\wedge AB$; при этом скобки не употребляются. Так, формула $(A \to (B \wedge C))$ может быть записана «по-польски» как $\to A \wedge BC$. (Почему для польской записи имеет место теорема об однозначности разбора?)

Б. *Представление формул деревьями.* С каждой формулой можно однозначно связать бинарное дерево, называемое иногда *деревом разбора*, листья которого помечены пропозициональными переменными, а внутренние вершины – связками. Вершины этого дерева находятся во взаимно-однозначном соответствии со вхождениями подформул в данную формулу (соответетвующей корню дерева).

Интересно отметить, что одна из первых формулировок логики высказваний, данная в XIX веке немецким учёным Г. Фреге, использовала вариант графического изображения деревьев в качестве записи формул. (Напрашивается сравнение с иероглифическим письмом.)

В. *Представление формул ориентированными ациклическими графами.* Если отождествить в дереве разбора формулы вершины, соответствующие вхождениям одной и той же подформулы, то получится структура, называемая ориентированным ациклическим графом (DAG). При таком представлении вершины графа соответствуют подформулам данной формулы, а стрелки соединяют каждые две подформулы, одна из которых является максимальной собственной подформулой другой. Этот способ представления формул является наиболее экономным и распостранённым вариантом представления формул в памяти компьютера.

## 1.4 Таблицы истинности

**Определение 1.24.** Обозначим $\mathbb{B} \rightleftharpoons \{\text{И}, \text{Л}\} \rightleftharpoons \{0, 1\}$. Функции $f : \mathbb{B}^n \to \mathbb{B}$ называются *булевыми функциями.*

**Определение 1.25.** *Оценкой пропозициональных переменных* (или просто *оценкой*) называется произвольная функция $f : \mathrm{Var} \to \mathbb{B}$.

**Определение 1.26.** *Истинностное значение* (или просто *значение*) формулы при данной оценке $f$ определяется индукцией по построению формулы в соответствии со следующими таблицами.

| $A$ | $\neg A$ |
|---|---|
| Л | И |
| И | Л |

| $A$ | $B$ | $A \wedge B$ | $A \vee B$ | $A \to B$ |
|---|---|---|---|---|
| Л | Л | Л | Л | И |
| Л | И | Л | И | И |
| И | Л | Л | И | Л |
| И | И | И | И | И |

С формальной точки зрения, оценка $f : \mathrm{Var} \to \mathbb{B}$ продолжается до функции $f : \mathrm{Fm} \to \mathbb{B}$, определённой на множестве всех формул, по следующим правилам.

$$\begin{aligned} f(\neg A) = \text{И} &\iff f(A) = \text{Л}; \\ f(A \wedge B) = \text{И} &\iff f(A) = \text{И и } f(B) = \text{И}; \\ f(A \vee B) = \text{И} &\iff f(A) = \text{И или } f(B) = \text{И}; \\ f(A \to B) = \text{И} &\iff f(A) = \text{Л или } f(B) = \text{И}. \end{aligned}$$

Если $f(A) = \text{И}$, то говорят, что формула $A$ *истинна* при оценке $f$. Иначе формула $A$ *ложна* при данной оценке.

Специально рассмотрим случай, когда число переменных конечно, то есть $\mathrm{Var} = \{P_1, \ldots, P_n\}$. Оценка $f$ определяется набором своих истинностных значений на переменных $P_1, \ldots, P_n$. Данному набору $\vec{x} = (x_1, \ldots, x_n) \in \mathbb{B}^n$ сопоставим оценку $f_{\vec{x}}$, определяемую таблицей

| $P_1$ | $P_2$ | $\ldots$ | $P_n$ |
|---|---|---|---|
| $x_1$ | $x_2$ | $\ldots$ | $x_n$ |

Таким образом, существует взаимно-однозначное соответствие между оценками и наборами из $\mathbb{B}^n$.

**Определение 1.27.** *Таблицей истинности* (или *истинностной таблицей*) формулы $A$ над переменными $P_1, \ldots, P_n$ называется таблица, указывающая значения формулы $A$ при всех возможных оценках переменных $P_1, \ldots, P_n$. (Существует $2^n$ таких оценок, каждая из них записывается в отдельной строке. Обычно оценки $f_{\vec{x}}$ упорядочены в соответствии с лексикографическим порядком на наборах $\vec{x}$.)

**Пример 1.28.**

| $P_1$ | $P_2$ | $P_1 \leftrightarrow P_2$ |
|---|---|---|
| Л | Л | И |
| Л | И | Л |
| И | Л | Л |
| И | И | И |

Таким образом, таблица истинности формулы $A$ над $n$ переменными задаёт булеву функцию $\varphi_A : \mathbb{B}^n \to \mathbb{B}$. Функция $\varphi_A$ определяется равенством
$$\varphi_A(\vec{x}) = f_{\vec{x}}(A),$$
верным для всех наборов $\vec{x} \in \mathbb{B}^n$.

## 1.5 Функциональная полнота

Всякую ли булеву функцию можно задать некоторой формулой? Ответ даёт следующая теорема.

**Теорема 1.29 (о функциональной полноте).** *Для любой функции $\varphi : \mathbb{B}^n \to \mathbb{B}$ найдётся такая формула $A$ от $n$ переменных, что $\varphi = \varphi_A$. При этом можно считать, что $A$ содержит лишь связки $\neg$ и $\vee$.*

Эта теорема показывает, что известных нам логических операций $\vee$, $\neg$ в принципе достаточно, чтобы определить все возможные логические операции.

**Доказательство.** Равенство $\varphi = \varphi_A$ означает, что для всех $\vec{x} \in \mathbb{B}^n$
$$\varphi(\vec{x}) = \varphi_A(\vec{x}) = f_{\vec{x}}(A).$$

Для $x \in \mathbb{B}$ положим
$$P^x = \begin{cases} P, & \text{если } x = \text{И}; \\ \neg P, & \text{если } x = \text{Л}. \end{cases}$$

Для произвольного $\vec{x} = (x_1, \ldots, x_n) \in \mathbb{B}^n$ обозначим
$$A_{\vec{x}} \rightleftharpoons \bigwedge_{i=1}^{n} P_i^{x_i}.$$
Легко видеть, что формула $A_{\vec{x}}$ истинна лишь при оценке $f_{\vec{x}}$. Другими словами, для любой оценки $f$
$$f(A_{\vec{x}}) = \text{И} \iff f = f_{\vec{x}}. \tag{1}$$

