

# Введение в математическую логику (осень 2018)

Механико-математический факультет МГУ, 2 курс

проф. В. Б. Шехтман

## Содержание

<b>Логика высказываний</b>	<b>2</b>
Пропозициональные формулы . . . . .	2
Подформулы . . . . .	3
Оценки и значения формул . . . . .	3
Булевы функции . . . . .	4
Нормальные формы . . . . .	6
Двойственность . . . . .	7
Булевы алгебры . . . . .	7
Исчисление высказываний . . . . .	12
Теорема о дедукции для исчисления высказываний . . . . .	15
Корректность исчисления высказываний для булевых алгебр . . . . .	16
Полнота исчисления высказываний . . . . .	18
<b>Логика предикатов</b>	<b>20</b>
Языки первого порядка: синтаксис . . . . .	21
Языки первого порядка: семантика . . . . .	23
Определение истинности в модели . . . . .	26
Изоморфизмы моделей . . . . .	28
Определимость и автоморфизмы . . . . .	30
Стандартные теории равенства и нормальные модели . . . . .	32
Теория конечной модели . . . . .	35
Общезначимость и равносильность . . . . .	37
Предваренная нормальная форма . . . . .	40
Исчисление предикатов . . . . .	43
Корректность исчисления предикатов . . . . .	46
Исчисление предикатов с равенством . . . . .	49
Непротиворечивость . . . . .	49
Пример: арифметика Пеано . . . . .	50
Модальное исчисление <b>S5</b> . . . . .	51
Семантика Крипке для <b>S5</b> . . . . .	51
Стандартный перевод модальных формул . . . . .	52
Свойства исчисления <b>S5</b> . . . . .	54
Полнота исчисления предикатов и ее следствия . . . . .	59
О нестандартных моделях арифметики . . . . .	61
Наивная теория множеств . . . . .	62
Теория множеств Цермело . . . . .	62
<b>Теория алгоритмов</b>	<b>66</b>
Алгоритмы . . . . .	66
Вычислимые функции . . . . .	66
Разрешимость и перечислимость . . . . .	66
Универсальная вычислимая функция. Неразрешимость . . . . .	67
О разрешимости теорий первого порядка . . . . .	68
Теорема Гёделя о неполноте . . . . .	69

# Введение в математическую логику (осень 2018)

В.Б. Шехтман

## Лекции 1-2

### ЛОГИКА ВЫСКАЗЫВАНИЙ

#### Пропозициональные формулы

Высказывания — это предложения естественного языка. Естественные языки — предмет изучения других наук: лингвистики и филологии. В математической логике рассматриваются формальные языки. Простейший из них — язык классической логики высказываний, который задается так.

**Определение 1.** Фиксируем счетное множество символов — так называемых *пропозициональных переменных*  $Var = \{P_1, P_2, \dots\}$ . Множество *пропозициональных формул*, обозначаемое  $Fm$ , строится из этих переменных, логических связок  $\wedge, \vee, \rightarrow, \neg$  и скобок по индукции, как наименьшее множество, удовлетворяющее условиям:

- (1) Если  $A \in Var$ , то  $A \in Fm$ .
- (2) Если  $A, B \in Fm$ , то  $(A \wedge B) \in Fm$ .
- (3) Если  $A, B \in Fm$ , то  $(A \vee B) \in Fm$ .
- (4) Если  $A, B \in Fm$ , то  $(A \rightarrow B) \in Fm$ .
- (5) Если  $A \in Fm$ , то  $\neg A \in Fm$ .

Таким образом, формулы представляют собой конечные последовательности знаков, т.е. некоторые слова в алфавите, состоящем из переменных, связок и скобок.<sup>1</sup>

Правила построения формул можно записать схематически так:

$$(1) P_i, \quad (2) \frac{A, B}{(A \wedge B)}, \quad (3) \frac{A, B}{(A \vee B)}, \quad (4) \frac{A, B}{(A \rightarrow B)}, \quad (5) \frac{A}{\neg A}.$$

Эти правила задают множество  $Fm$  с помощью «формальной грамматики». Обычно формальные языки описываются правилами такого типа.

При записи формул используют дополнительные сокращения: внешние скобки опускаются; для экономии внутренних скобок устанавливается приоритет связок:  $\wedge$  сильнее  $\vee$ ,  $\vee$  сильнее  $\rightarrow$ . И конечно,  $\neg$  сильнее всех, но это и так видно из записи.

Еще одно сокращение:

$$(A \leftrightarrow B) := ((A \rightarrow B) \wedge (B \rightarrow A)).$$

**Лемма 1.1** (Лемма об однозначном анализе формул). *Для любой формулы  $C$  выполнено ровно одно из условий:*

- (I)  $C \in Var$ ,
- (II) Существует единственная пара формул  $A, B$ , такая что  $C = (A \wedge B)$ ,
- (III) Существует единственная пара формул  $A, B$ , такая что  $C = (A \vee B)$ ,
- (IV) Существует единственная пара формул  $A, B$ , такая что  $C = (A \rightarrow B)$ ,
- (V) Существует единственная формула  $A$ , такая что  $C = \neg A$ .

Доказательство этой леммы мы пропустим; его можно найти, например, в [1], [5].

<sup>1</sup>Этот алфавит бесконечен за счет множества  $Var$ . Можно обойтись и конечным алфавитом, если каждую переменную  $P_n$  изображать в виде слова  $P1 \dots 1$  ( $n$  раз).

## Подформулы

Говоря не совсем точно, подформула — это часть формулы, которая тоже является формулой. Точное определение можно дать двумя способами.

**Определение 2.** Подсловом слова  $a_1 \dots a_n$  (где  $a_1, \dots, a_n$  — буквы) называется его часть, расположенная между какими-то двумя позициями, т.е. слово вида  $a_i \dots a_j$ , где  $i < j$ .<sup>2</sup> Подформулой формулы  $A$  называется любое ее подслово, которое является формулой.

Другой вариант: определяем отношение  $A \preceq B$  ( $A$  — подформула  $B$ ) индукцией по длине  $B$ .

**Определение 3** (Индуктивное определение подформулы).<sup>3</sup>

- Если  $B \in Var$ , то  $A \preceq B \Leftrightarrow A = B$ ,
- Если  $B = (C \wedge D)$ ,  $(C \vee D)$  или  $(C \rightarrow D)$  для формул  $C, D$ , то

$$A \preceq B \quad \Leftrightarrow \quad (A = B \text{ или } A \preceq C \text{ или } A \preceq D).$$

- Если  $B = \neg C$ , то

$$A \preceq B \quad \Leftrightarrow \quad (A = B \text{ или } A \preceq C).$$

Задача Докажите, что два определения подформулы эквивалентны.

(Более легкая часть: если  $A \preceq B$ , то  $A$  — подслово  $B$  и формула. Это делается индукцией по длине  $B$ .)

## Оценки и значения формул

**Определение 4.** *Оценкой (пропозициональных переменных)* называется любое отображение  $f : Var \rightarrow \mathbb{B}$ , где  $\mathbb{B} = \{и,л\} = \{1, 0\}$ .

**Лемма 2.1** (О продолжении оценок на формулы). . Для любой оценки

$f : Var \rightarrow \mathbb{B}$  существует единственное отображение  $\bar{f} : Fm \rightarrow \mathbb{B}$ , такое что для всех  $A, B \in Fm$

- (1)  $\bar{f}(A) = f(A)$ , если  $A \in Var$ ,
- (2)  $\bar{f}(A \wedge B) = 1 \Leftrightarrow \bar{f}(A) = \bar{f}(B) = 1$ ,
- (3)  $\bar{f}(A \vee B) = 1 \Leftrightarrow (\bar{f}(A) = 1 \text{ или } \bar{f}(B) = 1)$ ,
- (4)  $\bar{f}(A \rightarrow B) = 1 \Leftrightarrow (\bar{f}(A) = 0 \text{ или } \bar{f}(B) = 1)$ ,
- (5)  $\bar{f}(\neg A) = 1 \Leftrightarrow \bar{f}(A) = 0$ .

Заметим, что условия (2)–(5) можно записать иначе:

- (2)  $\bar{f}(A \wedge B) = \min(\bar{f}(A), \bar{f}(B))$ ,
- (3)  $\bar{f}(A \vee B) = \max(\bar{f}(A), \bar{f}(B))$ ,
- (4)  $\bar{f}(A \rightarrow B) = \max(1 - \bar{f}(A), \bar{f}(B))$ ,
- (5)  $\bar{f}(\neg A) = 1 - \bar{f}(A)$ .

**Доказательство** Определяем  $\bar{f}(C)$  индукцией по длине  $C$ . Если  $C$  — переменная, то все ясно:  $\bar{f}(C) = f(C)$ .

Пусть  $\bar{f}$  однозначно определена на всех формулах длины  $< n$ ,  $n > 1$ , и рассмотрим формулу  $C$  длины  $n$ . По лемме 1.1, возможен ровно один из случаев (II)–(V). В каждом случае  $\bar{f}$  однозначно доопределяется для  $C$ .

Например, в случае (II)  $C = (A \wedge B)$  для единственной пары формул  $(A, B)$ . Эти формулы  $A, B$  — длины  $< n$ , поэтому  $\bar{f}(A), \bar{f}(B)$  однозначно определены по предположению индукции. Тогда  $\bar{f}(C) = \min(\bar{f}(A), \bar{f}(B))$  тоже задается однозначно.

Аналогично рассуждаем для других случаев. ■

<sup>2</sup>Можно и дальше уточнить смысл такой записи: это слово  $b_1 \dots b_{j-i}$ , такое что  $b_k = a_{i+k-1}$  для всех  $k = 1, \dots, j-i$ .

<sup>3</sup>Знаки  $\preceq, \Leftrightarrow$ , которые встречаются в этом определении, относятся к метаязыку; они сокращают русский текст.

$\bar{f}(C)$  называется значением формулы  $C$  при оценке  $f$ ; мы будем обозначать его также через  $f(C)$ .

Заметим еще, что условия (2)–(5) можно переписать так:

- (2)  $\bar{f}(A \wedge B) = \bar{f}(A) \otimes \bar{f}(B)$ ,
- (3)  $\bar{f}(A \vee B) = \bar{f}(A) \oplus \bar{f}(B)$ ,
- (4)  $\bar{f}(A \rightarrow B) = \bar{f}(A) \oplus \bar{f}(B)$ ,
- (5)  $\bar{f}(\neg A) = \ominus \bar{f}(A)$ ,

где  $\oplus$ ,  $\otimes$ ,  $\ominus$ ,  $\ominus$  соответственно обозначают операции на множестве  $\mathbb{B}$ :  $\max$  (“дизъюнкция”),  $\min$  (“конъюнкция”),  $\max(1 - x, y)$  (“импликация”),  $1 - x$  “отрицание”. При таких обозначениях видна некоторая аналогия между условиями (2)–(5) и определением гомоморфизма (или линейного отображения) в алгебре. Лемма 2.1 является аналогом следующего утверждения: любое отображение базиса векторного пространства в другое пространство однозначно продолжается до линейного отображения.

**Лемма 2.2.** *Значение формулы  $A$  при некоторой оценке зависит только от значения этой оценки на переменных из  $A$ : если оценки  $f, g$  совпадают на всех переменных, входящих в  $A$ , то  $f(A) = g(A)$ .*

**Доказательство** Это утверждение достаточно очевидно. Формально оно доказывается индукцией по длине  $A$ ; например, если  $A = B \vee C$ , имеем:

$$f(A) = f(B) \oplus f(C) = g(B) \oplus g(C) = g(A)$$

(по определению значения формулы и предположению индукции). ■

## Булевы функции

**Определение 5.** Мы говорим, что формула  $A$  построена из переменных  $P_1, \dots, P_n$ , если в ней нет других переменных (но не обязательно все  $P_1, \dots, P_n$  в ней встречаются).

Если  $A$  построена из  $P_1, \dots, P_n$ , то используем запись  $A(P_1, \dots, P_n)$ .

Каждой формуле  $A(P_1, \dots, P_n)$  отвечает  $n$ -местная булева функция  $\varphi_A^n$  (или короче,  $\varphi_A$ ) из  $\mathbb{B}^n$  в  $\mathbb{B}$ , которая задает значения  $A$  при всевозможных оценках. Таблица значений этой функции называется *таблицей истинности* формулы  $A$ .

Дадим точное определение  $\varphi_A^n$ .

**Определение 6.** Для каждого двоичного вектора  $\vec{x} = (x_1, \dots, x_n) \in \mathbb{B}^n$  построим оценку  $f_{\vec{x}} : Var \rightarrow \mathbb{B}$ , такую что  $f_{\vec{x}}(P_i) = x_i$  при  $i \leq n$  и (например<sup>4</sup>)  $f_{\vec{x}}(P_i) = 0$  при  $i > n$ .

Положим  $\varphi_A^n(\vec{x}) = f_{\vec{x}}(A)$ .

**Определение 7.** Формула называется *тавтологией*, если при любой оценке она принимает значение 1.

Формула называется *выполнимой*, если найдется оценка, при которой она принимает значение 1.

Очевидно, что для любой формулы  $A$ :

- $A$  — тавтология  $\Leftrightarrow \neg A$  не выполнима.
- $A$  выполнима  $\Leftrightarrow \neg A$  — не тавтология.

**Определение 8.** Формулы  $A$  и  $B$  называются *равносильными* (или *эквивалентными*), если при всех оценках их значения совпадают.

Равносильность формул обозначается знаком  $\sim$ .<sup>5</sup>

Из леммы 2.2 сразу получаем, что формулы от одних и тех же переменных равносильны, если и только если (тождественно) совпадают их булевы функции.<sup>6</sup>

$$A(P_1, \dots, P_n) \sim B(P_1, \dots, P_n) \Leftrightarrow \varphi_A^n \equiv \varphi_B^n.$$

Также очевидно, что отношение равносильности рефлексивно, симметрично и транзитивно.

Обозначим через  $\top$  формулу  $P_1 \rightarrow P_1$ , а через  $\perp$  — формулу  $P_1 \wedge \neg P_1$ .

<sup>4</sup>На самом деле неважно, каковы значения при  $i > n$  (лемма 2.2).

<sup>5</sup>Это тоже символ метаязыка.

<sup>6</sup> $\equiv$  обозначает совпадение функций при всех значениях аргумента. Часто пишут ‘=’ вместо  $\equiv$ .

**Лемма 2.3.**

- (1)  $A \sim B \Leftrightarrow ((A \rightarrow B) \wedge (B \rightarrow A))$  — тавтология.  
 (2)  $A$  — тавтология  $\Leftrightarrow A \sim \top$ .

**Доказательство** (1) Заметим, что

$$f(A) = f(B) \Leftrightarrow f((A \rightarrow B) \wedge (B \rightarrow A)) = 1.$$

Действительно,

$$f((A \rightarrow B) \wedge (B \rightarrow A)) = 1 \Leftrightarrow f(A \rightarrow B) = f(B \rightarrow A) = 1$$

Обе эти импликации истинны только в двух случаях: когда формулы  $A, B$  обе истинны или обе ложны, т.е. когда  $f(A) = f(B)$ .

(2) совсем очевидно: тавтологичность  $A$  как раз и означает, что  $A$  равносильна формуле  $\top$ , которая всегда истинна. ■

Приведем список некоторых равносильностей; проверка их предлагается в качестве упражнения.

**Лемма 2.4.**

- (1)  $A \wedge B \sim B \wedge A, A \vee B \sim B \vee A$  (коммутативность).  
 (2)  $(A \wedge B) \wedge C \sim A \wedge (B \wedge C), (A \vee B) \vee C \sim A \vee (B \vee C)$  (ассоциативность).  
 (3)  $A \wedge A \sim A, A \vee A \sim A$  (идемпотентность).  
 (4)  $A \wedge (B \vee C) \sim (A \wedge B) \vee (A \wedge C), A \vee (B \wedge C) \sim (A \vee B) \wedge (A \vee C)$  (дистрибутивность).  
 (5)  $A \vee (A \wedge B) \sim A, A \wedge (A \vee B) \sim A$  (поглощение).  
 (6)  $A \wedge \neg A \sim \perp, A \vee \perp \sim A,$   
 $A \vee \neg A \sim \top, A \wedge \top \sim A.$   
 (7)  $\neg(A \vee B) \sim \neg A \wedge \neg B, \neg(A \wedge B) \sim \neg A \vee \neg B$  (законы Де Моргана).  
 (8)  $\neg\neg A \sim A$  (закон двойного отрицания).  
 (9)  $A \rightarrow B \sim \neg A \vee B.$

**Лемма 2.5.** Для любого вектора  $\vec{x} \in \mathbb{B}^n$  можно построить сигнальную формулу  $A_{\vec{x}}(P_1, \dots, P_n)$ , для которой

$$\varphi_{A_{\vec{x}}}^n(\vec{y}) = 1 \Leftrightarrow \vec{x} = \vec{y}.$$

Иными словами, таблица истинности  $A_{\vec{x}}$  содержит 1 только в строке  $\vec{x}$ .

**Доказательство** Для переменной  $P$  обозначим  $P^1 = P, P^0 = \neg P$ .

Очевидно, что для любой оценки  $f$  и  $s \in \mathbb{B}$

$$f(P^s) = 1 \Leftrightarrow f(P) = s.$$

Теперь для  $\vec{x} = (x_1, \dots, x_n)$  можно взять

$$A_{\vec{x}} = P_1^{x_1} \wedge \dots \wedge P_n^{x_n}.$$

В самом деле, для любой оценки  $f$

$$\begin{aligned} f(A_{\vec{x}}) = 1 &\Leftrightarrow (\text{так как } A_{\vec{x}} \text{ — конъюнкция}) \forall i < n \ f(P_i^{x_i}) = 1 \\ &\Leftrightarrow (\text{по замечанию выше}) \forall i < n \ f(P_i) = x_i. \end{aligned}$$

Таким образом, в таблице истинности для  $A_{\vec{x}}$  значение 1 появляется только в строке  $\vec{x}$ . ■

**Теорема 2.6** (Теорема о функциональной полноте). Любая булева функция отвечает формуле логики высказываний, точнее:

для любой функции  $\alpha : \mathbb{B}^n \rightarrow \mathbb{B}$  существует формула  $A(P_1, \dots, P_n)$ , такая что  $\varphi_A \equiv \alpha$ .

**Доказательство** Сначала рассмотрим случай, когда  $\alpha$  не всюду равна 0. Тогда положим

$$A = \bigvee \{A_{\vec{x}} \mid \alpha(\vec{x}) = 1\}.$$

Это означает дизъюнкцию нескольких формул вида  $A_{\vec{x}}$  — по всем векторам  $\vec{x}$ , на которых функция  $\alpha$  равна 1 (дизъюнкция одной формулы — это сама формула).

Докажем, что  $\varphi_A \equiv \alpha$ . Действительно,

$$\varphi_A(\vec{y}) = 1 \Leftrightarrow f_{\vec{y}}(A) = 1$$

по определению функции  $\varphi_A$  (определение 6). Но  $A$  — это дизъюнкция формул вида  $A_{\vec{x}}$ , поэтому

$$f_{\vec{y}}(A) = 1 \Leftrightarrow \exists \vec{x} (\alpha(\vec{x}) = 1 \text{ и } f_{\vec{y}}(A_{\vec{x}}) = 1).$$

По лемме 2.5,

$$f_{\vec{y}}(A_{\vec{x}}) = 1 \Leftrightarrow \vec{y} = \vec{x}.$$

Получаем:

$$\varphi_A(\vec{y}) = 1 \Leftrightarrow \exists \vec{x} (\alpha(\vec{x}) = 1 \text{ и } \vec{y} = \vec{x}) \Leftrightarrow \alpha(\vec{y}) = 1.$$

Таким образом, функции  $\varphi_A$  и  $\alpha$  принимают значение 1 в одних и тех же точках. Во всех остальных точках значение равно 0. Следовательно,  $\varphi_A \equiv \alpha$ .