Для данной функции $\varphi$ пусть список $\vec{x}_1, \ldots, \vec{x}_m$ исчерпывает все наборы $\vec{x} \in \mathbb{B}^n$ для которых $\varphi(\vec{x}) = \text{И}$, то есть
$$\varphi(\vec{x}) = \text{И} \iff \exists j\ \vec{x} = \vec{x}_j. \tag{2}$$

Положим теперь
$$A \rightleftharpoons \bigvee_{j=1}^{m} A_{\vec{x}_j},$$
тогда
$$\begin{aligned} f_{\vec{x}}(A) = \text{И} \quad &\iff \quad \exists j \ f_{\vec{x}}(A_{\vec{x}_j}) = \text{И} \\ &\iff \quad \exists j \ \vec{x} = \vec{x}_j \quad \text{по (1)} \\ &\iff \quad \varphi(\vec{x}) = \text{И} \quad \text{по (2).} \end{aligned}$$

Заметим теперь, что конъюнкция выражается через дизъюнкцию и отрицание, поскольку формула $A \wedge B$ равносильна $\neg(\neg A \vee \neg B)$ (см. ниже раздел 1.7). Поэтому, формулы $A_{\vec{x}}$ могут быть переписаны без использования знака $\wedge$. ⊠

## 1.6 Выполнимые формулы, тавтологии, логическое следование

### 1.6.1 Выполнимые формулы и тавтологии

**Определение 1.30.** Пропозициональная формула, истинная хотя бы при одной оценке пропозициональных переменных, называется *выполнимой*. Множество формул $\Gamma$ называется *выполнимым*, если существует оценка $f$, при которой истинны одновременно все формулы из $\Gamma$.

**Определение 1.31.** Пропозициональная формула, истинная при каждой оценке пропозициональных переменных, называется *тавтологией* (*тождественно истинной*).

Важность понятия тавтологии с точки зрения оснований математики (и логики в целом) состоит в том, что они выражают *универсальные законы* логики, верные независимо от содержания составляющих их высказываний. Запись $\models A$ выражает тот факт, что $A$ — тавтология.

**Определение 1.32.** Пропозициональная формула, ложная при каждой оценке пропозициональных переменных, называется *тождественно ложной*.

**Предложение 1.33.** *Следующие условия равносильны.*

(i) *Формула $A$ тождественно ложна.*

(ii) *Формула $A$ не является выполнимой.*

(iii) *Формула* $\neg A$ *— тавтология.*

**Доказательство.** Предложение непосредственно следует из определений. ⊠

### 1.6.2 Проверка формулы на выполнимость

В приложениях часто встречается задача проверки пропозициональной формулы на выполнимость. Наиболее прямолинейный алгоритм её решения состоит в построении всей таблицы истинности формулы, то есть перебора $2^n$ всех возможных оценок. Этот алгоритм работает экспоненциальное число шагов от числа переменных исходной формулы. Существуют более изощрённые и несколько более эффективные алгоритмы решения этой задачи, однако все они имеют экспоненциальную нижнюю оценку сложности.

Важной открытой проблемой является вопрос о существовании полиномиального по числу шагов алгоритма решения этой задачи. Поскольку выполнимость пропозициональной формулы является классическим примером так называемой NP-полной задачи, этот вопрос эквивалентен знаменитой проблеме P=NP? — одной из самых важных открытых математических проблем. В настоящее время доминирует гипотеза о том, что такого полиномиального алгоритма не существует.

### 1.6.3 Логическое следование

**Определение 1.34.** Пусть $\Gamma$ — некоторое множество формул логики высказываний и $A$ — формула логики высказываний. Говорят, что формула $A$ *логически следует* (или *семантически следует*) из множества $\Gamma$ (обозначение $\Gamma \vDash A$), если формула $A$ истинна при каждой оценке пропозициональных переменных, при которой истинны все формулы из $\Gamma$.

**Пример 1.35.** $\{P \vee Q, R, \neg Q\} \vDash P \wedge R$.

**Предложение 1.36.** $\{B_1, \ldots, B_n\} \vDash A$ *тогда и только тогда, когда формула* $(\bigwedge_{i=1}^n B_i) \to A$ *является тавтологией. В частности, формула* $A$ *— тавтология, если и только если* $A$ *логически следует из пустого множества формул.*

## 1.7 Равносильные формулы в логике высказываний

**Определение 1.37.** Формулы $A$ и $B$ называются *равносильными* (*эквивалентными*), обозначение $A \equiv B$, если при каждой оценке пропозициональных переменных значение $A$ совпадает со значением $B$. Другими словами, если $\varphi_A = \varphi_B$.

**Пример 1.38.** $P \to Q \equiv \neg Q \to \neg P$; $P \to Q \not\equiv \neg P \to \neg Q$.

Непосредственно из определений вытекают следующие факты.

**Утверждение 1.39.** (i) *Отношение $\equiv$ рефлексивно, симметрично и транзитивно.*

(ii) *Формулы $A$ и $B$ равносильны тогда и только тогда, когда формула $A \leftrightarrow B$ является тавтологией.*

(iii) *Формула $A$ — тавтология тогда и только тогда, когда $A \equiv \top$.*

**Основные равносильности:**

| | | | | | |
|---|---|---|---|---|---|
| $A \wedge B$ | $\equiv$ | $B \wedge A$ | $A \vee B$ | $\equiv$ | $B \vee A$ |
| $A \wedge (B \wedge C)$ | $\equiv$ | $(A \wedge B) \wedge C$ | $A \vee (B \vee C)$ | $\equiv$ | $(A \vee B) \vee C$ |
| $A \wedge A$ | $\equiv$ | $A$ | $A \vee A$ | $\equiv$ | $A$ |
| $A \wedge (B \vee C)$ | $\equiv$ | $(A \wedge B) \vee (A \wedge C)$ | $A \vee (B \wedge C)$ | $\equiv$ | $(A \vee B) \wedge (A \vee C)$ |
| $A \vee (A \wedge B)$ | $\equiv$ | $A$ | $A \wedge (A \vee B)$ | $\equiv$ | $A$ |
| $\neg(A \wedge B)$ | $\equiv$ | $\neg A \vee \neg B$ | $\neg(A \vee B)$ | $\equiv$ | $\neg A \wedge \neg B$ |
| $\neg\neg A$ | $\equiv$ | $A$ | $A \to B$ | $\equiv$ | $\neg A \vee B$ |

**Упражнение 1.40.** Равносильны ли формулы $P \to (Q \to R)$ и $(P \to Q) \to R$? Ответ: Нет. Рассмотрим такую оценку $g$, что $g(P) = g(Q) = g(R) = \text{Л}$.

**Упражнение 1.41.** Равносильны ли формулы $P \to (Q \to R)$ и $(P \wedge Q) \to R$? Ответ: Да.

**Замечание 1.42.** В задаче на упрощение формулы необходимо найти равносильную, но более короткую формулу. При этом длина понимается как общее количество всех вхождений символов в формулу.

**Упражнение 1.43.** *Упростить формулы:*

(i) $(P \leftrightarrow Q) \to P$. *Ответ:* $P \vee Q$.

(ii) $\neg P \to \neg Q$. *Ответ:* $Q \to P$.

(iii) $(P \vee Q) \wedge (P \vee R) \wedge (Q \vee R \vee \neg P)$. *Ответ:* $(P \vee (Q \wedge R)) \wedge (Q \vee R)$.

## 1.8 Правила подстановки и замены подформулы на эквивалентную

Для доказательства равносильности формул, помимо основных равносильностей, перечисленных в таблице, и правил, соответствующих рефлексивности, симметричности и транзитивности отношения $\equiv$, мы пользуемся правилами подстановки и замены на подформулы на эквивалентную.

**Определение 1.44.** Если $C$ и $D$ — формулы, а $P$ — пропозициональная переменная, то через $C[P/D]$ обозначим результат подстановки формулы $D$ вместо $P$ в формулу $C$.

Формальное определение даётся с помощью индукции по построению формулы $C$.

$$\begin{array}{l}
P[P/D] \rightleftharpoons D, \\
Q[P/D] \rightleftharpoons Q, \text{ если } Q \text{ — переменная, отличная от } P, \\
(\neg A)[P/D] \rightleftharpoons \neg(A[P/D]), \\
(A \wedge B)[P/D] \rightleftharpoons (A[P/D] \wedge B[P/D]), \\
(A \vee B)[P/D] \rightleftharpoons (A[P/D] \vee B[P/D]), \\
(A \to B)[P/D] \rightleftharpoons (A[P/D] \to B[P/D]).
\end{array}$$

**Пример 1.45.** Пусть $C = (P_1 \to P_2) \to P_2$ и $D = P_3 \to P_2$. Тогда

$$C[P_2/D] = (P_1 \to (P_3 \to P_2)) \to (P_3 \to P_2).$$

**Теорема 1.46 (о подстановке).** *Если $A$ — тавтология, $B$ — произвольная формула, а $P$ — пропозициональная переменная, то $A[P/B]$ — тавтология.*

**Доказательство.** Рассмотрим произвольную оценку $g$. Обозначим через $g'$ оценку, полученную из $g$ присвоением переменной $P$ значения $g(B)$. Индукцией по построению $C$ можно доказать, что $g(C[P/B]) = g'(C)$ для любой формулы $C$. Положим $C = A$. Так как формула $A$ истинна при оценке $g'$, то формула $A[P/B]$ истинна при оценке $g$. ⊠

**Пример 1.47.** Для любой формулы $B$ формула $B \vee \neg B$ является тавтологией. Например, формула $(P_3 \leftrightarrow P_1) \vee \neg(P_3 \leftrightarrow P_1)$ является тавтологией.

**Теорема 1.48.** *Пусть $A$, $B$, $C$ — формулы, а $P$ — пропозициональная переменная. Если $A \equiv B$, то $A[P/C] \equiv B[P/C]$.*

**Доказательство.** Пусть $A \equiv B$. В силу 1.39 $A \leftrightarrow B$ — тавтология. По теореме 1.46 $(A \leftrightarrow B)[P/C]$ — тавтология. Из определений следует, что $(A \leftrightarrow B)[P/C]$ совпадает с $A[P/C] \leftrightarrow B[P/C]$. В силу 1.39 $A[P/C] \equiv B[P/C]$. ⊠

**Пример 1.49.** Пусть $A = (P_1 \to P_2) \to P_2$, $B = P_1 \vee P_2$, $C = P_3 \to P_2$. Так как $(P_1 \to P_2) \to P_2 \equiv P_1 \vee P_2$, то $(P_1 \to (P_3 \to P_2)) \to (P_3 \to P_2) \equiv P_1 \vee (P_3 \to P_2)$.

**Лемма 1.50.** *Если $A \equiv B$, то $\neg A \equiv \neg B$. Если $A_1 \equiv B_1$ и $A_2 \equiv B_2$, то $A_1 \wedge A_2 \equiv B_1 \wedge B_2$, $A_1 \vee A_2 \equiv B_1 \vee B_2$, $A_1 \to A_2 \equiv B_1 \to B_2$.*

**Теорема 1.51 (о замене подформулы на эквивалентную).** *Пусть $A, B, C$ — формулы, а $P$ — пропозициональная переменная. Если $A \equiv B$, то $C[P/A] \equiv C[P/B]$.*

**Доказательство.** Теорема доказывается индукцией по построению формулы $C$. ⊠

**Пример 1.52.** Пусть $A = Q \vee Q$, $B = Q$, $C = P \wedge R$. Так как $Q \vee Q \equiv Q$, то $(Q \vee Q) \wedge R \equiv Q \wedge R$.

**Пример 1.53.** Существуют ли такие выполнимые формулы $A$ и $B$, что формула $A[P_1/B]$ не является выполнимой? Ответ: Да. Например, $A = \neg P_1$, $B = P_2 \vee \neg P_2$.

## 1.9 Нормальные формы

### 1.9.1 Дизъюнктивные и конъюнктивные нормальные формы

**Определение 1.54.** *Литералами* называются переменные и их отрицания.

**Пример 1.55.** Формулы $P_3$ и $\neg P_1$ являются литералами, а формулы $P_3 \vee P_1$ и $\neg\neg P_3$ — не являются.

**Определение 1.56.** *Элементарной конъюнкцией* называем формулу вида $\bigwedge_{i=1}^{n} L_i$, где $L_i$ — литералы.

**Пример 1.57.** Формула $(P \wedge \neg Q) \wedge \neg P$ является элементарной конъюнкцией, а формула $P \wedge (\neg Q \wedge \neg P)$ не является элементарной конъюнкцией.

**Определение 1.58.** *Дизъюнктивной нормальной формой (ДНФ)* называем формулу вида $\bigvee_{j=1}^{m} C_j$, где $C_j$ — элементарные конъюнкции.

**Пример 1.59.** Формулы $(P \wedge \neg R) \vee (Q \wedge R)$ и $(P \wedge Q \wedge R) \vee \neg P \vee \neg R$ являются дизъюнктивными нормальными формами.