Если же  $\alpha \equiv 0$ , то можно использовать формулу  $\perp$ . Она ложна при всех оценках, а потому  $\varphi_{\perp} \equiv \alpha$ . ■

## Лекция 3

### Нормальные формы

**Определение 9.** *Литерал* — это переменная или ее отрицание. *Элементарная конъюнкция от переменных*  $P_1, \dots, P_n$  — это конъюнкция литералов, построенных из этих переменных, в которой каждая переменная встречается ровно 1 раз.

Из определения ясно, что любая элементарная конъюнкция от  $P_1, \dots, P_n$  равносильна сигнальной формуле вида  $A_{\vec{x}}$ , где  $\vec{x}$  — двоичный вектор длины  $n$  (см. лекцию 2). Строго говоря, формула  $A_{\vec{x}}$  определена неоднозначно: в конъюнкции можно по-разному расставить скобки. Для единообразия будем записывать скобки слева направо:

$$A_{\vec{x}} = (\dots (P_1^{x_1} \wedge P_2^{x_2}) \dots \wedge P_{n-1}^{x_{n-1}}) \wedge P_n^{x_n}.$$

В дальнейшем будем считать, что все элементарные конъюнкции имеют такой вид.

**Определение 10.** *Совершенная дизъюнктивная нормальная форма* (СДНФ) от переменных  $P_1, \dots, P_n$  — это дизъюнкция различных элементарных конъюнкций от этих переменных.

Сюда включаются частные случаи: когда дизъюнкция берется по множеству, состоящему из одной формулы, а также случай пустой дизъюнкции — ее считаем равной  $\perp$ .

### Теорема 3.1.

- (1) Каждая формула, построенная из переменных  $P_1, \dots, P_n$ , равносильна некоторой СДНФ от этих переменных.
- (2) Каждая формула равносильна единственной СДНФ (с точностью до перестановок и расстановки скобок в дизъюнкциях):

$$\text{если } \bigvee_{\vec{x} \in I} A_{\vec{x}} \sim \bigvee_{\vec{x} \in J} A_{\vec{x}}, \text{ то } I = J.$$

**Доказательство** (1) уже доказано в процессе доказательства теоремы 2.6.

(2) Докажем единственность (это почти уже сделано). Заметим, что запись  $\bigvee_{\vec{x} \in I} A_{\vec{x}}$  не задает формулу однозначно, пока не определена расстановка скобок и порядок членов дизъюнкции. Для однозначности можно, например, считать, что скобки расставлены слева направо, а порядок членов определяется, исходя из порядка на множестве  $\mathbb{B}^n$  всех двоичных векторов  $\vec{x}$ . Порядок на  $\mathbb{B}^n$  можно задать, как в двоичной системе счисления:  $(0, \dots, 0, 0)$  — наименьший,  $(0, \dots, 0, 1)$  — следующий, и т.д.

Обозначим эту дизъюнкцию через  $A_I$ . Ее булева функция равна 1 в точности на множестве  $I$ :

$$\varphi_{A_I}(\vec{y}) = \begin{cases} 1, & \text{если } y \in I, \\ 0, & \text{если } y \notin I. \end{cases}$$

Действительно,

$$\begin{aligned} \varphi_{A_I}(\vec{y}) = 1 &\Leftrightarrow f_{\vec{y}}(A_I) = 1 \Leftrightarrow \exists \vec{x} \in I f_{\vec{y}}(A_{\vec{x}}) = 1 \text{ (т.к. } A_I \text{ — дизъюнкция)} \\ &\Leftrightarrow \exists \vec{x} \in I \vec{y} = \vec{x} \text{ (по лемме 2.5)} \Leftrightarrow y \in I. \end{aligned}$$

Поэтому, если  $I \neq J$ , то  $A_I \not\sim A_J$ : у них разные булевы функции. ■

По аналогии с элементарными конъюнкциями, можно определить *элементарные дизъюнкции*: они имеют вид  $P_1^{x_1} \vee \dots \vee P_n^{x_n}$ . И соответственно определяем *совершенную конъюнктивную нормальную форму* (СКНФ) (от  $P_1, \dots, P_n$ ) как конъюнкцию элементарных дизъюнкций (причем пустая конъюнкция считается равной  $\top$ ).

Справедлива следующая

**Теорема** (об СКНФ).

- (1) Каждая формула, построенная из переменных  $P_1, \dots, P_n$ , равносильна некоторой СКНФ от этих переменных.
- (2) Каждая формула равносильна единственной СКНФ, с точностью до перестановок и расстановки скобок в конъюнкциях и дизъюнкциях.

Дополнительная задача Докажите эту теорему.

## Двойственность

**Определение 11.** Для формулы  $A$ , построенной из  $\wedge, \vee, \neg$ , *двойственная формула*  $A^*$  получается заменой всех  $\wedge$  на  $\vee$  и наоборот. Более формальное определение  $A^*$  — по индукции:

$$\begin{aligned} A^* &= A && \text{для } A \in Var, \\ (A \wedge B)^* &= (A^* \vee B^*), \\ (A \vee B)^* &= (A^* \wedge B^*), \\ (\neg A)^* &= \neg A^*. \end{aligned}$$

**Теорема** (о двойственности). Если  $A \sim B$ , то  $A^* \sim B^*$ . В частности, если  $\vDash A$  (т.е.  $A \sim \top$ ), то  $\vDash \neg A^*$  (т.е.  $A^* \sim \top^* \sim \perp$ ).

Дополнительная задача Докажите эту теорему.

## Булевы алгебры

По аналогии с двузначными оценками и таблицами истинности, для логических связок  $\neg, \vee, \wedge$  можно построить таблицы с несколькими значениями истинности. Если желательно, чтобы сохранились основные свойства этих связок, мы приходим к понятию булевой алгебры.

**Определение 12.** Булевой алгеброй называется непустое множество с заданными на нем операциями и выделенными элементами  $(\mathcal{B}, \sqcup, \sqcap, -, \mathbf{0}, \mathbf{1})$ <sup>7</sup>, где

<sup>7</sup>В каждой алгебре имеются свои операции, поэтому точнее были бы обозначения  $\sqcup_{\mathcal{B}}, \sqcap_{\mathcal{B}}$  и т.д. Но для удобства мы опускаем индекс  $\mathcal{B}$ .

- $\sqcup, \sqcap$  — двуместные операции на  $\mathcal{B}$ ,
- $-$  — одноместная операция на  $\mathcal{B}$ ,
- $\mathbf{0}, \mathbf{1} \in \mathcal{B}$ ,

причем выполняются следующие свойства (см. лемму 2.4):

- (1)  $x \sqcup y = y \sqcup x$ ,  $x \sqcap y = y \sqcap x$  (коммутативность),
- (2)  $(x \sqcup y) \sqcup z = x \sqcup (y \sqcup z)$ ,  $(x \sqcap y) \sqcap z = x \sqcap (y \sqcap z)$  (ассоциативность),
- (3)  $x \sqcup x = x$ ,  $x \sqcap x = x$  (идемпотентность),
- (4)  $(x \sqcup y) \sqcap z = (x \sqcap y) \sqcup (x \sqcap z)$ ,  $(x \sqcap y) \sqcup z = (x \sqcup z) \sqcap (y \sqcup z)$  (дистрибутивность),
- (5)  $(x \sqcup y) \sqcap x = x$ ,  $(x \sqcap y) \sqcup x = x$  (поглощение),
- (6)  $x \sqcap -x = \mathbf{0}$ ,  $x \sqcup \mathbf{0} = x$ ,  $x \sqcup -x = \mathbf{1}$ ,  $x \sqcap \mathbf{1} = x$  (свойства  $\mathbf{0}$  и  $\mathbf{1}$ ),
- (7)  $-(x \sqcup y) = -x \sqcap -y$ ,  $-(x \sqcap y) = -x \sqcup -y$  (законы Де Моргана),
- (8)  $--x = x$  (закон двойного дополнения).

Операции  $\sqcup, \sqcap, -$  называются соответственно *булевой суммой* (или *объединением*), *булевым произведением* (или *пересечением*) и *дополнением*.  $\mathbf{0}, \mathbf{1}$  называются *нулем* и *единицей*.

Список основных тождеств, задающих булевы алгебры, в действительности можно сократить. Например, можно ограничиться только (1), (2), (5), (6) и одним из (4); остальные тождества следуют из этих.

В частности, идемпотентность получается так:

$$x = x \sqcap (x \sqcup \mathbf{0}) \text{ (по (5))} = x \sqcap x \text{ (по (6))}.$$

А закон двойного дополнения — так:

$$\begin{aligned} --x &= --x \sqcap \mathbf{1} = --x \sqcap (x \sqcup -x) = (--x \sqcap x) \sqcup (--x \sqcap -x) \\ &= (--x \sqcap x) \sqcup \mathbf{0} = --x \sqcap x \text{ (по (6), (4), (1));} \\ &\text{с другой стороны,} \\ x &= x \sqcap \mathbf{1} = --x \sqcap (-x \sqcup --x) = (x \sqcap -x) \sqcup (x \sqcap --x) \\ &= \mathbf{0} \sqcup (x \sqcap --x) = x \sqcap --x \text{ (тоже по (6), (4), (1));} \\ &\text{отсюда } --x = x. \end{aligned}$$

**Пример 1** Тривиальный пример булевой алгебры — одноэлементная алгебра (она обозначается  $\mathbf{1}$ ). В ней  $\mathbf{0} = \mathbf{1}$  и все операции дают  $\mathbf{1}$ ; тогда тождества из определения 12 очевидны.

**Пример 2** Двухэлементная булева алгебра  $\mathcal{2}$  на множестве  $\mathbb{B} = \{0, 1\}$ :

$$\mathcal{2} = (\{0, 1\}, \odot, \otimes, \ominus, 0, 1),$$

где  $x \odot y = \max(x, y)$ ,  $x \otimes y = \min(x, y)$ ,  $\ominus x = 1 - x$  (см. лекцию 1). То, что  $\mathcal{2}$  — булева алгебра, фактически доказано в лемме 2.4.

**Пример 3** Стандартный пример булевой алгебры — множество  $\mathcal{P}(E)$  всех подмножеств данного множества  $E$  с обычными операциями объединения, пересечения, дополнения (до  $E$ ) и  $\emptyset, E$  в качестве  $\mathbf{0}, \mathbf{1}$ .

**Предложение 3.2.** Пусть  $E$  — произвольное множество. Тогда  $(\mathcal{P}(E), \cup, \cap, -, \emptyset, E)$  (где  $-A = E \setminus A$ ) — булева алгебра.

**Доказательство** Надо проверить булевы тождества для  $\mathcal{P}(E)$ . При этом можно использовать равносильности из леммы 2.4.

Например, дистрибутивность

$$(x \cup y) \cap z = (x \cap z) \cup (y \cap z)$$



означает, что для любого  $a \in E$

$$(\bullet) \quad a \in (x \cup y) \cap z \Leftrightarrow a \in (x \cap z) \cup (y \cap z).$$

Чтобы это проверить, возьмем произвольное  $a$  и рассмотрим пропозициональные переменные  $P, Q, R$ , которые оценим соответственно как  $a \in x$ ,  $a \in y$ ,  $a \in z$ . Т.е. выберем оценку  $f$  такую, что

$$f(P) = 1 \Leftrightarrow a \in x; \quad f(Q) = 1 \Leftrightarrow a \in y; \quad f(R) = 1 \Leftrightarrow a \in z.$$

Тогда

$$a \in (x \cup y) \cap z \Leftrightarrow ((a \in x \text{ или } a \in y) \text{ и } a \in z) \Leftrightarrow f((P \vee Q) \wedge R) = 1,$$

и аналогично,

$$a \in (x \cap z) \cup (y \cap z) \Leftrightarrow f((P \wedge R) \vee (Q \wedge R)) = 1.$$

Но из леммы 2.4 мы знаем, что формулы  $(P \vee Q) \wedge R$  и  $(P \wedge R) \vee (Q \wedge R)$  равносильны (т.е. одновременно истинны или одновременно ложны). Отсюда следует  $(\bullet)$ .

Так же поступаем и с другими булевыми тождествами для  $\mathcal{P}(E)$ ; они превращаются в равносильности из леммы 2.4, если знаки  $\cup, \cap, -$  заменить соответственно на  $\vee, \wedge, \neg$ . ■

**Определение 13.** Изоморфизм булевых алгебр — это биекция, сохраняющая все операции.

Точнее, пусть  $\mathcal{A}, \mathcal{B}$  — булевы алгебры. Биекция  $\varphi : \mathcal{A} \rightarrow \mathcal{B}$  называется *изоморфизмом  $\mathcal{A}$  на  $\mathcal{B}$* , если  $\varphi(\mathbf{0}_{\mathcal{A}}) = \mathbf{0}_{\mathcal{B}}$ ,  $\varphi(\mathbf{1}_{\mathcal{A}}) = \mathbf{1}_{\mathcal{B}}$  и для всех  $x, y \in \mathcal{A}$

$$\varphi(x \sqcup_{\mathcal{A}} y) = \varphi(x) \sqcup_{\mathcal{B}} \varphi(y), \quad \varphi(x \sqcap_{\mathcal{A}} y) = \varphi(x) \sqcap_{\mathcal{B}} \varphi(y), \quad \varphi(-_{\mathcal{A}} x) = -_{\mathcal{B}} \varphi(x).$$

Если существует изоморфизм  $\mathcal{A}$  на  $\mathcal{B}$ , то алгебры  $\mathcal{A}, \mathcal{B}$  называются *изоморфными*.

Как легко видеть, изоморфность — отношение эквивалентности между алгебрами<sup>8</sup>.

В частности, алгебра  $\mathcal{2}$  изоморфна алгебре  $\mathcal{P}(\{a\})$  подмножеств 1-элементного множества, а тривиальная алгебра  $\mathcal{1}$  изоморфна алгебре  $\mathcal{P}(\emptyset)$ .

**Лемма 3.3.** В булевой алгебре можно определить частичный порядок, положив

$$a \leq b \Leftrightarrow a = (a \sqcap b).$$

Относительно этого порядка  $\mathbf{0}$  является наименьшим элементом,  $\mathbf{1}$  — наибольшим элементом.

**Доказательство**

- Рефлексивность  $a = a \sqcap a$  — это идемпотентность  $\sqcap$ .
- Транзитивность получается из ассоциативности:  
если  $a = a \sqcap b$  и  $b = b \sqcap c$ , то

$$a = a \sqcap b = a \sqcap (b \sqcap c) = (a \sqcap b) \sqcap c = a \sqcap c.$$

- Антисимметричность следует из коммутативности:  
если  $a = a \sqcap b$  и  $b = b \sqcap a$ , то  $a = b$ .
- $\mathbf{1}$  — наибольший:  $a = a \sqcap \mathbf{1}$  — по определению 12.
- $\mathbf{0}$  — наименьший, т.е.  $\mathbf{0} = \mathbf{0} \sqcap a$ . Это получается так:

$$\mathbf{0} \sqcap a = (-a \sqcap a) \sqcap a = -a \sqcap (a \sqcap a) = -a \sqcap a = \mathbf{0}.$$

■

<sup>8</sup>В более общем контексте понятие изоморфизма будет обсуждаться позже.

Если алгебра содержит более 2 элементов, то этот порядок — не линейный.

**Лемма 3.4.**  $a \leq b \Leftrightarrow -a \sqcup b = \mathbf{1}$ .

**Доказательство** ( $\Leftarrow$ ). Пусть  $-a \sqcup b = \mathbf{1}$ . Тогда

$$a = a \sqcap \mathbf{1} = a \sqcap (-a \sqcup b) = (a \sqcap (-a)) \sqcup (a \sqcap b) = \mathbf{0} \sqcup (a \sqcap b) = a \sqcap b.$$

по свойствам  $\mathbf{1}$ ,  $\mathbf{0}$  и дистрибутивности. Значит,  $a \leq b$ .

( $\Rightarrow$ ). Пусть  $a \leq b$ , т.е.  $a = a \sqcap b$ . Тогда

$$-a \sqcup b = -(a \sqcap b) \sqcup b = -a \sqcup -b \sqcup b = -a \sqcup \mathbf{1}$$

по закону Де Моргана и свойству  $\mathbf{1}$ . И заметим еще, что

$$-a \sqcup \mathbf{1} = -a \sqcup (-a \sqcup a) = (-a \sqcup -a) \sqcup a = -a \sqcup a = \mathbf{1}.$$

Следовательно,  $-a \sqcup b = \mathbf{1}$ . ■

**Определение 14.** Оценка в булевой алгебре  $\mathcal{B}$  — это отображение  $f : Var \rightarrow \mathcal{B}$ .

По аналогии с леммой 2.1, получаем:

**Лемма 3.5.** Для любой оценки  $f : Var \rightarrow \mathcal{B}$  существует единственное отображение  $\bar{f} : Fm \rightarrow \mathcal{B}$ , такое что для всех  $A, B \in Fm$

- (1)  $\bar{f}(A) = f(A)$ , если  $A \in Var$ ,
- (2)  $\bar{f}(A \wedge B) = \bar{f}(A) \sqcap \bar{f}(B)$ ,
- (3)  $\bar{f}(A \vee B) = \bar{f}(A) \sqcup \bar{f}(B)$ ,
- (4)  $\bar{f}(\neg A) = -\bar{f}(A)$ ,
- (5)  $\bar{f}(A \rightarrow B) = \bar{f}(\neg A \vee B) = -\bar{f}(A) \sqcup \bar{f}(B)$ .

Доказательство полностью аналогично лемме 2.1 (по индукции, используя однозначность анализа формул).

Как и в случае оценок в 2, пишем  $f(A)$  вместо  $\bar{f}(A)$ ;  $f(A)$  называется значением  $A$  в алгебре  $\mathcal{B}$  при оценке  $f$ .

**Определение 15.** Формулы  $A, B$  называются равносильными (эквивалентными) в булевой алгебре  $\mathcal{B}$ , если их значения в  $\mathcal{B}$  совпадают при всех оценках; обозначение:  $A \sim_{\mathcal{B}} B$ .

Формула  $A$  называется общезначимой в булевой алгебре  $\mathcal{B}$ , если ее значение в  $\mathcal{B}$  равно  $\mathbf{1}$  при любой оценке; обозначение:  $\mathcal{B} \vDash A$ .

Ясно, что равносильность и общезначимость в алгебре  $\mathcal{B}$  — это обычные равносильность ( $\sim$ ) и тавтологичность ( $\vDash$ ); они определялись в лекции 2.

Аналогично лемме 2.3, получаем:

**Лемма 3.6.**

- (1)  $A \sim_{\mathcal{B}} B \Leftrightarrow \mathcal{B} \vDash ((A \rightarrow B) \wedge (B \rightarrow A))$ .
- (2)  $\mathcal{B} \vDash A \Leftrightarrow A \sim_{\mathcal{B}} \top$ .

**Доказательство** Как и в лемме 2.3, проверяем, что для любой оценки  $f$ ,

$$f(A) = f(B) \Leftrightarrow f((A \rightarrow B) \wedge (B \rightarrow A)) = \mathbf{1}.$$

Обозначим  $a := f(A)$ ,  $b := f(B)$ . Нам надо показать, что

$$a = b \Leftrightarrow (a \oplus b) \sqcap (b \oplus a) = \mathbf{1},$$

где  $a \oplus b := -a \sqcup b$ .

Утверждение ( $\Rightarrow$ ) очевидно:  $a \oplus a = -a \sqcup a = \mathbf{1}$ ,  $\mathbf{1} \sqcap \mathbf{1} = \mathbf{1}$  по определению 12.  
 Чтобы доказать ( $\Leftarrow$ ), заметим сначала, что

$$x \sqcap y = \mathbf{1} \Rightarrow x = y = \mathbf{1}.$$

Действительно,  $x \sqcap y \leq x$ ,  $x \sqcap y \leq y$ , а  $\mathbf{1}$  — наибольший элемент (относительно  $\leq$ ).

Поэтому

$$(a \oplus b) \sqcap (b \oplus a) = \mathbf{1} \Rightarrow -a \sqcup b = -b \sqcup a = \mathbf{1}.$$

По лемме 3.4 из  $-a \sqcup b = -b \sqcup a = \mathbf{1}$  следует  $a \leq b$  и  $b \leq a$ , т.е.  $a = b$ . ■

Минимальные ненулевые элементы относительно порядка  $\leq$  в булевой алгебре называются *атомами*; их может быть несколько, а может не быть вообще.

Справедлива следующая теорема (в курсе не доказывается):

**Теорема 3.7** (Теорема Стоуна (\*)).

- (1) Всякая булева алгебра изоморфна алгебре множеств, т.е. подалгебре некоторой алгебры  $\mathcal{P}(E)$ .
- (2) Всякая конечная булева алгебра изоморфна алгебре вида  $\mathcal{P}(E)$ , и следовательно, состоит из  $2^n$  элементов для некоторого  $n$ .

В конечном случае в качестве  $E$  можно взять множество всех атомов данной алгебры.

Дополнительная задача Докажите часть (2) в теореме Стоуна.

Заметим, что не все булевы алгебры имеют вид  $\mathcal{P}(E)$ .

Пример 4 Рассмотрим, например, такое множество подмножеств натурального ряда:

$$\{V \subseteq \mathbb{N} \mid V \text{ конечно или } \mathbb{N} \setminus V \text{ конечно}\}.$$

В него входят  $\emptyset$  и  $\mathbb{N}$ . Очевидно, что оно замкнуто относительно дополнений, и нетрудно проверить, что оно замкнуто относительно объединений и пересечений, поэтому получается счетная подалгебра алгебры  $\mathcal{P}(\mathbb{N})$ .

Однако никакая алгебра  $\mathcal{P}(E)$  не может быть счетной: такие алгебры конечны при конечном  $E$  и несчетны при бесконечном  $E$  — в силу теоремы Кантора (которая будет обсуждаться в этом курсе позже).

Пример 5 Алгебра Линденбаума — Тарского.

Рассмотрим множество классов всех пропозициональных формул по отношению равносильности  $\mathcal{L} = \text{Fm}/\sim$ . Пусть  $\tilde{A}$  обозначает класс формулы  $A$ . Тогда определим

$$\mathbf{0} := \tilde{\perp}, \quad \mathbf{1} := \tilde{\top}, \quad \tilde{A} \sqcup \tilde{B} := \widetilde{A \vee B}, \quad \tilde{A} \sqcap \tilde{B} := \widetilde{A \wedge B}, \quad -\tilde{A} := \widetilde{\neg A}.$$

Корректность этого определения следует из того, что равносильность согласована с логическими связками: если  $A \sim A'$  и  $B \sim B'$ , то  $A \vee B \sim A' \vee B'$  и т.д.

Лемма 2.4 показывает, что  $\mathcal{L}$  — булева алгебра. Эта алгебра счетна, и в ней, как можно доказать, атомов нет (в отличие от примера 4).

Дополнительная задача Докажите последнее утверждение.

## Лекция 4

**Теорема 4.1.** Для любой нетривиальной булевой алгебры  $\mathcal{B}$  и формулы  $A$

$$\mathcal{B} \models A \Rightarrow \mathcal{2} \models A.$$

**Доказательство** Пусть  $\mathcal{B} \models A$ . Возьмем оценку  $f : Var \rightarrow \mathcal{2}$ , и рассмотрим “такую же” оценку в  $\mathcal{B}$ , т.е.  $F : Var \rightarrow \mathcal{B}$ , где

$$F(P_i) = \mathbf{1} \Leftrightarrow f(P_i) = 1$$

для каждого  $i$ . Из свойств булевых алгебр получаем:

$$\mathbf{0} \sqcup \mathbf{1} = \mathbf{1} \sqcup \mathbf{0} = \mathbf{1}, \quad \mathbf{0} \sqcup \mathbf{0} = \mathbf{0}, \quad \mathbf{1} \sqcup \mathbf{1} = \mathbf{1},$$

и аналогично для  $\sqcap$ .

Кроме того,

$$-\mathbf{0} = \mathbf{1}, \text{ т.к. } \mathbf{1} = \mathbf{0} \sqcup -\mathbf{0} = -\mathbf{0},$$

$$-\mathbf{1} = \mathbf{0}, \text{ т.к. } \mathbf{0} = \mathbf{1} \sqcap -\mathbf{1} = -\mathbf{1}.$$

Отсюда мы видим, что  $\mathbf{0}, \mathbf{1}$  образуют подалгебру в  $\mathcal{B}$ , изоморфную  $\mathcal{2}$ . Обозначим этот изоморфизм через  $\approx$ , т.е. пусть

$$\mathbf{1} \approx 1, \quad \mathbf{0} \approx 0.$$

Тогда для всех  $i$

$$F(P_i) \approx f(P_i),$$

откуда по индукции имеем для любой формулы  $B$

$$F(B) \approx f(B).$$

Здесь надо разбирать все случаи построения  $B$ , но это — рутинная проверка. Например, пусть  $B = C \vee D$ . Тогда  $F(B) = F(C) \sqcup F(D)$ ,  $f(B) = \max(f(C), f(D))$ , и если  $F(C) \approx f(C)$ ,  $F(D) \approx f(D)$ , то  $F(C) \sqcup F(D) \approx \max(f(C), f(D))$ . Это получается из равенств

$$\mathbf{0} \sqcup \mathbf{1} = \mathbf{1} \sqcup \mathbf{0} = \mathbf{1}, \quad \mathbf{0} \sqcup \mathbf{0} = \mathbf{0}, \quad \mathbf{1} \sqcup \mathbf{1} = \mathbf{1}.$$

Теперь для исходной формулы  $A$  получаем  $f(A) = 1$ , поскольку  $F(A) = \mathbf{1}$ .

Таким образом,  $\mathcal{2} \models A$ . ■

## Исчисление высказываний

Различные тавтологии можно получать как теоремы в некоторой аксиоматической системе — исчислении высказываний. Имеются разные варианты таких исчислений. Мы будем рассматривать исчисление *гильбертовского типа*. Оно задается множеством *аксиом* и *правил вывода*; теоремы выводятся из аксиом с помощью правил. В процессе вывода возникает *доказательство* — некоторая последовательность формул.

Приведем одну из формулировок исчисления высказываний (CL).

Схемы аксиом

- (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)  $(A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow (A \vee B \rightarrow C))$

$$(9) (A \rightarrow \neg B) \rightarrow ((A \rightarrow B) \rightarrow \neg A)$$

$$(10) \neg\neg A \rightarrow A$$

Здесь  $A, B, C$  — произвольные формулы. Поэтому каждая из схем (1)–(10) порождает бесконечную серию аксиом. Например, схема (1) задает аксиомы вида  $A \rightarrow (B \rightarrow A)$  и т.д.

Единственное правило вывода — Modus Ponens (MP), которое записывается так:

$$\frac{A, A \rightarrow B}{B}.$$

Эта запись означает, что если доказаны формулы  $A$  и  $A \rightarrow B$ , то можно доказать  $B$ .

Формальное понятие доказательства определяется следующим образом.

**Определение 16.** *Доказательство* (или *вывод*) формулы  $A$  в  $CL$  — это конечная последовательность формул, каждая из которых — аксиома или получается из предыдущих по правилу MP и которая заканчивается формулой  $A$ .

Точнее: доказательство — это такая последовательность формул

$A_1, \dots, A_n = A$ , что для всех  $k$  ( $1 \leq k \leq n$ )  $A_k$  — аксиома или существуют  $i, j < k$ , для которых  $A_j = A_i \rightarrow A_k$ .

Действительно, из  $A_i$  и  $A_i \rightarrow A_k$  по MP получается как раз  $A_k$ .

Любое математическое доказательство можно организовать аналогичным образом, если включить в него все промежуточные доказательства и выбрать подходящую систему аксиом и правил вывода (исчисления высказываний здесь уже не хватит). Однако на практике так не происходит, потому что доказательства упрощаются и сокращаются.

Формула  $A$ , для которой существует доказательство в  $CL$ , называется *теоремой  $CL$* , или *выводимой* в  $CL$ ; это записывается так:  $\vdash_{CL} A$ . Индекс  $CL$  не пишем, если ясно, что речь идет об этой системе.

Пример 1  $\vdash A \vee B \rightarrow B \vee A$ .

Приведем доказательство (с комментариями). Для удобства обозначим формулу  $B \vee A$  через  $C$ .

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

Формула 5 и есть нужная теорема.

Пример 2  $\vdash A \rightarrow A$ . Обозначим эту формулу  $B$ .

1.  $A \rightarrow B$  (аксиома 1)
2.  $A \rightarrow (B \rightarrow A)$  (аксиома 1)
3.  $(A \rightarrow (B \rightarrow A)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow A))$  (аксиома 2)
4.  $(A \rightarrow B) \rightarrow (A \rightarrow A)$  (2,3, MP)
5.  $A \rightarrow A$  (1,4, MP)

Расширим теперь определение вывода 16.

**Определение 17.** Пусть  $\Gamma$  — какое-то множество пропозициональных формул. *Вывод из  $\Gamma$*  формулы  $A$  в  $CL$  — это конечная последовательность формул, каждая из которых — аксиома или принадлежит  $\Gamma$  или получается из предыдущих по правилу MP и которая заканчивается формулой  $A$ .

Т.е. это последовательность формул  $A_1, \dots, A_n$ , где для всех  $k$

$A_k$  — аксиома или  $A_k \in \Gamma$  или существуют  $i, j < k$ , для которых  $A_j = A_i \rightarrow A_k$ .

Формула  $A$  *выводима из  $\Gamma$* , если существует вывод из  $\Gamma$ , содержащий  $A$ ; обозначение:  $\Gamma \vdash_{CL} A$ .

Если рассматриваются выводы из  $\Gamma$ , то формулы из  $\Gamma$  называются *гипотезами*. В математике (и в практической жизни) такие выводы часто встречаются: мы делаем какие-то предположения (временно считая их аксиомами), и получаем из них различные следствия.

Очевидно, что если  $\Gamma = \emptyset$ , то вывод из  $\Gamma$  — это обычный вывод из заданных аксиом (в  $CL$ ).

**Лемма 4.2.**

- (1) Если  $\Delta \subseteq \Gamma$  и  $\Delta \vdash A$ , то  $\Gamma \vdash A$ .
- (2) Если  $\Gamma \vdash A$ , то существует конечное  $\Delta \subseteq \Gamma$ , для которого  $\Delta \vdash A$ .
- (3) (“транзитивность выводимости”, или “сечение”)  
Если  $\Gamma \vdash A$ , и  $\Delta \vdash B$  для всех  $B \in \Gamma$ , то  $\Delta \vdash A$ .

Если условие  $\Delta \vdash B$  для всех  $B \in \Gamma$  обозначить как  $\Delta \vdash \Gamma$ , то утверждение (3) запишется так:

$$\text{Если } \Delta \vdash \Gamma \text{ и } \Gamma \vdash A, \text{ то } \Delta \vdash A.$$

Отсюда название “транзитивность”.

**Доказательство** (1) очевидно.

(2) также очевидно: можно составить  $\Delta$  из тех гипотез, которые встречаются в выводе  $A$ ; их конечное число.

(3) Предположим, что  $\Delta \vdash \Gamma$  и  $\Gamma \vdash A$ . Из (2) следует, что можно заменить  $\Gamma$  на его конечное подмножество  $\Gamma_1$ , т.е. мы имеем

$$\Delta \vdash \Gamma_1, \Gamma_1 \vdash A.$$

Пусть  $\Gamma_1 = \{B_1, \dots, B_n\}$ . Пусть  $\Pi_i$  — вывод  $B_i$  из  $\Delta$ . Возьмем вывод  $A$  из  $\Gamma_1$ ; в нем встречаются какие-то гипотезы  $B_i$ :

$$\dots B_{i_1}, \dots, B_{i_2}, \dots, A.$$

Заменяем в этом выводе каждую  $B_i$  на ее вывод  $\Pi_i$ :

$$\dots \Pi_{i_1}, \dots, \Pi_{i_2}, \dots, A.$$

Получится вывод  $A$  из  $\Delta$ . Действительно, все формулы из исходного вывода, кроме гипотез  $B_i$ , — аксиомы  $CL$  или получаются из предыдущих по МР. А в каждом вставном выводе  $\Pi_i$  все формулы — аксиомы  $CL$  или входят в  $\Delta$  или получаются по МР из предыдущих (внутри того же вывода). ■

Вместо  $\{A_1, \dots, A_n\} \vdash_{CL} B$  обычно пишут  $A_1, \dots, A_n \vdash_{CL} B$ . Говорят также, что  $\frac{A_1, \dots, A_n}{B}$  — производное правило  $CL$ .

Если из выводимости формул  $A_1, \dots, A_n$  следует выводимость  $B$ , то говорят, что  $\frac{A_1, \dots, A_n}{B}$  — допустимое правило  $CL$ .

**Лемма 4.3.** Всякое производное правило  $CL$  допустимо.<sup>9</sup>

**Доказательство** Пусть  $\Gamma = \{A_1, \dots, A_n\} \vdash B$ . Тогда, если  $\emptyset \vdash \Gamma$ , то  $\emptyset \vdash B$  — по транзитивности выводимости: ■

Транзитивность выводимости означает, что уже доказанные теоремы можно использовать в новых выводах, не повторяя из доказательств. Полученные допустимые правила также можно применять для сокращения доказательств.

Пример 3 Допустимо правило введения конъюнкции

$$\frac{A, B}{A \wedge B}.$$

<sup>9</sup>Обратное утверждение (при некотором уточнении понятия “правило вывода”) тоже верно, но в этом курсе мы его не доказываем.

Действительно,  $A, B \vdash A \wedge B$ :

1.  $A$  (гипотеза)
2.  $B$  (гипотеза)
3.  $A \rightarrow (B \rightarrow A \wedge B)$  (аксиома 5)
4.  $B \rightarrow A \wedge B$  (1,3, МР)
5.  $A \wedge B$  (2,4, МР)

## Теорема о дедукции для исчисления высказываний

**Теорема 4.4** (Теорема<sup>10</sup> о дедукции).

$$\Gamma, A \vdash_{CL} B \quad \Leftrightarrow \quad \Gamma \vdash_{CL} A \rightarrow B.$$

Здесь  $\Gamma, A$  обозначает множество  $\Gamma \cup \{A\}$ .

**Доказательство** Утверждение ( $\Leftarrow$ ) почти очевидно. Действительно, пусть  $\Gamma \vdash A \rightarrow B$ . Тогда имеем  $\Gamma, A \vdash A, A \rightarrow B$  и  $A, A \rightarrow B \vdash B$  (МР). Отсюда по транзитивности  $\Gamma, A \vdash B$ .

Утверждение ( $\Rightarrow$ ) доказывается индукцией по длине вывода  $B$  из  $\Gamma, A$ .

(1) Если этот вывод — длины 1, то  $B$  — аксиома или гипотеза. Если  $B$  — аксиома, то имеем вывод  $A \rightarrow B$  (из  $\emptyset$ ):

1.  $B$  (аксиома)
2.  $B \rightarrow (A \rightarrow B)$  (аксиома 1)
3.  $A \rightarrow B$  (1,2, МР)

(2) Если  $B \in \Gamma$ , то имеем такой же вывод  $A \rightarrow B$  из  $\Gamma$ :

1.  $B$  (гипотеза)
2.  $B \rightarrow (A \rightarrow B)$  (аксиома 1)
3.  $A \rightarrow B$  (1,2, МР)

(3) Если  $B = A$ , то  $A \rightarrow B = A \rightarrow A$ . Но  $\vdash A \rightarrow A$  (пример 2 выше).

(4) Предположим теперь, что  $\Gamma, A \vdash B$  и утверждение ( $\Rightarrow$ ) верно для всех более коротких выводов, т.е.

для всех  $C$ , если  $\Gamma, A \vdash C$  и вывод  $C$  из  $\Gamma, A$  короче, чем вывод  $B$ , то  $\Gamma \vdash A \rightarrow C$ .

Докажем, что  $\Gamma \vdash A \rightarrow B$ .

Рассмотрим вывод из  $\Gamma, A$ , который заканчивается формулой  $B$ . При этом  $B$  может оказаться аксиомой или гипотезой (тогда все предыдущие формулы для доказательства  $B$  не нужны). Но в этом случае  $\Gamma \vdash A \rightarrow B$  по (1)–(3).

Остается случай, когда  $B$  получается по МР из формул  $C, C \rightarrow B$ , причем  $\Gamma, A \vdash C$  и  $\Gamma, A \vdash C \rightarrow B$  с более короткими доказательствами. По предположению индукции имеем

$$(*) \quad \Gamma \vdash A \rightarrow C, \quad A \rightarrow (C \rightarrow B).$$

С другой стороны,

$$(**) \quad A \rightarrow C, \quad A \rightarrow (C \rightarrow B) \vdash A \rightarrow B :$$

1.  $A \rightarrow C$  (гипотеза)
2.  $A \rightarrow (C \rightarrow B)$  (гипотеза)
3.  $(A \rightarrow (C \rightarrow B)) \rightarrow ((A \rightarrow C) \rightarrow (A \rightarrow B))$  (аксиома 2)
4.  $(A \rightarrow C) \rightarrow (A \rightarrow B)$  (2,3, МР)
5.  $A \rightarrow B$  (1,4, МР)

Из (\*), (\*\*) по транзитивности получаем  $\Gamma \vdash A \rightarrow B$ . ■

<sup>10</sup>Конечно, это — не теорема нашего формального исчисления, а утверждение о его свойствах (“метатеорема”).

Отметим частный случай теоремы о дедукции для  $\Gamma = \emptyset$ :

$$A \vdash B \Leftrightarrow \vdash A \rightarrow B.$$

Пример 4 Допустимо правило силлогизма

$$\frac{A \rightarrow B, B \rightarrow C}{A \rightarrow C}.$$

Покажем, что это — производное правило, т.е.

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

По теореме дедукции это равносильно

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

Последнее утверждение очевидно: надо два раза применить МР.

## Корректность исчисления высказываний для булевых алгебр

**Теорема 4.5.** Если  $\vdash_{CL} A$ , то  $\mathcal{B} \vDash A$  для любой булевой алгебры  $\mathcal{B}$ .

### Доказательство

Доказываем теорему индукцией по длине вывода  $A$ . Имеется 2 случая:

(I)  $A$  — аксиома.

(II)  $A$  получается по МР из формул  $B, B \rightarrow A$  с более короткими выводами.

Начнем с более простого случая (II). По предположению индукции,  $\mathcal{B} \vDash B, B \rightarrow A$ . Рассмотрим произвольную оценку  $f$  в  $\mathcal{B}$ ; пусть  $f(A) = a$ . Докажем, что  $a = \mathbf{1}$ .

Поскольку  $\mathcal{B} \vDash B, B \rightarrow A$ , имеем:  $f(B) = f(B \rightarrow A) = \mathbf{1}$ . Тогда

$$\mathbf{1} = f(B \rightarrow A) = f(B) \oplus f(A) = \mathbf{1} \oplus a.$$

По лемме 3.4  $\mathbf{1} \leq a$ , и значит,  $a = \mathbf{1}$ , т.к.  $\mathbf{1}$  — наибольший элемент.