**Упражнение 1.60.** *Привести к дизъюнктивной нормальной форме формулу* $(P \vee Q) \to R$. *Ответ:* $(\neg P \wedge \neg Q) \vee R$.

Аналогично определяются элементарные дизъюнкции и конъюнктивные нормальные формы.

**Определение 1.61.** *Элементарной дизъюнкцией* называем формулу вида $\bigvee_{i=1}^{n} L_i$, где $L_i$ — литералы.

*Конъюнктивной нормальной формой (КНФ)* называем формулу вида $\bigwedge_{j=1}^{m} D_j$, где $D_j$ — элементарные дизъюнкции.

**Упражнение 1.62.** *Привести к конъюнктивной нормальной форме формулу* $(P \vee Q) \to R$. *Ответ:* $(\neg P \vee R) \wedge (\neg Q \vee R)$.

**Теорема 1.63.** *Каждая пропозициональная формула равносильна некоторой дизъюнктивной нормальной форме и некоторой конъюнктивной нормальной форме.*

**Доказательство (первый вариант).** Если $A$ тождественно ложна, в качестве её ДНФ можно взять формулу $P \wedge \neg P$, где $P$ — любая переменная. В противном случае достаточно заметить, что формула, построенная в доказательстве теоремы о функциональной полноте для функции $\varphi_A$ есть ДНФ.

**Доказательство (второй вариант).** Выразим $\to$ через $\neg$ и $\vee$. Далее преобразуем формулу, применяя таблицу основных эквивалентностей и активно пользуясь правилом замены подформулы на эквивалентную. Сначала проносим все отрицания максимально вглубь формулы и удаляем многократные отрицания. Затем, пользуясь дистрибутивностью, выносим все дизъюнкции максимально наружу. Пользуясь ассоциативностью $\wedge$ и $\vee$ расставляем правильно скобки.

Осталось заметить, что если $A$ — дизъюнктивная нормальная форма, то формула $\neg A$ превращается в конъюнктивную нормальную форму после переноса всех отрицаний вглубь и удаления двойных отрицаний. Значит, для того чтобы получить конъюнктивную нормальную форму формулы $A$, достаточно применить этот процесс к дизъюнктивной нормальной форме формулы $\neg A$. ⊠

### 1.9.2 Совершенные ДНФ и КНФ

В этом параграфе считаем фиксированным конечный набор переменных $\mathrm{Var} = \{P_1, \ldots, P_n\}$ и будем рассматривать лишь формулы от этих переменных.

**Определение 1.64.** Формула $A$ называется *совершенной ДНФ*, если $A$ — ДНФ и

- Каждая элементарная конъюнкция имеет вид $A_{\vec{x}} \rightleftharpoons \bigwedge_{i=1}^{n} P_i^{x_i}$ для некоторого $\vec{x} \in \mathbb{B}^n$.
- $A = \bigvee_{j=1}^{m} A_{\vec{x}_j}$, где $\vec{x}_1, \ldots \vec{x}_m \in \mathbb{B}^n$ попано различны и взяты в лексикографическом порядке.

Определение *совершенной КНФ* аналогично, с заменой дизъюнкций на конъюнкции и наоборот.

**Замечание 1.65.** Удобно расширить множество формул константами $\bot$ (ложь) и $\top$ (истина). Тем самым, формулами считаются и все выражения, построенные с помощью булевых связок из переменных и этих констант. Считаем $\bot$ совершенной ДНФ, а $\top$ — совершенной КНФ.

**Замечание 1.66.** Совершенные ДНФ и КНФ перестают быть совершенными, если рассматривать их как формулы от более широкого набора переменных. Поэтому имеет смысл говорить о совершенных ДНФ и КНФ лишь относительно некоторого фиксированного набора переменных.

**Теорема 1.67.** *Всякая формула $A$ равносильна некоторой совершенной ДНФ.*

**Доказательство (первый вариант).** Если $A$ тождественно ложна, в качестве её ДНФ можно взять $\bot$. В противном случае достаточно заметить, что формула, построенная в доказательстве теоремы о функциональной полноте для функции $\varphi_A$ есть совершенная ДНФ. ⊠

**Доказательство (второй вариант).** Сначала приведём формулу к ДНФ. Удалим противоречивые конъюнкции, воспользовавшись равносильностями:

$$A \wedge \neg A \equiv \bot, \quad \bot \wedge A \equiv \bot, \quad \bot \vee A \equiv A.$$

При этом формула либо приводится к виду $\bot$, либо в формуле останутся лишь элементарные конъюнкции без вхождений пар противоположных литералов. В оставшихся конъюнкциях удалим повторы литералов с помощью равносильности $A \wedge A \equiv A$. Для каждой конъюнкции добавим недостающие до полного набора $P_1, \ldots, P_n$ переменные, пользуясь равносильностью

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

С помощью ассоциативности и коммутативности добьёмся требуемого упорядочения всех членов и правильной расстановки скобок. ⊠

**Замечание 1.68.** $(A \wedge B) \vee (A \wedge \neg B) \equiv A \wedge (B \vee \neg B) \equiv A \wedge \top \equiv A$.

**Теорема 1.69.** *Совершенные ДНФ эквивалентных формул (графически) совпадают.*

**Доказательство.** . Для совершенной ДНФ каждая элементарная конъюнкция определяет некоторую выполняющую оценку, а сама ДНФ — множество всех таких оценок. ⊠

**Следствие 1.70.** *Совершенная ДНФ любой формулы $A$ единственна.*

Аналогичные теоремы имеют место и для совершенных КНФ.

**Упражнение 1.71.** *Привести к совершенной конъюнктивной нормальной форме формулу $\neg(P \leftrightarrow Q)$. Ответ: $(P \vee Q) \wedge (\neg P \vee \neg Q)$.*

### 1.9.3 Полнота исчисления эквивалентностей[2]

Следующая теорема является простым аналогом теоремы о полноте исчисления высказываний, доказываемой ниже. Смысл этого результата в том, что мы сводим (без потери информации) проверку эквивалентности формул к чисто механическим символьным преобразованиям. Исчисление эквивалентностей, фигурирующее неявно в данной теореме — представитель класса так называемых *эквациональных исчислений*, или *исчислений тождеств*, которые распространены в алгебре.

**Теорема 1.72.** *Всякая равносильность $A \equiv B$ может быть выведена из основных равносильностей (данных в таблице) и дополнительных равносильнольностей для констант $\top$ и $\bot$*

$$A \wedge \neg A \equiv \bot, \quad A \vee \neg A \equiv \top$$

[2]Необязательный материал.