В случае (I) надо доказывать общезначимость всех 10 аксиом. Это мы рассмотрим на следующей лекции. ■

## Лекция 5

### Корректность исчисления высказываний для булевых алгебр (окончание)

Продолжаем доказательство теоремы:

### Доказательство

Остается рассмотреть случаи, когда  $A$  — аксиома. Нам понадобится лемма о булевых алгебрах.

**Лемма 5.1.** В любой булевой алгебре

$$(1) x \leq x \sqcup y, y \leq x \sqcup y;$$

$$(2) \text{ если } x \leq z \text{ и } y \leq z, \text{ то } x \sqcup y \leq z;$$

$$(3) \text{ если } x \leq x' \text{ и } y \leq y', \text{ то } x \sqcup y \leq x' \sqcup y'.$$



**Доказательство** (1)  $x \sqcap (x \sqcup y) = x$  — поглощение и коммутативность; аналогично получаем  $y \sqcap (x \sqcup y) = y$ .

(2) Если  $x \sqcap z = x$ ,  $y \sqcap z = y$ , то по дистрибутивности

$$(x \sqcup y) \sqcap z = (x \sqcap z) \sqcup (y \sqcap z) = x \sqcup y.$$

(3) Пусть  $x \leq x'$  и  $y \leq y'$ . Тогда из (1) получаем

$$x \leq x' \leq x' \sqcup y', \quad y \leq y' \leq x' \sqcup y'.$$

Теперь, применив (2), имеем:

$$x \sqcup y \leq x' \sqcup y'.$$

■

Докажем теперь общезначимость аксиом  $CL$  в произвольной булевой алгебре  $\mathcal{B}$ .

Аксиома 1 Выберем оценку  $f$  в  $\mathcal{B}$ ; пусть  $f(A) = a$ ,  $f(B) = b$ . Нам надо доказать

$$a \oplus (b \oplus a) = \mathbf{1}.$$

По лемме 3.4 это равносильно

$$a \leq b \oplus a = -b \sqcup a.$$

Теперь можно применить лемму 5.1.

Общезначимость аксиом 3, 4, 6, 7, 10 проверяется легко (упражнение). Рассмотрим аксиомы 2, 8, 9.

Аксиома 2 Пусть дана оценка  $f$  в  $\mathcal{B}$ ,  $f(A) = a$ ,  $f(B) = b$ ,  $f(C) = c$ . Надо доказать

$$(a \oplus (b \oplus c)) \oplus ((a \oplus b) \oplus (a \oplus c)) = \mathbf{1}.$$

По лемме 3.4 это равносильно

$$a \oplus (b \oplus c) \leq (a \oplus b) \oplus (a \oplus c),$$

т.е.

$$-a \sqcup (-b \sqcup c) \leq -(a \sqcup b) \sqcup (-a \sqcup c),$$

или (применяя закон Де Моргана и ассоциативность)

$$-a \sqcup -b \sqcup c \leq (a \sqcap -b) \sqcup -a \sqcup c.$$

Благодаря почленному сложению неравенств (лемма 5.1 (3)), достаточно проверить

$$(*) \quad -b \leq (a \sqcap -b) \sqcup -a.$$

А это получается так:

$$-b = \mathbf{1} \sqcap (-b) = (a \sqcup -a) \sqcap (-b) = (a \sqcap -b) \sqcup (-a \sqcap -b) \leq (a \sqcap -b) \sqcup (-a)$$

— опять по лемме 5.1.

Аксиома 9 Надо доказать

$$(a \oplus -b) \oplus ((a \oplus b) \oplus -a) = \mathbf{1}.$$

Заметим, что

$$a \oplus \mathbf{0} = -a \sqcup \mathbf{0} = -a.$$

Значит, надо проверить, что

$$(a \oplus (b \oplus \mathbf{0})) \oplus ((a \oplus b) \oplus (a \oplus \mathbf{0})) = \mathbf{1}.$$

Но это мы установили при проверке аксиомы 2: надо взять  $c = \mathbf{0}$ .

Аксиома 8 Надо доказать

$$(a \oplus c) \oplus ((b \oplus c) \oplus ((a \sqcup b) \oplus c)) = \mathbf{1},$$

или

$$a \oplus c \leq (b \oplus c) \oplus ((a \sqcup b) \oplus c),$$

или

$$-a \sqcup c \leq -(-b \sqcup c) \sqcup -(a \sqcup b) \sqcup c,$$

или (если применить закон Де Моргана)

$$-a \sqcup c \leq (b \sqcap -c) \sqcup (-a \sqcap -b) \sqcup c.$$

По лемме 5.1 это сводится к

$$(\#) \quad -a \leq (b \sqcap -c) \sqcup (-a \sqcap -b) \sqcup c.$$

Для доказательства  $(\#)$  используем неравенства:

$$(**) \quad -a \leq (-a \sqcap -b) \sqcup b,$$

$$(***) \quad b \leq (b \sqcap -c) \sqcup c.$$

Каждое из них — это вариант неравенства  $(*)$  (см. выше). Теперь по лемме 5.1 получаем  $(\#)$ :

$$-a \leq (-a \sqcap -b) \sqcup b \leq (-a \sqcap -b) \sqcup (b \sqcap -c) \sqcup c.$$

■

**Следствие 5.2.** *CL* непротиворечиво, т.е. нет такой формулы  $A$ , что  $\vdash_{CL} A, \neg A$ .

*Доказательство.* Иначе обе формулы  $A, \neg A$  окажутся тавтологиями. ■

### Полнота исчисления высказываний

**Теорема 5.3** (Теорема о полноте *CL*). *Все тавтологии выводимы в CL:*

$$\mathcal{2} \models A \Rightarrow \vdash_{CL} A.$$

**Доказательство** Множество формул  $\Gamma \subseteq Ft$  называется *противоречивым* (в *CL*), если  $\Gamma \vdash A, \neg A$  для некоторой формулы  $A$ .

**Лемма 5.4.**

$$(1) \quad \Gamma \cup \{B\} \text{ противоречиво} \Leftrightarrow \Gamma \vdash \neg B$$

$$(2) \quad \text{Если } \Gamma \text{ противоречиво, то } \Gamma \vdash B \text{ для всех формул } B.$$

**Доказательство** (леммы).

$$(1) \quad (\Leftarrow) \text{ очевидно.}$$

Докажем  $(\Rightarrow)$ . Пусть  $\Gamma, B \vdash A, \neg A$ . Тогда по теореме дедукции

$$\Gamma \vdash B \rightarrow A, B \rightarrow \neg A.$$

С другой стороны,

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

Это получается из аксиомы 9, если заменить в ней  $A$  на  $B$  и наоборот и 2 раза применить МР. Тогда по транзитивности

$$\Gamma \vdash \neg B.$$

(2) Если  $\Gamma$  противоречиво, то и по-прежнему  $\Gamma \cup \{\neg B\}$  противоречиво. По (1) тогда  $\Gamma \vdash \neg\neg B$ . Добавив к этому выводу аксиому 10  $\neg\neg B \rightarrow B$  и применив МР, получаем  $\Gamma \vdash B$ . ■

Теорему 5.3 докажем от противного: предполагаем  $\not\vdash_{CL} A$  и доказываем  $2 \not\equiv A$ .

Пусть  $\Phi$  — множество всех подформул  $A$  и их отрицаний. Будем рассматривать различные  $\Gamma \subseteq \Phi$ .

Множество  $\Gamma \subseteq \Phi$  назовем *максимально непротиворечивым* (или просто — *максимальным*), если оно непротиворечиво, а всякое его собственное расширение внутри  $\Phi$  (т.е.  $\Gamma'$ , такое что  $\Gamma \subset \Gamma' \subseteq \Phi$ ) противоречиво.

Очевидно, что  $\Phi$  противоречиво — например, потому, что  $A, \neg A \in \Phi$ .

Множество  $\{\neg A\}$  непротиворечиво: иначе бы  $\vdash \neg\neg A$  (по лемме 5.4(1)), и тогда  $\vdash A$  — по аксиоме 10 и МР.

**Лемма 5.5.** *Любое непротиворечивое подмножество  $\Phi$  содержится в каком-то максимальном.*

**Доказательство** Если  $\Gamma \subseteq \Phi$  непротиворечиво и не максимально, то оно останется непротиворечивым при добавлении какой-то формулы из  $\Phi \setminus \Gamma$ . Расширим его, добавив эту формулу. Продолжаем процесс до тех пор, пока это возможно. Т.к.  $\Phi \setminus \Gamma$  конечно, через конечное число шагов получится максимальное множество. <sup>11</sup> ■

**Лемма 5.6.** *Пусть  $\Gamma$  — максимальное множество. Тогда*

- (0)  $\Gamma \vdash B \Rightarrow B \in \Gamma$  (для  $B \in \Phi$ );
- (1)  $\neg B \in \Gamma \Leftrightarrow B \notin \Gamma$  (для  $\neg B \in \Phi$ );
- (2)  $(B \wedge C) \in \Gamma \Leftrightarrow (B \in \Gamma \text{ и } C \in \Gamma)$  (для  $(B \wedge C) \in \Phi$ );
- (3)  $(B \vee C) \in \Gamma \Leftrightarrow (B \in \Gamma \text{ или } C \in \Gamma)$  (для  $(B \vee C) \in \Phi$ );
- (4)  $(B \rightarrow C) \in \Gamma \Leftrightarrow (B \notin \Gamma \text{ или } C \in \Gamma)$  (для  $(B \rightarrow C) \in \Phi$ ).

**Доказательство** (0) Доказываем от противного. Предположим, что  $B \in \Phi$ ,  $B \notin \Gamma$ . Тогда  $\Gamma \subset \Gamma \cup \{B\} \subseteq \Phi$ , поэтому  $\Gamma \cup \{B\}$  противоречиво (т.к.  $\Gamma$  максимально). Тогда по лемме 5.4(1)  $\Gamma \vdash \neg B$ , и следовательно,  $\Gamma \not\vdash B$  — иначе бы  $\Gamma$  было противоречиво.

(1)  $(\Rightarrow)$  очевидно, т.к.  $\Gamma$  непротиворечиво.

$(\Leftarrow)$  Сначала заметим, что если  $\neg B \in \Phi$ , то и  $B \in \Phi$  как подформула  $A$ . Действительно, если  $\neg B$  — отрицание подформулы  $A$ , то  $B$  — подформула; если же  $\neg B$  — подформула  $A$ , то  $B$  — тоже подформула. Тогда из  $B \notin \Gamma$  следует  $\Gamma \vdash \neg B$  (как в доказательстве (0)). Отсюда  $\neg B \in \Gamma$  — по (0).

(2) Нам дано, что  $(B \wedge C) \in \Phi$ . Тогда  $(B \wedge C)$  — подформула  $\Phi$ , поэтому и  $B, C$  — подформулы и лежат в  $\Phi$ .

$(\Rightarrow)$  Пусть  $(B \wedge C) \in \Gamma$ . Тогда  $\Gamma \vdash B, C$  (по аксиомам 3,4 и МР). Значит,  $B, C \in \Gamma$  — по (0).

$(\Leftarrow)$  Пусть  $B, C \in \Gamma$ . Тогда  $\Gamma \vdash B \wedge C$  (т.к.  $B, C \vdash B \wedge C$  — см. пример 3 из лекции 4). Отсюда  $(B \wedge C) \in \Gamma$  — по (0).

(3) Как и в случае (2), сначала заметим, что  $B, C \in \Phi$ .

$(\Leftarrow)$  Если  $B \in \Gamma$ , то  $\Gamma \vdash B \vee C$  (по аксиоме 6 и МР), и тогда  $(B \vee C) \in \Gamma$  — по (0). Если  $C \in \Gamma$ , рассуждаем аналогично (с аксиомой 7).

$(\Rightarrow)$  Доказываем от противного. Допустим  $(B \vee C) \in \Gamma$ , но  $B, C \notin \Gamma$ . Тогда  $\neg B, \neg C \in \Gamma$  — по (1).

Вспомним теперь, что из противоречивого множества выводится любая формула (лемма 5.4(1)), в частности,  $\perp$  ( $= P_1 \wedge \neg P_1$  — см. лекцию 2). Поэтому  $\neg B, B \vdash \perp$ , откуда  $\neg B \vdash B \rightarrow \perp$  — по теореме дедукции. Аналогично  $\neg C \vdash C \rightarrow \perp$ . В результате имеем:

$$\Gamma \vdash B \vee C, B \rightarrow \perp, C \rightarrow \perp.$$

Однако

$$B \vee C, B \rightarrow \perp, C \rightarrow \perp \vdash \perp$$

<sup>11</sup>Это рассуждение (его можно провести точнее, в рамках формальной теории множеств) показывает, что всякое конечное частично упорядоченное множество имеет максимальный элемент. В нашем случае это множество всех непротиворечивых подмножеств  $\Phi$ , содержащих  $\Gamma$ , упорядоченное по включению.

— это получится, если применить аксиому 8 и МР (дважды). По транзитивности,  $\Gamma \vdash \perp$ , и тогда  $\Gamma$  противоречиво: из  $\perp$  выводятся  $P_1, \neg P_1$ .

(4) Как и в остальных случаях, заметим, что  $B, C \in \Phi$ .

( $\Rightarrow$ ) Если  $(B \rightarrow C), B \in \Gamma$ , то  $\Gamma \vdash C$  по МР, и тогда  $C \in \Gamma$  (по (0)).

( $\Leftarrow$ ) Разбираем 2 случая.

Если  $B \notin \Gamma$ , то  $\neg B \in \Gamma$  (1). Но  $\neg B, B \vdash C$  (лемма 5.4(1)), откуда по теореме дедукции  $\neg B \vdash B \rightarrow C$ . Значит,  $\Gamma \vdash B \rightarrow C$ , и  $(B \rightarrow C) \in \Gamma$  — по (0).

Если  $C \in \Gamma$ , то  $\Gamma \vdash B \rightarrow C$  по аксиоме 1 и МР, и опять  $(B \rightarrow C) \in \Gamma$  — по (0). ■

Закончим теперь доказательство теоремы. Исходное непротиворечивое множество  $\neg A$  расширим до максимального  $\Gamma$  (лемма 5.5). Возьмем оценку  $f : Var \rightarrow \{0, 1\}$  такую, что для всех переменных  $P_i$  из  $\Phi$

$$f(P_i) = 1 \Leftrightarrow P_i \in \Gamma.$$

На всех других переменных зададим  $f$  как угодно. Тогда справедливо следующее утверждение:

$$f(F) = 1 \Leftrightarrow F \in \Gamma$$

для всех  $F \in \Phi$ . Это утверждение доказывается индукцией по длине  $F$ .

- Если  $F \in Var$ , то утверждение верно по определению.
- Пусть  $F = \neg B$ , тогда  $B \in \Phi$ , и по предположению индукции,

$$f(B) = 1 \Leftrightarrow B \in \Gamma$$

Имеем:

$$f(F) = 1 \Leftrightarrow f(B) = 0 \Leftrightarrow B \notin \Gamma \Leftrightarrow F = \neg B \in \Gamma$$

по лемме 5.6.

- Пусть  $F = (B \wedge C)$ , тогда  $B, C \in \Phi$ , и по предположению индукции,

$$f(B) = 1 \Leftrightarrow B \in \Gamma, \quad f(C) = 1 \Leftrightarrow C \in \Gamma.$$

Тогда

$$f(F) = 1 \Leftrightarrow f(B) = f(C) = 1 \Leftrightarrow (B \in \Gamma \text{ и } C \in \Gamma) \Leftrightarrow F = (B \wedge C) \in \Gamma$$

по лемме 5.6.

- Связки  $\vee, \rightarrow$  рассматриваются аналогично.

Применив доказанное утверждение к  $F = \neg A$ , получаем  $f(\neg A) = 1$ , и следовательно,  $f(A) = 0$ . Итак,  $\mathcal{B} \not\models A$ . ■

**Теорема 5.7.** Для любой пропозициональной формулы  $A$  и нетривиальной булевой алгебры  $\mathcal{B}$  следующие утверждения эквивалентны.

(1)  $\vdash_{CL} A$ ,

(2)  $\mathcal{B} \models A$ ,

(3)  $\mathcal{B} \models A$ .

**Доказательство** (1)  $\Rightarrow$  (2) — это теорема корректности 4.5, (2)  $\Rightarrow$  (3) — теорема 4.1, а (3)  $\Rightarrow$  (1) — теорема полноты 5.3. ■

## Лекция 6

### ЛОГИКА ПРЕДИКАТОВ

## Языки первого порядка: синтаксис

Отличия языка 1-го порядка от языка логики высказываний:

- Вместо пропозициональных переменных используются атомарные формулы.
- Для индуктивного построения формул, кроме логических связок, применяются кванторы.

**Определение 18.** *Сигнатурой (первого порядка)* называется четверка вида  $\Omega = (Pred_\Omega, Const_\Omega, Fun_\Omega, \nu)$ , в которой

- $Pred_\Omega, Const_\Omega, Fun_\Omega$  — попарно не пересекающиеся множества,
- $Pred_\Omega \neq \emptyset$ ,
- $\nu : Pred_\Omega \cup Fun_\Omega \longrightarrow \mathbb{N}_+ = \{1, 2, \dots\}$ .

Множества  $Pred_\Omega, Const_\Omega, Fun_\Omega$  называются соответственно множеством *предикатных символов*, множеством (*предметных*) *констант* и множеством *функциональных символов* сигнатуры  $\Omega$ .  $\nu$  называется *функцией валентности*.

Предикатный или функциональный символ  $G$  называется  *$n$ -местным ( $n$ -арным)*, если  $\nu(G) = n$ . Чтобы это подчеркнуть, его обозначают  $G^n$ .

**Определение 19.** Алфавит языка первого порядка сигнатуры  $\Omega$  состоит из

- всех предикатных символов, констант и функциональных символов  $\Omega$ ;
- счетного множества свободных (предметных) переменных  $FVar = \{a_0, a_1, \dots\}$ ;
- счетного множества связанных (предметных) переменных  $BVar = \{v_0, v_1, \dots\}$ ;
- логических связок:  $\vee, \wedge, \rightarrow, \neg$ ;
- кванторов:  $\forall, \exists$ ;
- технических символов:  $(, )$  (скобки),  $“,”$  (запятая).

Предполагаем, что все эти множества попарно не пересекаются.

Как правило, для обозначения свободных переменных мы будем использовать  $a, b, c, \dots$  вместо символов  $a_i$ , а для связанных —  $x, y, z, \dots$  вместо  $v_i$ .

Язык первого порядка данной сигнатуры состоит из двух видов слов в этом алфавите: термов и формул.

**Определение 20.** *Термы сигнатуры  $\Omega$*  строятся индуктивно:

- все константы — термы,
- все свободные переменные — термы,
- если  $f^n \in Fun_\Omega$  и  $t_1, \dots, t_n$  — термы, то  $f(t_1, \dots, t_n)$  — терм.

Таким образом, мы индукцией по длине слова, определяем, какие слова считаются термами. Это определение можно сформулировать иначе:

Множество термов сигнатуры  $\Omega$  — это наименьшее множество слов  $X$ , такое что

- $Const_\Omega \subseteq X$ ,
- $FVar \subseteq X$ ,
- если  $f^n \in Fun_\Omega$  и  $t_1, \dots, t_n \in X$ , то  $f(t_1, \dots, t_n) \in X$ .

**Определение 21.** *Атомарные формулы сигнатуры  $\Omega$*  — это слова вида  $P(t_1, \dots, t_n)$ , где  $P^n \in Pred_\Omega$ , а  $t_1, \dots, t_n$  — термы сигнатуры  $\Omega$ .