*по правилу замены подформулы на эквивалентную и правилам*

$$\frac{B \equiv A}{A \equiv B}, \quad \frac{A \equiv B \quad B \equiv C}{A \equiv C}.$$

**Доказательство.** По теореме о СДНФ равносильные формулы приводятся к графически равным СДНФ. При этом достаточно пользоваться лишь основными и дополнительными равносильностями и указанными правилами для вывода новых равносильностей (см. второй способ доказательства теоремы о СДНФ). Нам нужно лишь вывести следующие используемые в доказательстве теоремы о СДНФ равносильности для констант: $\bot \wedge A \equiv \bot$, $\bot \vee A \equiv A$, $A \wedge \top \equiv A$. Получаем:

- $A \wedge \bot \equiv A \wedge (A \wedge \neg A) \equiv (A \wedge A) \wedge \neg A \equiv A \wedge \neg A \equiv \bot$.
- $A \vee \bot \equiv A \vee (A \wedge \neg A) \equiv A$ по закону поглощения.
- $A \wedge \top \equiv A \wedge (A \vee \neg A) \equiv A$, аналогично.

Таким образом, от $A$ к $B$ можно перейти по цепочке эквивалентностей

$$A = A_0 \equiv A_1 \equiv \dots \equiv A' = B' \equiv \dots \equiv B_1 \equiv B_0 = B,$$

где $A'$ и $B'$ — СДНФ формул $A$ и $B$, соответственно, а каждый переход $A_i \equiv A_{i+1}$ и $B_{i+1} \equiv B_i$ получается заменой некоторой подформулы на эквивалентную в соответствии с одной из известных нам основных или дополнительных эквивалентностей. ⊠

## 1.10 Другие варианты формальной семантики

### 1.10.1 Теоретико-множественная семантика

Пусть $U$ — непустое множество; $\mathcal{P}(U)$ — множество всех его подмножеств.

**Определение 1.73.** *Оценкой* называется функция $f : \mathrm{Var} \to \mathcal{P}(U)$. *Значение* $f(A) \subseteq U$ формулы $A$ при оценке $f$ определяется индуктивно по правилам:

- $f(\neg A) \rightleftharpoons U \setminus f(A)$
- $f(A \wedge B) \rightleftharpoons f(A) \cap f(B)$
- $f(A \vee B) \rightleftharpoons f(A) \cup f(B)$
- $f(A \to B) \rightleftharpoons (U \setminus f(A)) \cup f(B)$

**Замечание 1.74.** Если взять $U = \{0\}$, теоретико-множественная семантика сводится к стандартной двузначной: Л $= \varnothing$, И $= U$.

**Замечание 1.75.** Если взять $U = \mathbb{R}^2$ и если для $P \in \mathrm{Var}\ f(P)$ — круги на плоскости, получаем *диаграммы Венна*, известные из школы.

### 1.10.2 Алгебраическая семантика[3]

**Определение 1.76.** Множество $\mathbf{B}$ с заданными на нём константами 0, 1 и операциями $\neg$, $\wedge$, $\vee$, $\to$, которые удовлетворяют равенствам

$$a \wedge \neg a = 0, \quad a \vee \neg a = 1$$

и равенствам, соответствующим таблице основных эквивалентностей, называется *булевой алгеброй.*

В таблице основных эквивалентностей заменяем $\equiv$ на $=$ и большие латинские буквы $A$, $B$, $C$ (означающие произвольные формулы) на маленькие $a$, $b$, $c$ (означающие элементы множества $\mathbf{B}$), получаем список *тождеств булевой алгебры:*

| | | | | | |
|---|---|---|---|---|---|
| $a \wedge b$ | $=$ | $b \wedge a$ | $a \vee b$ | $=$ | $b \vee a$ |
| $a \wedge (b \wedge c)$ | $=$ | $(a \wedge b) \wedge c$ | $a \vee (b \vee c)$ | $=$ | $(a \vee b) \vee c$ |
| $a \wedge a$ | $=$ | $a$ | $a \vee a$ | $=$ | $a$ |
| $a \wedge (b \vee c)$ | $=$ | $(a \wedge b) \vee (a \wedge c)$ | $a \vee (b \wedge c)$ | $=$ | $(a \vee b) \wedge (a \vee c)$ |
| $a \vee (a \wedge b)$ | $=$ | $a$ | $a \wedge (a \vee b)$ | $=$ | $a$ |
| $\neg(a \wedge b)$ | $=$ | $\neg a \vee \neg b$ | $\neg(a \vee b)$ | $=$ | $\neg a \wedge \neg b$ |
| $\neg\neg a$ | $=$ | $a$ | $a \to b$ | $=$ | $\neg a \vee b$ |
| $a \wedge \neg a$ | $=$ | $0$ | $a \vee \neg a$ | $=$ | $1$ |

**Примеры булевых алгебр.**

- $\mathbb{B} \rightleftharpoons \{0, 1\}$;
- $\mathcal{P}(U)$ для любого $U$;
- $\mathrm{Fm}/{\equiv}$ (*алгебра Линденбаума*), то есть множество классов равносильных формул с синтаксически определёнными операциями $\wedge$, $\vee$, $\to$, $\neg$. Более формально, если $[A]$ обозначает класс эквивалентности формулы $A$, то операция $\wedge$ на классах определяется следующим образом: $[A] \wedge [B] \rightleftharpoons [A \wedge B]$, и аналогично определены остальные операции. Лемма 1.50 гарантирует корректность этих определений.

[3] Необязательный материал.

**Определение 1.77.** *Оценкой* на булевой алгебре называется функция $f$ : $\mathrm{Var} \to \mathbf{B}$. *Значение* $f(A) \in \mathbf{B}$ формулы $A$ при оценке $f$ вычисляется в соответствии с заданными на $\mathbf{B}$ операциями, в частности $f(A \wedge B) = f(A) \wedge f(B)$ и т.д.

Непосредственно следует из определений следует

**Лемма 1.78.** *Для любой оценки $f : \mathrm{Var} \to \boldsymbol{B}$ на булевой алгебре, если $A \equiv B$ — одна из основных или дополнительных эквивалентностей, то $f(A) = f(B)$ в $\boldsymbol{B}$.*

Следующая теорема показывает, что каждая из указанных семантик задаёт одно и то же множество тавтологий.