**Определение 22.** *Формулы сигнатуры  $\Omega$*  строятся индуктивно:

- все атомарные формулы являются формулами;
- если  $A, B$  — формулы, то  $(A \wedge B)$  — формула;
- если  $A, B$  — формулы, то  $(A \vee B)$  — формула;

- если  $A, B$  — формулы, то  $(A \rightarrow B)$  — формула;
- если  $A$  — формула, то  $\neg A$  — формула;
- если  $A$  — формула,  $a \in FVar$ ,  $x \in BVar$  и  $x$  не входит в  $A$ , то  $\exists x[x/a]A$  — формула;
- если  $A$  — формула,  $a \in FVar$ ,  $x \in BVar$  и  $x$  не входит в  $A$ , то  $\forall x[x/a]A$  — формула.

В этом определении запись  $[x/a]A$  означает результат замены всех вхождений переменной  $a$  в  $A$  на переменную  $x$  (в частности,  $[x/a]A = A$ , если  $a$  не входит в  $A$ ).

Обозначения (для сигнатуры  $\Omega$ ):

$Tm_\Omega$  — множество всех термов,

$Fm_\Omega$  — множество всех формул,

$AFm_\Omega$  — множество всех атомарных формул.

Замечание В любой формуле кванторы по одной и той же переменной могут встречаться только в непересекающихся подформулах. Например, если  $P^1 \in Pred_\Omega$  и  $x \in BVar$ , то

$$\exists x P(x) \wedge \exists x \neg P(x)$$

— формула, а

$$\exists x(P(x) \wedge \exists x \neg P(x))$$

— не формула.

Существуют и другие варианты определения формулы. Самый распространенный вариант: свободные и связанные переменные не различаются, а кванторы применяются без ограничений. Такое определение формулы проще, но при этом варианте усложняется формулировка исчисления предикатов.

При более экзотическом варианте определения связанные переменные исчезают, а вместо них появляются пустые окошки, которые соединяются связями со своими кванторами. Похожее определение используется в “Теории множеств” Бурбаки.

Пример Рассмотрим сигнатуру колец (или сигнатуру арифметики). В ней имеются константы  $0, 1$ , предикатный символ  $=^2$ , и функциональные символы  $+^2, \cdot^2$ .

Атомарные формулы имеют вид  $=(t_1, t_2)$ , что мы будем записывать более привычным образом:  $(t_1 = t_2)$ . Аналогично, термы  $+(t_1, t_2), \cdot(t_1, t_2)$  записываются как  $(t_1 + t_2), (t_1 \cdot t_2)$ .

В этой сигнатуре можно написать формулу

$$\exists x((x + x) = a),$$

которая означает, что  $a$  — четное число (если речь идет о натуральных или целых числах).

Для коммутативных колец формула

$$\neg(a = 0) \wedge \exists x((x \cdot a) = 0) \wedge \neg(x = 0)$$

означает, что  $a$  — делитель нуля, а формула

$$\exists x((x \cdot a) = 1)$$

— что  $a$  обратим.

**Лемма 6.1** (Лемма об однозначном анализе термов и формул). *Для данной сигнатуры  $\Omega$*

- (1) *Каждый терм есть либо константа, либо свободная переменная, либо имеет вид  $f(t_1, \dots, t_n)$  для единственного функционального символа  $f^n$  и термов  $t_1, \dots, t_n$ .*
- (2) *Каждая атомарная формула имеет вид  $P(t_1, \dots, t_n)$  для единственного предикатного символа  $P^n$  и термов  $t_1, \dots, t_n$ .*
- (3) *Для любой формулы  $C$  выполнено ровно одно из условий:*
  - $C$  — атомарная,
  - Существует единственная пара формул  $A, B$ , такая что  $C = (A \wedge B)$ ,
  - Существует единственная пара формул  $A, B$ , такая что  $C = (A \vee B)$ ,

- Существует единственная пара формул  $A, B$ , такая что  $C = (A \rightarrow B)$ ,
- Существует единственная формула  $A$ , такая что  $C = \neg A$ ,
- $C = \exists x[x/a]A$  для некоторой формулы  $A$  и  $a \in FVar$ ,  $x \in BVar$ ,
- $C = \forall x[x/a]A$  для некоторой формулы  $A$  и  $a \in FVar$ ,  $x \in BVar$ .

Доказательство опускаем. Отметим, что в последних двух случаях формула  $A$  уже не единственна: например,

$$\exists xP(x) = \exists x[x/a]P(a) = \exists x[x/b]P(b).$$

## Языки первого порядка: семантика

**Определение 23.** Модель сигнатуры  $\Omega$ , или  $\Omega$ -структура, — это пара вида  $M = (\underline{M}, \mathcal{I})$ , где  $\underline{M}$  — непустое множество (носитель модели),

$\mathcal{I}$  — функция, определенная на множестве  $Pred_\Omega \cup Const_\Omega \cup Fun_\Omega$  (интерпретирующая функция), причем

- Если  $c \in Const_\Omega$ , то  $\mathcal{I}(c) \in \underline{M}$ ,
- Если  $P^n \in Pred_\Omega$ , то  $\mathcal{I}(P) : \underline{M}^n \rightarrow \{\text{и}, \text{л}\}$ <sup>12</sup> (т.е.  $\mathcal{I}(P)$  —  $n$ -местный предикат на  $\underline{M}$ ),
- Если  $f^n \in Fun_\Omega$ , то  $\mathcal{I}(f) : \underline{M}^n \rightarrow \underline{M}$  (т.е.  $\mathcal{I}(f)$  —  $n$ -местная операция на  $\underline{M}$ ).

В дальнейшем для заданной модели  $M = (\underline{M}, \mathcal{I})$  пишем  $c_M, P_M, F_M$  соответственно вместо  $\mathcal{I}(c), \mathcal{I}(P), \mathcal{I}(f)$  и  $m \in M$  вместо  $m \in \underline{M}$ .

**Определение 24.** Терм, не содержащий переменных (т.е. построенный из констант и функциональных символов), называется *замкнутым*. Для сигнатуры  $\Omega$  множество всех замкнутых термов обозначается  $CTm_\Omega$ ,

Для замкнутого терма  $t$  сигнатуры  $\Omega$  индукцией по длине определяется его значение в модели  $M$  сигнатуры  $\Omega$ ; оно обозначается  $|t|_M$ .

- $|c|_M := c_M$  для  $c \in Const_\Omega$ ,
- $|f(t_1, \dots, t_n)|_M := f_M(|t_1|_M, \dots, |t_n|_M)$  для  $f^n \in Fun_\Omega$ ,  $t_1, \dots, t_n \in CTm_\Omega$ .

**Определение 25.** Замкнутая атомарная формула имеет вид  $P^n(t_1, \dots, t_n)$ , где  $t_1, \dots, t_n$  — замкнутые термы.

Для замкнутой атомарной формулы сигнатуры  $\Omega$  ее значение в модели  $M$  той же сигнатуры определяется так:

$$|P(t_1, \dots, t_n)|_M := P_M(|t_1|_M, \dots, |t_n|_M).$$

**Определение 26.** Модель  $M$  сигнатуры, содержащей 2-местный предикатный символ равенства  $=$ , называется *нормальной*, если для всех  $m_1, m_2$  из  $M$

$$=_M(m_1, m_2) = \begin{cases} \text{и}, & \text{если } m_1, m_2 \text{ совпадают,} \\ \text{л}, & \text{иначе.} \end{cases}$$

**Пример** Модель сигнатуры колец — это произвольное непустое множество  $\underline{M}$  с выбранными как угодно элементами  $0_M, 1_M$ , предикатом  $=_M$  (как в определении 26) и операциями  $+_M, \cdot_M$ . Она не обязана быть кольцом.

Если  $M = \mathbb{N}$  с обычным пониманием символов  $0, 1, +, \cdot$ , то  $|(1 + 1) \cdot 1|_M$  равно 2 (но символа 2 в нашей сигнатуре нет, это — элемент модели).

Если же  $M = \mathbb{Z}_2$  (кольцо вычетов *mod 2*), то  $|(1 + 1) \cdot 1|_M$  равно  $0_M$ .

Замкнутая атомарная формула  $1 + 1 = 0$  принимает значение *и* в модели  $\mathbb{Z}_2$  и *л* в модели  $\mathbb{N}$ .

<sup>12</sup> Как и в логике высказываний, далее мы будем отождествлять значения истинности *и*, *л* с 0, 1. Пока мы этого не делаем — во избежание путаницы.

**Лемма 6.2.** Пусть  $M$  — модель сигнатуры  $\Omega$ . Значения замкнутых термов в  $M$  определены корректно. Это означает, что существует единственное отображение  $t \mapsto |t|_M$  из  $CTm_\Omega$  в  $\underline{M}$ , удовлетворяющее условиям из определения 24:

- $|c|_M = c_M$  для  $c \in Const_\Omega$ ,
- $|f(t_1, \dots, t_n)|_M = f_M(|t_1|_M, \dots, |t_n|_M)$  для  $f^n \in Fun_\Omega$ ,  $t_1, \dots, t_n \in CTm_\Omega$ .

**Доказательство** Аналогично лемме 2.1. Индукцией по длине  $t$  доказываем, что  $|t|_M$  определяется однозначно.

Базис индукции: если  $t$  — константа, то все очевидно.

Шаг индукции. По лемме 6.1,  $t = f(t_1, \dots, t_n)$  для единственного функционального символа  $f$  и термов  $t_1, \dots, t_n$ . По предположению индукции, значения  $|t_1|_M, \dots, |t_n|_M$  определены однозначно, и тогда  $|t|_M = f_M(|t_1|_M, \dots, |t_n|_M)$  тоже задается однозначно. ■

**Лемма 6.3.** Значения замкнутых атомарных формул в модели определены корректно.

**Доказательство** Очевидное следствие лемм 6.1 и 6.2. ■

**Определение 27.** Формула, не содержащая свободных переменных, называется *замкнутой*, или *предложением*.

Для сигнатуры  $\Omega$  множество всех замкнутых формул обозначается  $CFm_\Omega$ .

Значение произвольной замкнутой формулы в модели определяется по индукции; оно отражает интуитивное понимание связок и кванторов. Точное определение мы дадим в лекции 7, а пока отметим лишь, что для связок  $\vee, \wedge, \neg$  определение аналогично логике высказываний. Т.е.  $|A \wedge B| = \min(|A|, |B|)$ ,  $|\neg A| = 1 - |A|$  и т.д.

**Определение 28.** Пусть  $M$  — модель сигнатуры  $\Omega$ ,  $A$  — замкнутая формула сигнатуры  $\Omega$ . Говорят, что  $A$  *истинна* (или *выполнима*) в  $M$ , если  $|A|_M = 1$ . В этом случае также говорят, что  $M$  — *модель*  $A$  и пишут  $M \models A$ .

Замкнутая формула называется *выполнимой*, если она имеет модель; *общезначимой* — если она истинна во всех моделях данной сигнатуры.

**Определение 29.** Теорией первого порядка в сигнатуре  $\Omega$  называется любое множество замкнутых формул этой сигнатуры; элементы теории называются также ее *аксиомами*.

Говорят, что теория  $T$  *выполнима* в модели  $M$ , или что  $M$  — *модель*  $T$ , и пишут  $M \models T$ , если все формулы из  $T$  истинны в  $M$ .

Теория называется *выполнимой* (или *совместной*), если она имеет модель.

**Пример 1** Рассмотрим *сигнатуру равенства*. В ней единственный 2-местный предикатный символ “ $=$ ” (равенство) и нет ни констант, ни функциональных символов. *Чистая теория равенства* (которую мы обозначим  $Eq$ ) содержит 3 аксиомы:

$$\begin{aligned} \forall x(x = x), \\ \forall x \forall y(x = y \rightarrow y = x), \\ \forall x \forall y \forall z(x = y \wedge y = z \rightarrow x = z). \end{aligned}$$

Всякая модель  $M$  сигнатуры равенства — это непустое множество с произвольным 2-местным предикатом  $=_M$ . Если же  $M \models Eq$ , то предикат  $=_M$  должен быть рефлексивным, симметричным и транзитивным (такой предикат называется *эквивалентностью*).

В любой нормальной модели  $M$  истинны все аксиомы  $Eq$ ; в этом случае  $=_M$  — предикат равенства.

**Определение 30.** Пусть  $T$  — теория,  $A$  — замкнутая формула в ее сигнатуре. Говорят, что  $A$  *логически* (или *семантически*) *следует из*  $T$  (обозначение:  $T \models A$ ), если  $A$  истинна во всех моделях  $T$ .



Очевидны следующие свойства:

1. Если  $T$  не выполнима, то  $T \models A$  для всех  $A$ .
2.  $T \not\models A \Leftrightarrow T \cup \{\neg A\}$  выполнима.

**Определение 31.** Теория  $T$  называется *полной*, если для любой замкнутой формулы  $A$  в ее сигнатуре хотя бы одна из формул  $A$ ,  $\neg A$  логически следует из  $T$ .

Очевидно, что всякая невыполнимая теория полна: из нее следуют все формулы той же сигнатуры. Если же теория выполнима и полна, то либо  $T \models A$ , либо  $T \models \neg A$ , но не одновременно: в модели  $T$  не могут быть истинны и  $A$ , и  $\neg A$ .

**Определение 32.** *Элементарной теорией* модели  $M$  называется множество всех замкнутых формул в ее сигнатуре, истинных в  $M$ ; обозначение:  $Th(M)$ .

Пример 2 Любая теория  $Th(M)$  полна: если замкнутая формула  $A$  верна в  $M$ , то она принадлежит теории  $Th(M)$  и значит, следует из нее; если же  $A$  ложна в  $M$ , то  $\neg A \in Th(M)$ , поэтому  $Th(M) \models \neg A$ .

Пример 3 Чистая теория равенства  $Eq$  неполна. Чтобы в этом убедиться, рассмотрим формулу

$$A_{=1} := \forall x \forall y (x = y).$$

Заметим, что в нормальной модели  $M$

$$M \models A_{=1} \Leftrightarrow |M| = 1$$

(где  $|M|$  — мощность модели  $M$ , т.е. мощность ее носителя). Поэтому

- $Eq \not\models \neg A_{=1}$  — т.к. теория  $Eq \cup \{A_{=1}\}$  выполнима: у нее есть 1-элементная нормальная модель.
- $Eq \not\models A_{=1}$  — т.к. теория  $Eq \cup \{\neg A_{=1}\}$  выполнима: у нее есть (например) 10-элементная нормальная модель.

Пример 4 Теория  $T = Eq \cup \{A_{=1}\}$  полна. Аккуратно это утверждение мы докажем позже (см. лекцию 9), но интуитивно оно понятно: все нормальные модели этой теории одноэлементны и потому они не отличимы никакими формулами. А ненормальные модели можно не учитывать. Значит, не могут быть выполнимы обе теории  $T \cup \{A\}$ ,  $T \cup \{\neg A\}$ .

## Лекция 7

**Определение 33.** Теории  $T_1, T_2$  одной сигнатуры называются *эквивалентными (равносильными)*, если у них одни и те же модели; обозначение:  $T_1 \sim T_2$ .

Обозначим через  $[T]$  множество всех логических следствий теории  $T$ . Заметим, что

$$T_1 \sim T_2 \Leftrightarrow [T_1] = [T_2].$$

Действительно, если модели у теорий  $T_1, T_2$  одинаковые, то и формулы, которые верны в этих моделях — одни и те же, т.е.  $[T_1] = [T_2]$ . Наоборот, если следствия у теорий одинаковые, то любая формула из  $T_2$  является следствием  $T_1$ , т.е. верна во всех моделях  $T_1$ . Значит, всякая модель  $T_1$  оказывается моделью  $T_2$ . Аналогично, всякая модель  $T_2$  является моделью  $T_1$ .

**Определение 34.** Модели  $M_1, M_2$  одной сигнатуры называются *элементарно эквивалентными*, если в них истинны одни и те же замкнутые формулы, т.е.  $Th(M_1) = Th(M_2)$ ; обозначение:  $M_1 \equiv M_2$ .

**Лемма 7.1.** Пусть  $T$  — выполнимая теория. Следующие условия эквивалентны:

- (1)  $T$  полна.
- (2) Любое выполнимое расширение теории  $T$  эквивалентно  $T$ .
- (3)  $[T] = Th(M)$  для некоторой модели  $M$ .

(4) Все модели  $T$  элементарно эквивалентны.

**Доказательство** (1)  $\Rightarrow$  (2). Пусть  $T$  полна, докажем (2). Пусть  $T' \supseteq T$ ; тогда очевидно, что  $[T'] \supseteq [T]$ . Предположим, что  $T' \not\approx T$ . Тогда найдется формула  $A \in ([T'] \setminus [T])$ . Поскольку  $T \not\models A$  и  $T$  полна, получаем  $T \models \neg A$ . Но тогда и  $T' \models \neg A$ . С другой стороны,  $T' \models A$ . Значит,  $T'$  невыполнима.

(2)  $\Rightarrow$  (3). Предположим (2). Если  $M \models T$ , то  $T \subseteq Th(M)$ . Теория  $Th(M)$  выполнима, поэтому она эквивалентна  $T$  (в силу (2)). Тогда  $[T] = [Th(M)]$ . Но  $[Th(M)] = Th(M)$ , т.к. все логические следствия  $Th(M)$  истинны в  $M$ .

(3)  $\Rightarrow$  (4). Предположим (3). Тогда из  $M' \models T$  следует  $M' \models Th(M)$ . Значит, всякая замкнутая формула, истинная в  $M$ , будет истинной в  $M'$ . И наоборот, если  $M \not\models A$ , т.е.  $M \models \neg A$ , то  $M' \models \neg A$ , т.е.  $M' \not\models A$ . Итак,  $M \equiv M'$ .

(4)  $\Rightarrow$  (1). Предположим (4) и допустим, что  $T$  неполна. Тогда для некоторой замкнутой формулы  $A$ ,  $T \not\models A$  и  $T \not\models \neg A$ . Это означает, что обе теории  $T \cup \{\neg A\}$ ,  $T \cup \{A\}$  выполнимы. Их модели оказываются моделями  $T$ , которые не элементарно эквивалентны.  $\blacksquare$

### Определение истинности в модели

Пусть  $M$  — модель сигнатуры  $\Omega$ ; предполагаем, что ее носитель  $\underline{M}$  состоит из совершенно новых элементов, которые не являются словами, содержащими символы из  $\Omega$ . Через  $\Omega \cup M$  обозначим *расширенную сигнатуру модели  $M$* , которая получается из  $\Omega$  добавлением множества новых констант  $\underline{M}$ ; т.е.  $Const_{\Omega \cup M} = Const_{\Omega} \cup \underline{M}$ , в остальном же  $\Omega \cup M$  не отличается от  $\Omega$ .<sup>13</sup>

**Определение 35.** Пусть  $M$  — модель сигнатуры  $\Omega$ . *Терм, оцененный в  $M$*  — это замкнутый терм расширенной сигнатуры  $M$ ; аналогично, *формула, оцененная в  $M$*  — это замкнутая формула сигнатуры  $\Omega \cup M$ .

Согласно нашим обозначениям,  $CTm_{\Omega \cup M}$  — множество всех термов, оцененных в  $M$ ; а  $CFm_{\Omega \cup M}$  — множество всех формул, оцененных в  $M$ .

**Определение 36.** Для терма  $t$ , оцененного в модели  $M$ , индукцией по длине определяется его *значение*  $|t|_M$ :

- $|c|_M := c_M$  для  $c \in Const_{\Omega}$ ,
- $|m|_M := m$  для  $m \in \underline{M}$ ,
- $|f(t_1, \dots, t_n)|_M := f_M(|t_1|_M, \dots, |t_n|_M)$  для  $f^n \in Fun_{\Omega}$ ,  $t_1, \dots, t_n \in CTm_{\Omega \cup M}$ .

Корректность этого определения проверяется, как в лемме 6.2.