**Теорема 1.79.** *Для любого множества $U$ и любой булевой алгебры $\boldsymbol{B}$ равносильны следующие утверждения.*

(i) *$A$ — тавтология;*

(ii) *$f(A) = U$ для любой оценки $f : \mathrm{Var} \to \mathcal{P}(U)$;*

(iii) *$f(A) = 1$ для любой оценки $f : \mathrm{Var} \to \boldsymbol{B}$.*

**Доказательство.** Утверждение (iii) влечёт (i), поскольку если $f : \mathrm{Var} \to \mathbb{B}$ — оценка, при которой $f(A) = \text{Л}$, мы можем определить соответствующую оценку $f' : \mathrm{Var} \to \mathbf{B}$ на булевой алгебре $\mathbf{B}$ отождествляя И с $1 \in \mathbf{B}$ и Л с $0 \in \mathbf{B}$. При этом для любой формулы $C$ имеем

$$f(C) = \text{И} \iff f'(C) = 1$$

и тем самым $f'(A) = 0$. Аналогично, (ii) влечёт (i).

Докажем, что (i) влечёт (iii). Допустим, что $A$ тавтология. По теореме о полноте исчисления эквивалентностей, равносильность $A \equiv \top$ выводится из основных и дополнительных эквивалентностей по известным правилам. Индукцией по длине цепочки вывода $A \equiv \top$ на основе леммы 1.78 легко установить, что $f(A) = f(\top) = 1$ при любой оценке $f$.

Отметим, что (i) влечёт (ii) поскольку $\mathcal{P}(U)$ есть булева алгебра. ⊠

# 2 Исчисление высказываний

В этом разделе буквы $A$, $B$ и т. д. обозначают формулы логики высказываний, а буквы $\Gamma$, $\Delta$ и т. д. обозначают множества формул логики высказываний.

## 2.1 Аксиомы и правила вывода исчисления высказываний

**Определение 2.1.** *Классическое исчисление высказываний* задаётся следующими аксиомами и правилами вывода:

**Аксиомы:**

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

**Правило вывода:** $\dfrac{A \quad A \to B}{B}$ (*modus ponens*, MP).

**Определение 2.2.** *Выводом в исчислении высказываний* (или просто *выводом*) называется конечная последовательность формул, каждая из которых является аксиомой или получается из некоторых предыдущих формул по правилу вывода.

**Пример 2.3.** Следующая последовательность формул является выводом:

$$
\begin{array}{ll}
P \to Q \vee P & \\
Q \to Q \vee P & \\
(P \to Q \vee P) \to ((Q \to Q \vee P) \to (P \vee Q \to Q \vee P)) & \\
(Q \to Q \vee P) \to (P \vee Q \to Q \vee P) & \text{(MP)} \\
P \vee Q \to Q \vee P & \text{(MP).}
\end{array}
$$

**Определение 2.4.** Формула $A$ называется *выводимой* в исчислении высказываний или *теоремой* исчисления высказываний (обозначение $\vdash A$), если существует вывод, в котором последняя формула есть $A$.

**Пример 2.5.** $\vdash P \vee Q \to Q \vee P$.

**Пример 2.6.** $\vdash A \to A$.

**Доказательство.** В аксиоме 2 возьмём $B = (A \to A)$ и $C = A$.

$$
\begin{array}{ll}
(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A)) & \\
A \to ((A \to A) \to A) & \\
(A \to (A \to A)) \to (A \to A) & \text{(MP)} \\
A \to (A \to A) & \\
A \to A & \text{(MP).}
\end{array}
$$

$\boxtimes$

## 2.2 Выводимость из гипотез

**Определение 2.7.** Пусть $\Gamma$ — некоторое множество формул. *Выводом из* $\Gamma$ называется конечная последовательность формул, каждая из которых либо принадлежит множеству $\Gamma$, либо является аксиомой, либо получается из предыдущих формул по правилу вывода. Элементы множества $\Gamma$ называются *гипотезами.*

**Пример 2.8.** Следующая последовательность формул является выводом из множества гипотез $\{P \wedge Q\}$:

$$
\begin{array}{ll}
P \wedge Q & \text{(гипотеза)} \\
P \wedge Q \to P & \\
P & \text{(MP)} \\
P \wedge Q \to Q & \\
Q & \text{(MP)} \\
Q \to (P \to Q \wedge P) & \\
P \to Q \wedge P & \text{(MP)} \\
Q \wedge P & \text{(MP).}
\end{array}
$$

**Определение 2.9.** Формула $A$ называется *выводимой из множества формул* $\Gamma$ (обозначение $\Gamma \vdash A$), если существует вывод из $\Gamma$, в котором последняя формула есть $A$.

**Замечание 2.10.** Вместо $\{B_1, \ldots, B_n\} \vdash A$ обычно пишут $B_1, \ldots, B_n \vdash A$. Выражение $\Gamma \vdash A, B$ означает $\Gamma \vdash A$ и $\Gamma \vdash B$.

**Пример 2.11.** $P \wedge Q \vdash Q \wedge P$.

**Замечание 2.12.** Выводимость из гипотез обладает следующими простыми свойствами.

- Если $\Delta \subseteq \Gamma$ и $\Delta \vdash A$, то $\Gamma \vdash A$ (*монотонность*).
- Если $\Gamma \vdash A$, то существует такое конечное множество $\Delta \subseteq \Gamma$, что $\Delta \vdash A$ (*компактность*).
- Если $\Gamma \vdash A$ и для каждой формулы $B \in \Gamma$ имеет место $\Delta \vdash B$, то $\Delta \vdash A$ (*транзитивность*).

## 2.3 Корректность исчисления высказываний

**Предложение 2.13 (корректность).** *Всякая выводимая формула является тавтологией.*

**Доказательство.** Теорема доказывается индукцией по длине вывода формулы $A$. ⊠

Аналогично доказывается несколько более общее утверждение, связывающее синтаксическое и семантическое отношения следования.

**Предложение 2.14.** *Если* $\Gamma \vdash A$, *то* $\Gamma \vDash A$.

## 2.4 Теорема о дедукции для исчисления высказываний

Следующая теорема существенно упрощает построение выводов в исчислении высказываний.

**Теорема 2.15 (о дедукции).** *Если* $\Gamma \cup \{A\} \vdash B$, *то* $\Gamma \vdash (A \to B)$.

**Доказательство.** Теорема доказывается индукцией по длине вывода формулы $B$ из множества гипотез $\Gamma \cup \{A\}$.

Если $B$ является аксиомой или принадлежит $\Gamma$, то искомый вывод выглядит так:

$$
\begin{array}{ll}
B & \\
B \to (A \to B) & \\
(A \to B) & \text{(MP).}
\end{array}
$$

Если $B$ совпадает с $A$, то используем пример 2.6.

Если $B$ получена из некоторых предыдущих формул по правилу вывода modus ponens, то эти формулы имеют вид $C$ и $C \to B$. Согласно предположению индукции $\Gamma \vdash (A \to C)$ и $\Gamma \vdash (A \to (C \to B))$. Искомый вывод формулы $B$ из множества гипотез $\Gamma \cup \{A\}$ состоит из этих двух выводов и следующих формул:

$$
\begin{array}{ll}
(A \to (C \to B)) \to ((A \to C) \to (A \to B)) & \\
(A \to C) \to (A \to B) & \text{(MP)} \\
A \to B & \text{(MP).}
\end{array}
$$

⊠

**Замечание 2.16.** Вместо $\Gamma \cup \{A\} \vdash B$ обычно пишут $\Gamma, A \vdash B$.

**Пример 2.17.** Из примера 2.11 и теоремы 2.15 следует, что $\vdash P \wedge Q \to Q \wedge P$.

**Следствие 2.18.** *Пусть* $\Gamma$ *— некоторое множество формул. Тогда* $\Gamma \vdash (A \to B)$ *в том и только том случае, когда* $\Gamma \cup \{A\} \vdash B$.

**Доказательство.** Достаточность доказана в теореме 2.15. Необходимость доказывается одним применением правила modus ponens. ⊠

## 2.5 Полезные выводимые правила

Приведём несколько полезных примеров выводимых правил, обосновываемых с помощью теоремы о дедукции.

**Пример 2.19.** (*силлогизм*) $A \to B, B \to C \vdash A \to C$.

**Доказательство.** Дважды по правилу modus ponens выводим

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

Отсюда получаем требуемое по теореме о дедукции. ⊠

**Пример 2.20.** (*контрапозиция*) $A \to B \vdash \neg B \to \neg A$.

**Доказательство.** По модулю теоремы о дедукции достаточно вывести $A \to B,\ \neg B \vdash \neg A$. Строим следующий вывод:

$$\begin{array}{ll}
A \to B & \\
\neg B & \\
(A \to B) \to ((A \to \neg B) \to \neg A) & \\
(A \to \neg B) \to \neg A & \text{(MP)} \\
\neg B \to (A \to \neg B) & \\
A \to \neg B & \text{(MP)} \\
\neg A & \text{(MP).}
\end{array}$$

⊠

**Пример 2.21.** (*ex falso*) $A, \neg A \vdash B$.

ex falso sequitur quodlibet (лат.) «из ложного следует всё, что угодно»

**Доказательство.** Выводим, опираясь на аксиомы 1 (дважды), 9 и 10:

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

⊠

## 2.6 Непротиворечивые множества формул

**Определение 2.22.** Множество формул $\Gamma$ называется *противоречивым*, если для некоторой формулы $A$ имеем $\Gamma \vdash A$ и $\Gamma \vdash \neg A$. В противном случае $\Gamma$ называется *непротиворечивым*.

**Замечание 2.23.** Если $\Gamma$ противоречиво, то $\Gamma \vdash B$ для любой формулы $B$ в силу выводимости $A, \neg A \vdash B$.

**Замечание 2.24.** $\Gamma$ противоречиво, если и только если существует конечное противоречивое подмножество $\Gamma_0 \subseteq \Gamma$.

**Лемма 2.25.** $\Gamma \cup \{B\}$ *противоречиво* $\iff$ $\Gamma \vdash \neg B$.

**Доказательство.** Если $\Gamma \vdash \neg B$, то $\Gamma \cup \{B\}$ противоречиво, поскольку в качестве $A$ можно взять $B$.

Если $\Gamma, B \vdash A, \neg A$, то по теореме о дедукции $\Gamma \vdash B \to A, B \to \neg A$. По аксиоме $(B \to A) \to ((B \to \neg A) \to \neg B)$ отсюда следует $\Gamma \vdash \neg B$. $\boxtimes$

**Определение 2.26.** $\Gamma$ называется *максимальным непротиворечивым* множеством, если $\Gamma$ непротиворечиво и для любой формулы $A \notin \Gamma$ $\Gamma \cup \{A\}$ противоречиво.

**Пример 2.27.** Пусть $f$ — фиксированная оценка, тогда множество $\Gamma_f \rightleftharpoons \{A : f(A) = \text{И}\}$ — максимальное непротиворечивое.

**Теорема 2.28 (Линденбаума).** *Для всякого непротиворечивого множества формул* $\Gamma_0$ *найдётся максимальное непротиворечивое* $\Gamma \supseteq \Gamma_0$.

**Доказательство (для счётного числа переменных).** Пусть $A_0, A_1, \ldots$ — пересчёт всех формул языка. Определим последовательность множеств, начинающуюся с данного множества $\Gamma_0$,

$$\Gamma_0 \subseteq \Gamma_1 \subseteq \cdots \subseteq \Gamma_n \subseteq \ldots$$

по следующему правилу:

$$\Gamma_{n+1} = \begin{cases} \Gamma_n \cup \{A_n\}, \text{ если } \Gamma_n \cup \{A_n\} \text{ непротиворечиво;} \\ \Gamma_n, \text{ иначе.} \end{cases}$$

Положим $\Gamma \rightleftharpoons \bigcup_{n \geq 0} \Gamma_n$. Утверждение теоремы вытекает из следующей леммы.

**Лемма 2.29.** (i) *Для любого* $n$ *множество* $\Gamma_n$ *непротиворечиво.*

(ii) $\Gamma$ *— максимальное непротиворечивое множество.*

**Доказательство.** Утверждение (i) доказывается индукцией по $n$. Из (i) вытекает непротиворечивость $\Gamma$ (в силу свойства компактности). Поэтому для доказательства утверждения (ii) достаточно установить максимальность.

Допустим $A \notin \Gamma$. Поскольку в исходном пересчёте встречаются все формулы, для некоторого $k$ формула $A$ есть $A_k$. Поскольку $A_k \notin \Gamma$, множество $\Gamma_k \cup \{A_k\}$ противоречиво (иначе мы присоединили бы $A_k$ на шаге $k$). Значит, противоречиво и объемлющее множество $\Gamma \cup \{A_k\}$. $\boxtimes$

**Замечание 2.30.** Для несчётного языка теорема Линденбаума доказывается, опираясь на лемму Цорна (эквивалентную аксиоме выбора). Как нетрудно показать, объединение возрастающей цепи непротиворечивых множеств непротиворечиво. Отсюда непосредственно вытекает требуемый результат.