**Определение 37.** Для формулы  $C$ , оцененной в модели  $M$ , ее “логической длиной” назовем число вхождений в нее логических связок и кванторов. Индукцией по логической длине формулы  $C$  определяется ее *значение*  $|C|_M$ :

- $|P(t_1, \dots, t_n)|_M := P_M(|t_1|_M, \dots, |t_n|_M)$  для  $P^n \in Pred_{\Omega}$ ,  $t_1, \dots, t_n \in CTm_{\Omega \cup M}$ .
- $|A \wedge B|_M := \min(|A|_M, |B|_M)$ ,
- $|A \vee B|_M := \max(|A|_M, |B|_M)$ ,
- $|A \rightarrow B|_M := \max(1 - |A|_M, |B|_M)$ ,
- $|\neg A|_M := 1 - |A|_M$ ,
- $|\exists x[x/a]A|_M := 1 \Leftrightarrow$  существует  $m \in \underline{M}$ , такой что  $|[m/a]A|_M = 1$ ,
- $|\forall x[x/a]A|_M := 1 \Leftrightarrow$  для всех  $m \in \underline{M}$ ,  $|[m/a]A|_M = 1$ ,

<sup>13</sup>Техническое требование, чтобы все элементы из  $\underline{M}$  были новыми, нужно для корректности дальнейших определений. Чтобы его обойти, для всех элементов можно ввести “новые имена”, т.е. добавить к  $Const_{\Omega}$  не  $\underline{M}$ , а другое множество, которое находится с ним в биективном соответствии и состоит из новых элементов. Мы не будем этим заниматься.

Здесь  $[m/a]A$  обозначает оцененную формулу, полученную из  $A$  заменой всех вхождений  $a$  на  $m$ .<sup>14</sup> Заметим, что последние 2 пункта определения можно записать и так:

$$\begin{aligned} |\exists x[x/a]A|_M &= \max_{m \in \underline{M}} |[m/a]A|_M, \\ |\forall x[x/a]A|_M &= \min_{m \in \underline{M}} |[m/a]A|_M. \end{aligned}$$

Докажем корректность этих определений.

**Лемма 7.2.**

- (1) Для любой модели  $M$  существует единственное отображение  $t \mapsto |t|_M$  оцененных в  $M$  термов в  $\underline{M}$ , удовлетворяющее условиям из определения 36.
- (2) Для любой модели  $M$  существует единственное отображение  $A \mapsto |A|_M$  оцененных в  $M$  формул в  $\{0, 1\}$ , удовлетворяющее условиям из определения 37.

**Доказательство** (1) Рассуждаем, как в лемме 6.2. Лемма 6.1 об однозначном анализе сохраняется для оцененных термов с небольшим отличием: они бывают 3 видов. При этом важно, что элементы  $M$  не являются константами  $\Omega$  и не представляются в виде  $f(t_1, \dots, t_n)$ . Но это уже было оговорено.

(2) Аналогично лемме 2.1. Применим лемму 6.1 об однозначном анализе формул (для оцененных формул она не меняется).

1. Если  $A = P(t_1, \dots, t_n)$  — атомарная, то  $|A|_M$  однозначно определено — по лемме 6.3.
2. Если  $A = (B \wedge C)$ , то надо положить  $|A|_M = \min(|B|_M, |C|_M)$ . Формулы  $B, C$  единственны по лемме 6.1, а  $|B|_M, |C|_M$  определены однозначно по предположению индукции ( $B, C$  — меньшей длины, чем  $A$ ). Поэтому  $|A|_M$  задается однозначно.
- 3, 4, 5. Аналогично рассуждаем в случаях  $A = \neg B, (B \vee C), (B \rightarrow C)$ .
6. Пусть  $A = \exists x[x/a]B$ . Тогда надо определить  $|A|_M = \max_{m \in \underline{M}} |[m/a]B|_M$ .  $B$  и  $[m/a]B$  — меньшей длины, чем  $A$ , поэтому  $|A|_M$  задается однозначно при данном выборе  $B$ .

Однако теперь уже  $B$  не единственна. Рассмотрим другую формулу  $B'$ , такую что  $A = \exists x[x/a']B'$  для некоторой свободной переменной  $a'$ , причем  $x$  не входит в  $B'$ . Тогда  $[x/a']B' = [x/a]B$ , поэтому  $B'$  получается из  $B$  при замене  $a$  на  $a'$  (или: заменой сначала всех  $a$  на  $x$ , а потом — всех  $x$  на  $a'$ ). Т.е.  $B' = [a'/a]B$ .

Отсюда получаем, что при всех  $m \in M$

$$[m/a']B' = [m/a'] [a'/a]B = [m/a]B.$$

Поэтому если мы определили

$$|A|_M = \max_{m \in \underline{M}} |[m/a]B|_M,$$

то также получаем и

$$|A|_M = \max_{m \in \underline{M}} |[m/a']B'|_M.$$

Таким образом,  $|A|_M$  в этом случае определено однозначно — независимо от того, используем мы  $B$  или  $B'$  для построения  $A$ .

7. Случай  $A = \forall x[x/a]B$  рассматривается аналогично. ■

**Пример** Рассмотрим *сигнатуру колец*, содержащую равенство ( $=$ ), константы 0, 1 и функциональные символы:  $\cdot, +$  (2-местные).

В термах записываем их привычным образом:  $t_1 \cdot t_2, t_1 + t_2$ .

Рассмотрим формулу  $\exists x(x \cdot x = 1 + 1)$  в моделях  $\mathbb{R}$  и  $\mathbb{Q}$  (с обычным пониманием нуля, единицы, сложения и умножения). Имеем:

$$\mathbb{R} \models \exists x(x \cdot x = 1 + 1),$$

<sup>14</sup>Строго говоря, надо доказывать, что это — действительно формула; доказательство рутинное, по индукции. Мы определяем значения только для замкнутых формул. Заметим, что если формула  $\forall x[x/a]A$  (или  $\exists x[x/a]A$ ) замкнута, то  $A$  не может содержать никаких свободных переменных, кроме  $a$ . И тогда  $[m/a]A$  снова оказывается замкнутой. Т.е. определение осмысленно.

т.к.

$$\mathbb{R} \models \sqrt{2} \cdot \sqrt{2} = 1 + 1.$$

Отметим, что здесь возникает оцененная формула  $\sqrt{2} \cdot \sqrt{2} = 1 + 1$ , с константами двух видов: 1 берется из исходной сигнатуры, а  $\sqrt{2}$  — из модели; в сигнатуре колец такого символа нет.

С другой стороны,

$$\mathbb{Q} \models \neg \exists x (x \cdot x = 1 + 1),$$

т.к.

$$\mathbb{Q} \not\models r \cdot r = 1 + 1$$

для всех  $r \in \mathbb{Q}$ .

## Изоморфизмы моделей

Определим теперь точно, какие модели будут считаться “одинаковыми”.

**Определение 38.** Пусть  $M, M'$  — модели сигнатуры  $\Omega$ . Отображение  $\alpha : \underline{M} \rightarrow \underline{M}'$  называется *изоморфизмом  $M$  на  $M'$* , если

- $\alpha$  — биекция,
- $\alpha(c_M) = c_{M'}$  для всех  $c \in \text{Const}_\Omega$ ,
- $\alpha(f_M(m_1, \dots, m_k)) = f_{M'}(\alpha(m_1), \dots, \alpha(m_k))$  для всех  $f^k \in \text{Fun}_\Omega$  и  $m_1, \dots, m_k \in \underline{M}$ ,
- $P_M(m_1, \dots, m_k) = P_{M'}(\alpha(m_1), \dots, \alpha(m_k))$  для всех  $P^k \in \text{Pred}_\Omega$  и  $m_1, \dots, m_k \in \underline{M}$ .

Если говорить не совсем строго, изоморфизм сохраняет значения всех констант, предикатов и функций из нашей сигнатуры.

Запись  $\alpha : M \cong M'$  означает, что  $\alpha$  — изоморфизм  $M$  на  $M'$ .

### Лемма 7.3.

- (1) Если  $\alpha : M \cong M'$  и  $\beta : M' \cong M''$ , то  $\beta\alpha : M \cong M''$  ( $\beta\alpha$  обозначает композицию).
- (2) Если  $\alpha : M \cong M'$ , то  $\alpha^{-1} : M' \cong M$ .

Доказательство — непосредственной проверкой (упражнение).

**Определение 39.** Модели  $M, M'$  называются *изоморфными* (обозначение:  $M \cong M'$ ), если существует изоморфизм  $\alpha : M \cong M'$ .

Очевидно, что  $M \cong M$ , а из леммы 7.3 получаем, что изоморфность моделей также обладает свойствами симметричности и транзитивности, т.е.  $\cong$  задает отношение эквивалентности на классе всех моделей данной сигнатуры.

Посмотрим, как изменяются значения термов и формул при изоморфизме.

Пусть  $M, M'$  — модели сигнатуры  $\Omega$ ,  $\alpha : M \cong M'$ . Для терма  $t$ , оцененного в  $M$ , обозначим через  $\alpha \cdot t$  терм, полученный заменой всех констант  $m$  из  $M$  на их образы  $\alpha(m)$ . Формально  $\alpha \cdot t$  надо определять по индукции и доказывать, что  $\alpha \cdot t$  — терм, оцененный в  $M'$ . (Это — простое упражнение.)

Аналогично по формуле  $A$ , оцененной в  $M$ , строится формула  $\alpha \cdot A$ , оцененная в  $M'$ .

**Теорема 7.4.** Пусть  $M, M'$  — модели сигнатуры  $\Omega$ ,  $\alpha : M \cong M'$ .

- (1) Если  $t \in \text{CTm}_{\Omega \cup M}$ , то  $|\alpha \cdot t|_{M'} = \alpha(|t|_M)$ .
- (2) Если  $A \in \text{CFm}_{\Omega \cup M}$ , то  $|\alpha \cdot A|_{M'} = |A|_M$ .

**Доказательство** (1) Рассуждаем индукцией по длине  $t$ . Возможны 3 случая.

(1.1) (базис индукции).  $t = c$ , для  $c \in Const_\Omega$ .

Тогда  $\alpha \cdot t = t = c$ . Имеем:

$$|\alpha \cdot t|_{M'} = c_{M'} = \alpha(c_M) = \alpha(|t|_M)$$

по определению значения терма (опр. 36) и определению изоморфизма (опр. 38).

(1.2) (базис индукции).  $t = m$ , для  $m \in \underline{M}$ . Тогда  $\alpha \cdot t = \alpha(m)$ , и утверждение очевидно:

$$|\alpha \cdot t|_{M'} = \alpha(m) = \alpha(|t|_M)$$

по определению значения терма (опр. 36).

(1.3) (шаг индукции).  $t = f(t_1, \dots, t_n)$  для функционального символа  $f^n$  и термов  $t_1, \dots, t_n$ . Тогда

$$\alpha \cdot t = f(\alpha \cdot t_1, \dots, \alpha \cdot t_n).$$

Получаем:

$$(*) \quad |\alpha \cdot t|_{M'} = f_{M'}(|\alpha \cdot t_1|_{M'}, \dots, |\alpha \cdot t_n|_{M'}) = f_{M'}(\alpha(|t_1|_M), \dots, \alpha(|t_n|_M))$$

по опр. 36 и предположению индукции для термов  $t_i$ . Далее,

$$(**) \quad f_{M'}(\alpha(|t_1|_M), \dots, \alpha(|t_n|_M)) = \alpha(f_M(|t_1|_M, \dots, |t_n|_M)) = \alpha(|t|_M)$$

по определению изоморфизма (опр. 38) и опр. 36. Утверждение (1) следует из (\*) и (\*\*). ■

Утверждение (2) докажем на следующей лекции.

## Лекция 8

**Доказательство** (окончание)

(2) Применяем индукцию по числу вхождений логических связок и кванторов в  $A$ .

(2.1) (базис индукции)  $A = P(t_1, \dots, t_n)$  — атомарная ( $P^n$  — предикатный символ,  $t_1, \dots, t_n$  — термы).

Доказательство — почти такое же, как в случае (1.3).

$$|A|_M = P_M(|t_1|_M, \dots, |t_n|_M)$$

(опр. 36 лекции 7). С другой стороны,

$$\begin{aligned} |\alpha \cdot A|_{M'} &= P_{M'}(|\alpha \cdot t_1|_{M'}, \dots, |\alpha \cdot t_n|_{M'}) = P_{M'}(\alpha(|t_1|_M), \dots, \alpha(|t_n|_M)). \\ &= P_M(|t_1|_M, \dots, |t_n|_M). \end{aligned}$$

по (1) и определению изоморфизма. Отсюда получаем:

$$|\alpha \cdot A|_{M'} = |A|_M.$$

$$(2.2) \quad A = (B \wedge C).$$

$$(2.3) \quad A = (B \vee C),$$

$$(2.4) \quad A = (B \rightarrow C),$$

$$(2.5) \quad A = \neg B.$$

Эти простые случаи оставляются читателю в качестве упражнения.

$$(2.6) \quad A = \exists x[x/a]B.$$

По определению истинности

$$(*) \quad |\alpha \cdot A|_{M'} = |\exists x[x/a](\alpha \cdot B)|_{M'} = \max_{m' \in M'} |[m'/a](\alpha \cdot B)|_{M'} = \max_{m \in M} |[\alpha(m)/a](\alpha \cdot B)|_{M'}$$

Последнее равенство следует из сюръективности  $\alpha$ : все  $m' \in M'$  — это в точности  $\alpha$ -образы всех  $m \in M$ .

Также по определению истинности и предположению индукции для  $[m/a]B$

$$(**) \quad |A|_M = \max_{m \in M} |[m/a]B|_M = \max_{m \in M} |\alpha \cdot [m/a]B|_M$$

Но

$$(***) \quad \alpha \cdot [m/a]B = [\alpha(m)/a](\alpha \cdot B).$$

Действительно, левая часть получается из  $B$  сначала заменой  $a$  на  $m$ , а потом — всех элементов из  $M$  на их образы. В итоге  $a$  заменится на  $\alpha(m)$ . В правой части: сначала в  $B$  все элементы из  $M$  заменяются на их образы, а потом  $a$  сразу заменяется на  $\alpha(m)$ .

Собирая вместе (\*), (\*\*), (\*\*\*) , получаем

$$|\alpha \cdot A|_{M'} = |A|_M.$$

$$(2.7) \quad A = \forall x[x/a]B.$$

Этот случай совершенно аналогичен (2.6);  $\max$  заменяется на  $\min$ . ■

**Теорема 8.1.** Если  $M \cong M'$ , то  $M \equiv M'$ .

**Доказательство** Пусть  $\alpha : M \cong M'$ . Если  $A$  — замкнутая формула данной сигнатуры, то  $\alpha \cdot A = A$ , т.к.  $A$  не содержит констант из  $M$ . По теореме 7.4(2)

$$|A|_M = |A|_{M'},$$

или

$$M \models A \Leftrightarrow M' \models A.$$

Это выполняется для любой замкнутой  $A$ , а потому  $Th(M) = Th(M')$ , т.е.  $M \equiv M'$ . ■

## Определимость и автоморфизмы

**Определение 40.**  $k$ -местный предикат на множестве  $M$  — это отображение  $\gamma : M^k \rightarrow \{0, 1\}$ .  $k$ -местное отношение на множестве  $M$  — это множество  $R \subseteq M^k$ .

Любому  $k$ -местному отношению  $R \subseteq M^k$  соответствует  $k$ -местный предикат — его характеристическая функция  $\gamma : M^k \rightarrow \{0, 1\}$ :

$$\gamma(m_1, \dots, m_k) = \begin{cases} 1, & \text{если } (m_1, \dots, m_k) \in R, \\ 0 & \text{иначе.} \end{cases}$$

И наоборот, предикату  $\gamma : M^k \rightarrow \{0, 1\}$  соответствует отношение

$$R = \{(m_1, \dots, m_k) \mid \gamma(m_1, \dots, m_k) = 1\}.$$

В частности, при  $k = 1$ : подмножествам  $M$  соответствуют одноместные предикаты на  $M$ .

**Определение 41.** *Параметрами* формулы  $A$  (некоторой сигнатуры) называются входящие в нее свободные переменные.  $FV(A)$  обозначает множество всех параметров формулы  $A$ .

Формулу  $A$  мы записываем в виде  $A(b_1, \dots, b_k)$ , если хотим отметить, что  $FV(A) \subseteq \{b_1, \dots, b_k\}$ . При этом некоторые  $b_i$  могут и не встречаться в  $A$ . Подразумевается, что все  $b_i$  различны.

Аналогичную терминологию и обозначения применяем для термов; разница лишь в том, что в термах могут встречаться только свободные переменные. Т.е. параметры терма  $t$  — это все входящие в него переменные; их множество обозначается  $FV(t)$ . Запись  $t(b_1, \dots, b_k)$  означает, что  $FV(t) \subseteq \{b_1, \dots, b_k\}$ .

**Определение 42.** Рассмотрим формулу  $A(\vec{b})$ , где  $\vec{b} = (b_1, \dots, b_k)$ .

$k$ -местный предикат, определяемый формулой  $A(\vec{b})$  в модели  $M$  — это  $A_M : M^k \rightarrow \{0, 1\}$ , такой что для всех  $m_1, \dots, m_k$

$$A_M(m_1, \dots, m_k) = |[m_1, \dots, m_k/b_1, \dots, b_k]A|_M.$$

Здесь использовано обозначение многократной подстановки:  
 $[m_1, \dots, m_k / b_1, \dots, b_k]A$  получается из  $A$  заменой  $b_1, \dots, b_k$  соответственно на  $m_1, \dots, m_k$ . В сокращенных обозначениях определение записывается так:

$$A_M(\vec{m}) = |A(\vec{m})|_M.$$

для всех  $\vec{m} \in M^k$ .<sup>15</sup>

Примеры Рассмотрим опять сигнатуру колец и ее модель  $\mathbb{N}$  — множество натуральных чисел с обычными сложением, умножением, нулем и единицей. Рассмотрим в этой модели 2-местный предикат  $m_1 \leq m_2$ . Он определим формулой  $\exists x(b_1 + x = b_2)$ :

$$\mathbb{N} \models \exists x(m_1 + x = m_2) \Leftrightarrow m_1 \leq m_2.$$

В этой формуле используется только сложение, поэтому определимость сохранится и для более бедной сигнатуры, в которой есть только  $+$  и  $=$ .

Для того, чтобы задать порядок на множестве действительных чисел  $\mathbb{R}$ , сложения уже не хватит, т.е. в  $\mathbb{R}$  как модели сигнатуры  $\{+, =\}$  предикат  $m_1 \leq m_2$  не определим — это мы установим чуть позже. Но легко доказать определимость в сигнатуре колец:

$$\mathbb{R} \models \exists x(m_1 + x \cdot x = m_2) \Leftrightarrow m_1 \leq m_2.$$

Докажем необходимое условие определимости предиката в модели.

Как и в алгебре, *автоморфизм* модели — это ее изоморфизм на себя.

**Теорема 8.2.** Пусть  $\alpha$  — автоморфизм модели  $M$  сигнатуры  $\Omega$ ,  $A(b_1, \dots, b_k)$  — формула той же сигнатуры. Тогда для всех  $m_1, \dots, m_k \in M$

$$A_M(\alpha(m_1), \dots, \alpha(m_k)) = A_M(m_1, \dots, m_k).$$

В сокращенной записи:

$$A_M(\alpha\vec{m}) = A_M(\vec{m}).$$

Таким образом, определимый в  $M$  предикат инвариантен при всех автоморфизмах  $M$ .