**Предложение 2.31.** *Пусть* $\Gamma$ *— максимальное непротиворечивое множество. Тогда для любых формул* $A$, $B$

(i) $\neg A \in \Gamma \iff A \notin \Gamma$;

(ii) $(A \wedge B) \in \Gamma \iff A \in \Gamma$ *и* $B \in \Gamma$;

(iii) $(A \vee B) \in \Gamma \iff A \in \Gamma$ *или* $B \in \Gamma$;

(iv) $(A \to B) \in \Gamma \iff A \notin \Gamma$ *или* $B \in \Gamma$.

**Доказательство.** (i) Рассуждаем от противного. Если обе формулы $A, \neg A \in \Gamma$, то $\Gamma$ противоречиво. Если же $A, \neg A \notin \Gamma$, то противоречивы, соответственно, множества $\Gamma \cup \{A\}$ и $\Gamma \cup \{\neg A\}$ в силу максимальности. Отсюда по лемме 2.25 получаем $\Gamma \vdash \neg A, \neg\neg A$, т.е. $\Gamma$ противоречиво.

(ii) Пусть $(A \wedge B) \in \Gamma$, $A \notin \Gamma$. Тогда, в силу максимальности, $\Gamma \cup \{A\}$ противоречиво, откуда $\Gamma \vdash \neg A$. С другой стороны, по аксиоме $(A \wedge B) \to A$ имеем $A \wedge B \vdash A$. Значит, $\Gamma \vdash A$, т.е. $\Gamma$ противоречиво.

Аналогично рассматриваем случай $(A \wedge B) \in \Gamma$, $B \notin \Gamma$.

Пусть теперь $(A \wedge B) \notin \Gamma$ и $A, B \in \Gamma$. Тогда по максимальности $\Gamma \vdash \neg(A \wedge B)$. С другой стороны, по аксиоме $A \to (B \to (A \wedge B))$ имеем $\Gamma \vdash A \wedge B$, т.е. $\Gamma$ противоречиво.

(iii) доказывается аналогично (ii).

(iv) Допустим $(A \to B) \in \Gamma$, $A \in \Gamma$, $B \notin \Gamma$. Тогда $\Gamma \cup \{B\}$ противоречиво, откуда $\Gamma \vdash \neg B$. С другой стороны, по правилу modus ponens $\Gamma \vdash B$, т.е. $\Gamma$ противоречиво.

Допустим $(A \to B) \notin \Gamma$, $A \notin \Gamma$. Тогда в силу максимальности $\Gamma \vdash \neg A$, $\Gamma \vdash \neg(A \to B)$.

Заметим, что $\neg(A \to B) \vdash A$. Действительно, из $A, \neg A \vdash B$ получаем $\neg A \vdash A \to B$, отсюда с помощью контрапозиции и снятия двойного отрицания $\neg(A \to B) \vdash \neg\neg A \vdash A$.

Поскольку $\Gamma \vdash \neg(A \to B)$, отсюда получаем $\Gamma \vdash A$, т.е. $\Gamma$ противоречиво.

Случай $(A \to B) \notin \Gamma$, $B \in \Gamma$ рассматривается аналогично, с использованием выводимости $\neg(A \to B) \vdash \neg B$. Последняя вытекает с помощью контрапозиции из очевидного $B \vdash A \to B$. ⊠

## 2.7 Теорема о полноте исчисления высказываний

**Теорема 2.32.** *Множество* $\Gamma$ *непротиворечиво тогда и только тогда, когда* $\Gamma$ *выполнимо.*

**Доказательство.** Выполнимость влечёт непротиворечивость. Пусть $f$ — такая оценка, что $f(A) = \text{И}$ для всех формул $A \in \Gamma$. Простой индукцией по построению вывода убедимся, что $f(B) = \text{И}$ для любой формулы $B$ такой, что $\Gamma \vdash B$. Тем самым, $B$ не может быть противоречием.

Непротиворечивость влечёт выполнимость. Допустим $\Gamma$ непротиворечиво. По теореме Линденбаума расширим $\Gamma$ до максимального непротиворечивого множества формул $\Gamma'$. Определим оценку $f$ следующим образом: для любой переменной $P$

$$f(P) = \text{И} \stackrel{\text{def}}{\iff} P \in \Gamma'.$$

Утверждение теоремы вытекает из следующей леммы.

**Лемма 2.33.** *Для любой формулы* $A$

$$f(A) = \textit{И} \iff A \in \Gamma'.$$

**Доказательство.** Индукция по построению формулы $A$.

Если $A$ — переменная, то утверждение верно непосредственно по определению $f$.

Если $A = \neg B$, то пользуясь последовательно определением оценки, предположением индукции и предложением 2.31 (i) имеем

$$f(\neg B) = \text{И} \iff f(B) \neq \text{И} \iff B \notin \Gamma' \iff (\neg B) \in \Gamma'.$$

Если $A = (B \to C)$, то аналогично по предложению 2.31 (iv) получаем

$$\begin{aligned} f(B \to C) = \text{И} &\iff (f(B) \neq \text{И} \text{ или } f(C) = \text{И}) \iff \\ &\iff (B \notin \Gamma' \text{ или } C \in \Gamma') \iff (B \to C) \in \Gamma'. \end{aligned}$$

Оставшиеся случаи рассматриваются аналогично. ⊠

Поскольку $\Gamma \subseteq \Gamma'$, для любой $A \in \Gamma$ получаем $f(A) = \text{И}$, что и требовалось. ⊠

**Теорема 2.34 (полнота).** *Всякая тавтология выводима в исчислении высказываний.*

Полнота исчисления высказываний следует из более общего свойства *сильной полноты.*

**Теорема 2.35 (сильная полнота).** *Для любого множества формул* $\Gamma$ *и любой формулы* $A$

$$\Gamma \vDash A \ \Rightarrow\ \Gamma \vdash A.$$

**Доказательство.** Заметим, что $\Gamma \vDash A$ влечёт невыполнимость множества $\Gamma \cup \{\neg A\}$. По теореме 2.32 множество $\Gamma \cup \{\neg A\}$ противоречиво и тем самым $\Gamma \vdash \neg\neg A \vdash A$. ⊠

Таким образом, семантическое следование в логике высказываний равносильно выводимости из гипотез:

**Следствие 2.36.** $\Gamma \vDash A \iff \Gamma \vdash A$.

**Следствие 2.37 (компактность).** $\Gamma \vDash A \iff \Gamma_0 \vDash A$ *для некоторого конечного подмножества* $\Gamma_0 \subseteq \Gamma$.