**Доказательство** По определению 42 и теореме 7.4

$$A_M(\alpha\vec{m}) = |A(\alpha\vec{m})|_M = |A(\vec{m})|_M = A_M(\vec{m}).$$

■

Поскольку предикаты соответствуют отношениям, мы можем говорить и об определимости отношений:  $k$ -местное отношение  $R$  определимо в  $M$  формулой  $A(\vec{b})$ , если определим соответствующий предикат, т.е. для всех  $\vec{m} \in M^k$

$$M \models A(\vec{m}) \Leftrightarrow \vec{m} \in R.$$

В частности (при  $k = 1$ ): подмножество  $S \subseteq M$  определимо формулой  $A(a)$ , если для всех  $m \in M$

$$M \models A(m) \Leftrightarrow m \in S.$$

Теорема 8.2 означает, что определимые отношения инвариантны при автоморфизмах:

$$\vec{m} \in R \Leftrightarrow \alpha\vec{m} \in R.$$

Пример 1 Рассмотрим множество действительных чисел  $\mathbb{R}$  как модель сигнатуры  $\{=^2, +^2, 0\}$ , с обычным пониманием этих символов.

У этой модели есть автоморфизм  $\alpha(x) = -x$ : это отображение — биекция (обратно само к себе), сохраняет 0 и сумму.

<sup>15</sup>Для краткости мы пишем  $M^k$  вместо  $\underline{M}^k$ .

Предикат  $m_1 \leq m_2$  не определим в этой модели, т.к. он не инвариантен при этом автоморфизме: неверно, что  $m_1 \leq m_2 \Leftrightarrow -m_1 \leq -m_2$ .

**Пример 2** Рассмотрим  $\mathbb{Z}$  в той же сигнатуре, что в примере 1. Тогда подмножество  $\mathbb{N}$  не определимо: оно не инвариантно при автоморфизме  $\alpha(x) = -x$ .

Однако, если добавить в сигнатуру умножение,  $\mathbb{N}$  станет определимым. Для этого можно применить теорему Лагранжа о представимости всякого натурального числа в виде суммы 4 квадратов:

$$\mathbb{Z} \models \exists x_1 \exists x_2 \exists x_3 \exists x_4 (x_1^2 + x_2^2 + x_3^2 + x_4^2 = m) \Leftrightarrow m \in \mathbb{N},$$

где  $x^2$  обозначает  $x \cdot x$ .

Конечно же, и в этой сигнатуре не все подмножества определимы: определимых подмножеств (как и всех формул в данной сигнатуре) — счетное число, а всех подмножеств — континуум.

**Определение 43.** Подмножества  $\mathbb{N}$ , определимые в сигнатуре колец (она же — сигнатура арифметики), называются *арифметическими*.

Как и в случае  $\mathbb{Z}$ , таких множество таких подмножеств счетно. Однако теорема 8.1 никак не помогает построить конкретные неарифметические множества: легко видеть, что единственный автоморфизм модели  $\mathbb{N}$  — тождественный (Упражнение).

## Стандартные теории равенства и нормальные модели

Пусть  $A = A(b_1, \dots, b_n)$  — формула. Если же  $x_1, \dots, x_n$  — какие-то (различные) связанные переменные, не входящие в  $A$ , то результат подстановки  $[x_1, \dots, x_n/b_1, \dots, b_n]A$  будем обозначать через  $A(x_1, \dots, x_n)$ . (Заметим, что выражение  $A(x_1, \dots, x_n)$  — не формула, но может быть частью формулы: например, последовательное навешивание кванторов  $\forall x_n, \dots, \forall x_1$  дает формулу  $\forall x_1 \dots \forall x_n A(x_1, \dots, x_n)$ .)

**Лемма 8.3.** Пусть  $A(b_1, \dots, b_n)$  — формула сигнатуры  $\Omega$ ,  $x_1, \dots, x_n$  — (различные) связанные переменные, не входящие в  $A$ . Тогда для любой модели  $M$  сигнатуры  $\Omega$

$$M \models \forall x_1 \dots \forall x_n A(x_1, \dots, x_n) \Leftrightarrow \text{для всех } m_1, \dots, m_n \in M \quad M \models A(m_1, \dots, m_n),$$

$$M \models \exists x_1 \dots \exists x_n A(x_1, \dots, x_n) \Leftrightarrow \text{для некоторых } m_1, \dots, m_n \in M \quad M \models A(m_1, \dots, m_n).$$

**Доказательство** Мы рассмотрим только случай кванторов  $\forall$ ; для  $\exists$  доказательство аналогично.

Утверждение следует из определения истинности (формально — индукцией по  $n$ ). А именно,  $A = \forall x_1 [x_1/b_1]B(b_1)$ , где

$$B(b_1) := \forall x_2 \dots \forall x_n A(b_1, x_2, \dots, x_n).$$

И тогда

$$(1) \quad M \models A \Leftrightarrow \text{для всех } m_1 \in M \quad M \models B(m_1).$$

Но

$$B(m_1) = \forall x_2 \dots \forall x_n A(m_1, x_2, \dots, x_n);$$

это формула в сигнатуре  $\Omega \cup M$ . Применим к ней предположение индукции:

$$(2) \quad M \models \forall x_2 \dots \forall x_n A(m_1, x_2, \dots, x_n) \Leftrightarrow$$

$$\text{для всех } m_2, \dots, m_n \in M \quad M \models A(m_1, m_2, \dots, m_n).$$

Из (1) и (2) получаем утверждение леммы. Это — шаг индукции, а базис (при  $n = 1$ ) очевиден. ■

Теперь рассмотрим сигнатуру  $\Omega$ , содержащую предикатный символ равенства ( $=$ ) (и, возможно, другие символы). В этой сигнатуре рассмотрим теорию  $Eq_\Omega$  со следующими *стандартными аксиомами равенства*.

(O) Аксиомы теории  $Eq$  (лекция 7, пример 1) — рефлексивность, симметричность и транзитивность.



$$(I) \forall x_1 \dots \forall x_n \forall y_1 \dots \forall y_n \left( \bigwedge_{i=1}^n x_i = y_i \rightarrow (P^n(x_1, \dots, x_n) \leftrightarrow P^n(y_1, \dots, y_n)) \right)$$

для всех  $P^n \in \text{Pred}_\Omega$ .

$$(II) \forall x_1 \dots \forall x_n \forall y_1 \dots \forall y_n \left( \bigwedge_{i=1}^n x_i = y_i \rightarrow f^n(x_1, \dots, x_n) = f^n(y_1, \dots, y_n) \right)$$

для всех  $f^n \in \text{Fun}_\Omega$ .

Запишем эти аксиомы в сокращенном виде:

$$(I) \forall \vec{x} \forall \vec{y} (\vec{x} = \vec{y} \rightarrow (P^n(\vec{x}) \leftrightarrow P^n(\vec{y}))).$$

$$(II) \forall \vec{x} \forall \vec{y} (\vec{x} = \vec{y} \rightarrow f^n(\vec{x}) = f^n(\vec{y})).$$

Здесь  $\vec{\forall}$  обозначает кванторы  $\forall$  по всем переменным  $x_1, y_1, \dots, x_n, y_n$ , а  $\vec{x} = \vec{y}$  — сокращение для  $x_1 = y_1 \wedge \dots \wedge x_n = y_n$ .

**Лемма 8.4.** Если  $M$  — нормальная модель сигнатуры с равенством  $\Omega$ , то  $M \models Eq_\Omega$ .

**Доказательство** Для аксиом (0) это тривиально (и уже отмечалось).

По лемме 8.3, формула (I) верна в  $M$ , если и только если для всех  $\vec{m}, \vec{m}' \in M^n$

$$M \models \vec{m} = \vec{m}' \rightarrow (P(\vec{m}) \leftrightarrow P(\vec{m}'))$$

(где  $\vec{m} = \vec{m}'$  — сокращение для  $m_1 = m'_1 \wedge \dots \wedge m_n = m'_n$ ).

Но последнее утверждение очевидно: в нормальной модели

$M \models \vec{m} = \vec{m}'$  означает, что  $\vec{m}$  и  $\vec{m}'$  совпадают; тогда и  $|P(\vec{m})|_M = |P(\vec{m}')|_M$ , а потому  $|P(\vec{m}) \leftrightarrow P(\vec{m}')|_M = 1$ .

Следовательно, верна импликация

$$\vec{m} = \vec{m}' \rightarrow (P(\vec{m}) \leftrightarrow P(\vec{m}')).$$

Аналогично рассуждаем для формулы (II):

$$M \models \vec{m} = \vec{m}' \rightarrow f(\vec{m}) = f(\vec{m}'),$$

т.к. из совпадения  $\vec{m}$  и  $\vec{m}'$  следует совпадение  $f_M(\vec{m})$  и  $f_M(\vec{m}')$ . ■

Покажем теперь, как из произвольной модели теории  $Eq_\Omega$  построить элементарно эквивалентную нормальную модель.

Пусть  $M \models Eq_\Omega$ . Тогда предикат  $=_M$  задает отношение эквивалентности на  $\underline{M}$ , которое мы обозначим  $\approx$ . Т.е.

$$m_1 \approx m_2 \Leftrightarrow =_M(m_1, m_2) = 1 \Leftrightarrow M \models m_1 = m_2.$$

Это действительно отношение эквивалентности, благодаря аксиомам  $Eq$ . Класс эквивалентности элемента  $m$  по  $\approx$  обозначим через  $\widetilde{m}$ .

На фактормножестве  $\underline{M}/\approx$  зададим нормальную модель  $\widetilde{M}$  сигнатуры  $\Omega$  следующим образом:

$$\begin{aligned} c_{\widetilde{M}} &:= \widetilde{c}_M, \\ f_M^k(\widetilde{m}_1, \dots, \widetilde{m}_k) &:= f_M^k(\widetilde{m}_1, \dots, \widetilde{m}_k), \\ P_M^k(\widetilde{m}_1, \dots, \widetilde{m}_k) &:= P_M^k(m_1, \dots, m_k) \end{aligned}$$

(где соответственно,  $c \in \text{Const}_\Omega$ ,  $f^k \in \text{Fun}_\Omega$ ,  $P^k \in \text{Pred}_\Omega$ ).

**Лемма 8.5.**  $\widetilde{M}$  корректно определена.

**Доказательство** Надо проверить, что если заменить  $m_i$  на эквивалентные элементы, то правые части в определении  $f_M^k$  и  $P_M^k$  не изменятся.

Действительно, пусть  $m_1 \approx m'_1, \dots, m_k \approx m'_k$ . Это означает, что  $M \models m_i = m'_i$  для  $i \leq k$ , и тогда, в обозначениях из леммы 8.4,  $M \models \vec{m} = \vec{m}'$ , где  $\vec{m} = (m_1, \dots, m_k)$ ,  $\vec{m}' = (m'_1, \dots, m'_k)$ . Как уже мы видели в лемме 8.4, из аксиомы (I) тогда следует, что  $M \models f(\vec{m}) = f(\vec{m}')$ , т.е.  $\widetilde{f_M(\vec{m})} = \widetilde{f_M(\vec{m}')}$ .

Аналогично, из аксиомы (II) получаем:  $M \models P(\vec{m}) \leftrightarrow P(\vec{m}')$ , т.е.  $P_M(\vec{m}) = P_M(\vec{m}')$ . ■

## Лекция 9

На прошлой лекции по модели  $M$  стандартной теории равенства  $Eq_\Omega$  мы построили модель  $\widetilde{M}$  с носителем  $\underline{M}/\approx$ . Тогда имеется сюръекция

$$\alpha : \underline{M} \longrightarrow \underline{M}/\approx,$$

переводящая каждый элемент  $t \in M$  в его класс эквивалентности  $\widetilde{t}$ . Благодаря определению  $\widetilde{M}$ ,  $\alpha$  — сильный гомоморфизм, т.е.

- $\alpha(f_M(\vec{m})) = f_{\widetilde{M}}(\alpha\vec{m})$  (для  $\vec{m} \in M^k$ ,  $f^k \in Fun_\Omega$ ),
- $P_M(\vec{m}) = P_{\widetilde{M}}(\alpha\vec{m})$  (для  $\vec{m} \in M^k$ ,  $P^k \in Pred_\Omega$ ), кроме случая, когда  $P$  есть  $=$ .

Для символа  $=$  также имеем<sup>16</sup>

$$=_{\underline{M}}(m_1, m_2) = =_{\widetilde{M}}(\alpha(m_1), \alpha(m_2)).$$

**Теорема 9.1** (Лемма о нормализации).

(1) Для любого оцененного терма  $t \in Tm_{\Omega \cup M}$

$$|\alpha \cdot t|_{\widetilde{M}} = |\widetilde{t}|_M.$$

(2) Для любой оцененной формулы  $A \in Fm_{\Omega \cup M}$

$$|\alpha \cdot A|_{\widetilde{M}} = |A|_M.$$

(3)  $M \equiv \widetilde{M}$ .

**Доказательство** См. теорему 7.4. В доказательстве используется только то, что  $\alpha$  — сюръекция.<sup>17</sup> ■

Итак, для теорий, содержащих стандартные аксиомы равенства, можно рассматривать только нормальные модели.

**Теорема 9.2.** Пусть  $T$  — теория в сигнатуре с равенством  $\Omega$ , содержащая  $Eq_\Omega$ . Предположим, что все нормальные модели  $T$  изоморфны (такая теория называется сильно категоричной). Тогда  $T$  полна.

**Доказательство** По лемме 7.1 достаточно доказать, что все модели  $T$  элементарно эквивалентны.

Рассмотрим модели  $M, M' \models T$ . По лемме 8.5,  $M \equiv \widetilde{M}$ ,  $M' \equiv \widetilde{M}'$ . Поэтому  $\widetilde{M}, \widetilde{M}' \models T$ . Т.к. эти модели нормальны, по условию они изоморфны. Следовательно,  $\widetilde{M} \equiv \widetilde{M}'$  (теорема 8.1). В итоге имеем  $M \equiv M'$ . ■

<sup>16</sup>Здесь знак  $=$  употребляется в двух смыслах.

<sup>17</sup>Можно заметить, что для нормальных моделей сигнатуры с равенством сюръективный гомоморфизм всегда биективен: условие  $M \models m_1 = m_2 \Leftrightarrow M' \models \alpha(m_1) = \alpha(m_2)$  как раз и означает, что  $\alpha$  — биекция. Но сейчас у нас другой случай.

Пример 1 В сигнатуре  $\{=\}$  рассмотрим теорию  $Eq \cup \{A_{=n}\}$ , где

$$A_{=n} := \exists x_1 \dots \exists x_n \left( \bigwedge_{i \neq j} (x_i \neq x_j) \wedge \forall x_{n+1} \bigvee_{i \leq n} (x_{n+1} = x_i) \right).$$

(Здесь мы используем обычное сокращение:  $(x_i \neq x_j) := \neg(x_i = x_j)$ .)

Эта аксиома утверждает, что в (нормальной) модели ровно  $n$  элементов. Очевидно, что данная теория сильно категорична.

Пример 2 Теперь рассмотрим теорию линейных порядков  $LO$  в сигнатуре с 2-местными предикатными символами  $<, =$ . Кроме стандартных аксиом равенства, она содержит аксиомы:

$\forall x \neg(x < x)$  (иррефлексивность)

$\forall x \forall y \forall z (x < y \wedge y < z \rightarrow x < z)$  (транзитивность)

$\forall x \forall y (x < y \vee y < x \vee x = y)$  (линейность)

Каждая теория  $LO + A_{=n}$  сильно категорична, потому что конечные линейные порядки с одинаковым числом элементов изоморфны.

Пример 3 Рассмотрим сигнатуру групп, содержащую равенство ( $=$ ), константу  $e$  (“единица”), функциональные символы:  $\cdot$  (2-местный, “умножение”),  $^{-1}$  (1-местный, “обращение”).

Используем привычную запись:  $t_1 \cdot t_2, t^{-1}$ .

Рассмотрим в этой сигнатуре теорию групп  $Gr$  со следующими аксиомами.

I. Стандартные аксиомы равенства.

II. Аксиомы групп.

$$\forall x \forall y \forall z ((x \cdot y) \cdot z = x \cdot (y \cdot z)).$$

$$\forall x ((x \cdot e = x) \wedge (e \cdot x = x)).$$

$$\forall x ((x \cdot x^{-1} = e) \wedge (x^{-1} \cdot x = e)).$$

Ясно, что модели теории групп — в точности группы (с единицей и операциями умножения и обращения). У этой теории имеются полные расширения:

1. Теории  $Gr + A_{=p}$ , где  $p$  — простое (лекция 7), сильно категоричны (т.к. группа простого порядка — циклическая), а потому полны.

2. Если к  $Gr$  добавить аксиому коммутативности умножения, получится теория абелевых групп  $AGr$ . Теория  $Gr + A_{=6}$  неполна (почему?), но  $AGr + A_{=6}$  полна, т.к. сильно категорична: ее модели изоморфны  $\mathbb{Z}_6$ .

В дальнейшем мы рассматриваем только теории с равенством и нормальные модели; отдельные исключения будут оговариваться.

## Теория конечной модели

**Определение 44.** Теория  $T$  называется *конечно аксиоматизируемой*, если она эквивалентна некоторой конечной теории.

Очевидно, что конечная теория  $T$  эквивалентна теории, состоящей из одной формулы  $\bigwedge T$ .

**Теорема 9.3.** В конечной сигнатуре с равенством элементарная теория конечной модели конечно аксиоматизируема и сильно категорична.

**Доказательство** Пусть  $M$  — конечная модель конечной сигнатуры  $\Omega$ .

Мы построим формулу  $A_M$ , которая полностью описывает  $M$ .

Пусть  $\underline{M} = \{m_1, \dots, m_n\}$ . Положим

$$A_M := \exists v_1 \dots \exists v_n \psi_M(v_1, \dots, v_n),$$

где

$$\psi_M(a_1, \dots, a_n) := \bigwedge_{1 \leq i < j \leq n} (a_i \neq a_j) \wedge \forall v_{n+1} \bigvee_{i=1}^n (v_{n+1} = a_i) \wedge$$

$$\begin{aligned}
& \bigwedge \{c = a_i \mid c \in Const_\Omega, c_M \text{ равно } m_i\} \wedge \\
& \bigwedge \{f^k(a_{i_1}, \dots, a_{i_k}) = a_j \mid f^k \in Pred_\Omega, f_M^k(m_{i_1}, \dots, m_{i_k}) \text{ равно } m_j\} \wedge \\
& \bigwedge \{P^k(a_{i_1}, \dots, a_{i_k}) \mid P^k \in Pred_\Omega, M \models P^k(m_{i_1}, \dots, m_{i_k})\} \wedge \\
& \bigwedge \{\neg P^k(a_{i_1}, \dots, a_{i_k}) \mid P^k \in Pred_\Omega, M \not\models P^k(m_{i_1}, \dots, m_{i_k})\}.
\end{aligned}$$

**Лемма 9.4.** Для нормальной модели  $M'$  сигнатуры  $\Omega$

$$M' \models A_M \Leftrightarrow M' \cong M.$$

**Доказательство**

( $\Leftarrow$ ) Заметим, что

$$M \models \psi_M(m_1, \dots, m_n).$$

Действительно,

$$\begin{aligned}
\psi_M(m_1, \dots, m_n) &= \bigwedge_{1 \leq i < j \leq n} (m_i \neq m_j) \wedge \forall v_{n+1} \bigvee_{i=1}^n (v_{n+1} = m_i) \wedge \\
& \bigwedge \{c = m_i \mid c \in Const_\Omega, c_M \text{ равно } m_i\} \wedge \\
& \bigwedge \{f^k(m_{i_1}, \dots, m_{i_k}) = m_j \mid f^k \in Pred_\Omega, f_M^k(m_{i_1}, \dots, m_{i_k}) \text{ равно } m_j\} \wedge \\
& \bigwedge \{P^k(m_{i_1}, \dots, m_{i_k}) \mid P^k \in Pred_\Omega, M \models P^k(m_{i_1}, \dots, m_{i_k})\} \wedge \\
& \bigwedge \{\neg P^k(m_{i_1}, \dots, m_{i_k}) \mid P^k \in Pred_\Omega, M \not\models P^k(m_{i_1}, \dots, m_{i_k})\}.
\end{aligned}$$

Проверим, что все 6 членов этой конъюнкции (все они — тоже конъюнкции, кроме второго) истинны в  $M$ .

- (1)  $M \models \bigwedge_{1 \leq i < j \leq n} (m_i \neq m_j)$ , т.к.  $M$  нормальна и все  $m_i$  различны,
- (2)  $M \models \forall v_{n+1} \bigvee_{i=1}^n (v_{n+1} = m_i)$ , т.к. всякий элемент из  $M$  равен одному из  $m_i$ .
- (3)  $M \models \bigwedge \{c = m_i \mid c \in Const_\Omega, c_M \text{ равно } m_i\}$ , т.к. для всякой константы  $c$ ,  $M \models c = m_i$ , если  $c_M$  равно  $m_i$  — это очевидно, по определению истинности (см. определения 36, 37 лекции 7).
- (4) Аналогично, для четвертого члена:  $M \models f(m_{i_1}, \dots, m_{i_k}) = m_j$ , если  $f_M(m_{i_1}, \dots, m_{i_k})$  равно  $m_j$ .
- (5) Истинность пятого члена означает, что  $M \models P^k(m_{i_1}, \dots, m_{i_k})$ , если  $M \models P^k(m_{i_1}, \dots, m_{i_k})$ . Это тривиальность.
- (6) Также очевидно.

Теперь по лемме 8.3, из  $M \models \psi_M(m_1, \dots, m_n)$  получаем  $M \models A_M$ . И тогда, если  $M \cong M'$ , то и  $M' \models A_M$  — по теореме 8.1.

( $\Rightarrow$ ) Предположим, что  $M' \models A_M$  и построим изоморфизм  $M$  на  $M'$ . Снова по лемме 8.3, найдутся  $m'_1, \dots, m'_n \in M'$ , для которых

$$M' \models \psi_M(m'_1, \dots, m'_n).$$

Для удобства опять распишем  $\psi_M(m'_1, \dots, m'_n)$ :

$$\begin{aligned}
& \bigwedge_{1 \leq i < j \leq n} (m'_i \neq m'_j) \wedge \forall v_{n+1} \bigvee_{i=1}^n (v_{n+1} = m'_i) \wedge \\
& \bigwedge \{c = m'_i \mid c \in Const_\Omega, c_M \text{ равно } m_i\} \wedge
\end{aligned}$$

$$\bigwedge \{f^k(m'_{i_1}, \dots, m'_{i_k}) = m'_j \mid f^k \in \text{Pred}_\Omega, f^k_M(m_{i_1}, \dots, m_{i_k}) \text{ равно } m_j\} \wedge \\ \bigwedge \{P^k(m'_{i_1}, \dots, m'_{i_k}) \mid P^k \in \text{Pred}_\Omega, M \models P^k(m_{i_1}, \dots, m_{i_k})\} \wedge \\ \bigwedge \{\neg P^k(m'_{i_1}, \dots, m'_{i_k}) \mid P^k \in \text{Pred}_\Omega, M \not\models P^k(m_{i_1}, \dots, m_{i_k})\}.$$

Докажем, что отображение  $\varphi$ , переводящее каждый  $m_i$  в  $m'_i$  — искомый изоморфизм.

1.  $\varphi$  — инъекция. Это обеспечивает 1-й член конъюнкции: при  $i < j$   $M \models m'_i \neq m'_j$ , т.е.  $m'_i$  и  $m'_j$  не совпадают.

2.  $\varphi$  — сюръекция. Об этом говорит 2-й член конъюнкции: любой элемент  $m' \in M'$  равен одному из  $m'_i$ , т.к.  $M \models \bigvee_{i=1}^n (m' = m'_i)$  и  $M$  нормальна.

3.  $\varphi(c_M)$  равно  $c_{M'}$ . Это получается из 3-го члена: если  $c_M$  равно  $m_i$ , то  $M' \models c = m'_i$ , т.е.  $c_{M'}$  равно  $m'_i$  (которое и есть  $\varphi(c_M)$ ).

4.  $\varphi(f^k_M(m_{i_1}, \dots, m_{i_k}))$  равно  $f^k_{M'}(\varphi(m_{i_1}), \dots, \varphi(m_{i_k}))$ , т.е.  $f^k_{M'}(m'_{i_1}, \dots, m'_{i_k})$ .

В самом деле, если  $f^k_M(m_{i_1}, \dots, m_{i_k})$  равно  $m_j$ , то из 4-го члена,  $M' \models m'_j = f^k(m'_{i_1}, \dots, m'_{i_k})$ , т.е.  $\varphi(m_j)$  равно  $f^k_{M'}(m'_{i_1}, \dots, m'_{i_k})$ .

5.  $M' \models P^k(m'_{i_1}, \dots, m'_{i_k}) \Leftrightarrow M \models P^k(m_{i_1}, \dots, m_{i_k})$ .

Действительно, если  $M \models P^k(m_{i_1}, \dots, m_{i_k})$ , то из 5-го члена,  $M' \models P^k(m'_{i_1}, \dots, m'_{i_k})$ .

Если же  $M \not\models P^k(m_{i_1}, \dots, m_{i_k})$ , то из 6-го члена,  $M' \not\models P^k(m'_{i_1}, \dots, m'_{i_k})$ . ■

Продолжим доказательство теоремы 9.3.

Заметим, что  $\text{Th}(M) \sim \{A_M\}$ .<sup>18</sup> Действительно, по лемме 9.4  $A_M \in \text{Th}(M)$  и значит,

$$M' \models \text{Th}(M) \Rightarrow M' \models A_M.$$

Обратно, пусть  $M' \models A_M$ . По той же лемме,  $M' \cong M$ . И тогда  $M' \models \text{Th}(M)$ .

Итак,  $\text{Th}(M)$  конечно аксиоматизируема.

Также  $\text{Th}(M)$  сильно категорична, т.к. эквивалентная ей теория  $\{A_M\}$  сильно категорична по лемме 9.4. ■

**Следствие 9.5.** Если  $M$  — конечная модель и  $M' \equiv M$ , то  $M' \cong M$ .

**Доказательство** Если  $M' \equiv M$ , то  $M' \models \text{Th}(M)$ . Тогда, по теореме 9.3,  $M' \cong M$ . ■

## Общезначимость и равносильность

**Определение 45.** Замкнутые формулы  $A, B$  (в некоторой сигнатуре) называются *равносильными*, если формула  $A \leftrightarrow B$  общезначима (см. определение 11 лекции 6).

Как и в логике высказываний, равносильность обозначается знаком  $\sim$ . И мы имеем аналог леммы 2.3:

**Лемма 9.6.**  $A \sim B$  тогда и только тогда, когда для любой модели  $M$  (данной сигнатуры)  $|A|_M = |B|_M$ .

**Лемма 9.7.** Пусть  $A(\vec{b})$  — формула сигнатуры  $\Omega$ ;  $\vec{x}, \vec{y}$  — списки (той же длины, что  $\vec{b}$ ) различных связанных переменных, не входящих в  $A$ .

$$(1) \forall \vec{x} A(\vec{x}) \sim \forall \vec{y} A(\vec{y}).$$

(2) Если формула  $A$  замкнута,  $x$  — связанная переменная, не входящая в  $A$ , то  $A \sim \forall x A$ .

Здесь  $\forall \vec{x}$  обозначает последовательность кванторов  $\forall$  по переменным из списка  $\vec{x}$ ; аналогично — для  $\vec{y}$ .

<sup>18</sup>Эквивалентность здесь понимается относительно нормальных моделей. Если рассматривать произвольные модели, то надо добавить еще  $Eq_\Omega$ .

**Доказательство** (1) следует из леммы 8.3: получается, что

$$M \models \forall \vec{x} A(\vec{x}) \Leftrightarrow \text{для всех } \vec{m} \text{ из } M, M \models A(\vec{m}).$$

и

$$M \models \forall \vec{y} A(\vec{y}) \Leftrightarrow \text{для всех } \vec{m} \text{ из } M, M \models A(\vec{m}).$$

Поэтому

$$M \models \forall \vec{x} A(\vec{x}) \Leftrightarrow M \models \forall \vec{y} A(\vec{y}).$$

Значит, эти формулы равносильны (лемма 9.4).

(2) — очевидное следствие определения истинности. Действительно, в этом случае  $M \models \forall x A$  (где  $\forall x A$  получается как  $\forall x[x/a]A$  с переменной  $a$ , не входящей в  $A$ ) равносильно  $M \models A$ , т.к. при замене фиктивного  $a$  на любое  $t$  с формулой  $A$  ничего не произойдет. ■

**Определение 46.** Пусть  $b_1, \dots, b_n$  — список параметров формулы  $A$  в алфавитном порядке<sup>19</sup>, и пусть  $x_1, \dots, x_n$  — список первых связанных переменных, не входящих в  $A$ , также в алфавитном порядке. Тогда *универсальным замыканием* формулы  $A$  называется формула  $\forall x_1 \dots \forall x_n[x_1, \dots, x_n/b_1, \dots, b_n]A$ .

Так определенное универсальное замыкание задается однозначно по  $A$ . Но на самом деле нас интересует эта формула с точностью до равносильности. Леммы 8.3, 9.7 показывают, что мы можем расположить  $b_1, \dots, b_n$  в любом порядке, и переменные  $x_1, \dots, x_n$  тоже можно выбрать как угодно — лишь бы они не входили в  $A$  — все построенные формулы окажутся равносильными. Поэтому универсальным замыканием называют любую из них.

Универсальное замыкание  $A$  (какое-нибудь) будем обозначать  $\bar{\forall}A$ .

Теперь можно определить общезначимость и равносильность для произвольных формул.

**Определение 47.** Формула  $A$  называется *общезначимой*, если общезначимо ее универсальное замыкание.

Формулы  $A, B$  называются *равносильными*, если общезначима формула  $\bar{\forall}(A \leftrightarrow B)$ .

Для произвольных формул общезначимость по-прежнему обозначается знаком  $\models$ , а равносильность — знаком  $\sim$ .

Таким образом, по лемме 8.3

$$\models A(\vec{a}) \Leftrightarrow \text{для любой модели } M \text{ и } \vec{m} \text{ из } M, M \models A(\vec{m}),^{20}$$

$$A(\vec{a}) \sim B(\vec{a}) \Leftrightarrow \text{для любой модели } M \text{ и } \vec{m} \text{ из } M, |A(\vec{m})|_M = |B(\vec{m})|_M.$$

**Лемма 9.8.**

(1)  $\sim$  задает отношение эквивалентности на  $Fm_\Omega$ .

(2)  $A \sim \forall \vec{x}[\vec{x}/\vec{b}]A$ , если  $\vec{b}$  — список различных свободных переменных, не входящих в  $A$ ;  $\vec{x}$  — список различных связанных переменных, не входящих в  $A$ ,

**Доказательство** (1) Можно использовать замечание перед формулировкой леммы. Ясно, что если  $|A(\vec{m})|_M = |B(\vec{m})|_M$  и  $|B(\vec{m})|_M = |C(\vec{m})|_M$ , то  $|A(\vec{m})|_M = |C(\vec{m})|_M$ .

(2) Применяем несколько раз лемму 9.7 и транзитивность  $\sim$ . ■

Пусть теперь  $F(P_1, \dots, P_n)$  — пропозициональная формула, построенная из пропозициональных переменных  $P_1, \dots, P_n$ , а  $B_1, \dots, B_n$  — формулы сигнатуры  $\Omega$ . Пусть  $S$  — подстановка, заменяющая каждое вхождение  $P_i$  на  $B_i$ . При этой замене из  $F$  получится формула сигнатуры  $\Omega$ , которую мы обозначим  $SF$ , или  $F(B_1, \dots, B_n)$ . Такая формула называется *подстановочным примером* формулы  $F$ .

Сформулируем две леммы, которые докажем на следующей лекции.

<sup>19</sup>Этот порядок задается нумерацией множества  $FVar$ , см. лекцию 6.

<sup>20</sup>Подразумевается, что  $M$  — в нужной сигнатуре, а  $\vec{m}$  — список ее элементов нужной длины.

**Лемма 9.9** (Лемма о тавтологиях). *Подстановочные примеры тавтологий общезначимы.*

**Лемма 9.10.**

- (1) Если  $F_1 \sim F_2$ , то  $SF_1 \sim SF_2$  (для любых пропозициональных формул  $F_1, F_2$  и подстановки  $S$ ).
- (2)  $\neg\forall x[x/a]A \sim \exists x[x/a]\neg A$ .
- (3)  $\neg\exists x[x/a]A \sim \forall x[x/a]\neg A$ .
- (4)  $\mathcal{Y}x[x/a](A \circ B) \sim (\mathcal{Y}x[x/a]A \circ B)$ , если  $a$  не входит в  $B$  (и  $x$  не входит ни в  $A$ , ни в  $B$ ).  
Здесь  $\mathcal{Y}$  обозначает квантор  $\forall$  или  $\exists$ ,  $a \circ$  — связку  $\vee$  или  $\wedge$ .
- (5) Если  $A \sim B$ , то  $\neg A \sim \neg B$ .
- (6) Если  $A \sim A'$  и  $B \sim B'$  то  $(A \circ B) \sim (A' \circ B')$  (где  $\circ$  — это  $\vee$ ,  $\wedge$  или  $\rightarrow$ ).
- (7) Если  $A \sim B$ , то  $\mathcal{Y}x[x/a]A \sim \mathcal{Y}x[x/a]B$  (при условии, что  $x$  не входит ни в  $A$ , ни в  $B$ ).
- (8)  $\mathcal{Y}x[x/a]A \sim \mathcal{Y}y[y/a]A \sim \mathcal{Y}y[y/b][b/a]A$ , если  $x, y, b$  не входят в  $A$  (здесь  $x, y \in BVar$ ,  $a, b \in FVar$ )

## Лекция 10

**Лемма 9.9** (Лемма о тавтологиях). *Подстановочные примеры тавтологий общезначимы.*

**Доказательство** Рассмотрим подстановку  $S$ , заменяющую  $P_1, \dots, P_n$  на  $B_1, \dots, B_n$ . Формулы  $B_i$  запишем как  $B_i(a_1, \dots, a_k)$ , считая, что список свободных переменных  $a_1, \dots, a_k$  содержит все параметры этих формул.

Рассмотрим произвольную модель  $M$  данной сигнатуры и ее элементы  $m_1, \dots, m_k$ . Обозначим  $B'_i := B_i(m_1, \dots, m_k)$  (это — оцененные в  $M$  формулы), и построим оценку пропозициональных переменных  $\theta : Var \rightarrow \{0, 1\}$  так:

$$\theta(P_i) := |B'_i|_M.$$

Утверждение Для любой пропозициональной формулы  $F(P_1, \dots, P_n)$

$$\theta(F) = |SF(m_1, \dots, m_k)|_M.$$

Это легко проверяется по индукции (по длине  $F$ ). Действительно, если  $F = P_i$ , то это следует из определения  $\theta$ , т.к.  $SP_i = B_i$ . А шаг индукции очевиден: например, при  $F = F_1 \wedge F_2$  имеем:  $SF = SF_1 \wedge SF_2$ ,

$$\theta(F) = \min(\theta(F_1), \theta(F_2)),$$

$$|SF(m_1, \dots, m_k)|_M = \min(|SF_1(m_1, \dots, m_k)|_M, |SF_2(m_1, \dots, m_k)|_M),$$

и можно применить предположение индукции.

Из доказанного утверждения сразу следует, что если  $F$  — тавтология, то  $M \models SF(m_1, \dots, m_k)$  для любой  $M$  и при любом выборе  $m_1, \dots, m_k$ . Это дает общезначимость  $SF$ . ■

**Лемма 9.10.**

- (1) Если  $F_1 \sim F_2$ , то  $SF_1 \sim SF_2$  (для любых пропозициональных формул  $F_1, F_2$  и подстановки  $S$ ).
- (2)  $\neg\forall x[x/a]A \sim \exists x[x/a]\neg A$ .
- (3)  $\neg\exists x[x/a]A \sim \forall x[x/a]\neg A$ .
- (4)  $\mathcal{Y}x[x/a](A \circ B) \sim (\mathcal{Y}x[x/a]A \circ B)$ , если  $a$  не входит в  $B$  (и  $x$  не входит ни в  $A$ , ни в  $B$ ).  
Здесь  $\mathcal{Y}$  обозначает квантор  $\forall$  или  $\exists$ ,  $a \circ$  — связку  $\vee$  или  $\wedge$ .
- (5) Если  $A \sim B$ , то  $\neg A \sim \neg B$ .
- (6) Если  $A \sim A'$  и  $B \sim B'$  то  $(A \circ B) \sim (A' \circ B')$  (где  $\circ$  — это  $\vee$ ,  $\wedge$  или  $\rightarrow$ ).
- (7) Если  $A \sim B$ , то  $\mathcal{Y}x[x/a]A \sim \mathcal{Y}x[x/a]B$  (при условии, что  $x$  не входит ни в  $A$ , ни в  $B$ ).
- (8)  $\mathcal{Y}x[x/a]A \sim \mathcal{Y}y[y/a]A \sim \mathcal{Y}y[y/b][b/a]A$ , если  $x, y, b$  не входят в  $A$  (здесь  $x, y \in BVar$ ,  $a, b \in FVar$ )

**Доказательство** (1) Если  $(F_1 \leftrightarrow F_2)$  — тавтология, то по лемме 9.9

$\models S(F_1 \leftrightarrow F_2)$ . Но  $S(F_1 \leftrightarrow F_2) = (SF_1 \leftrightarrow SF_2)$ . Тогда по определению равносильности  $SF_1 \sim SF_2$ .

(2) Запишем  $A$  как  $A(a, \vec{b})$ ; надо проверить, что в любой модели  $M$  для всех  $\vec{m}$

$$|\neg \forall x A(x, \vec{m})|_M = |\exists x \neg A(x, \vec{m})|_M.$$

Но это сразу следует из определения истинности:

$$|\neg \forall x A(x, \vec{m})|_M = 1 \Leftrightarrow |\forall x A(x, \vec{m})|_M = 0 \Leftrightarrow$$

$$\text{не для всех } k \in M |A(k, \vec{m})|_M = 1 \Leftrightarrow$$

$$\text{найдется } k \in M, \text{ для которого } |A(k, \vec{m})|_M = 0 \Leftrightarrow$$

$$\text{найдется } k \in M, \text{ для которого } |\neg A(k, \vec{m})|_M = 1 \Leftrightarrow |\exists x \neg A(x, \vec{m})|_M = 1.$$

(3) Доказывается аналогично (2) (упражнение).

(4) Проверим это для  $\mathcal{Y} = \exists$  и  $\circ = \wedge$ ; остальные случаи разбираются аналогично.

Запишем  $A$  как  $A(a, \vec{b})$ , а  $B$  — как  $B(\vec{b})$  (поскольку  $a$  не входит в  $B$ ). Надо доказать, что в любой модели  $M$  для любого  $\vec{m}$

$$(*) \quad |\exists x (A(x, \vec{m}) \wedge B(\vec{m}))|_M = 1 \Leftrightarrow |\exists x A(x, \vec{m}) \wedge B(\vec{m})|_M = 1.$$

В самом деле,

$$|\exists x (A(x, \vec{m}) \wedge B(\vec{m}))|_M = 1 \Leftrightarrow \text{найдется } k, \text{ такое что } |A(k, \vec{m}) \wedge B(\vec{m})|_M = 1 \Leftrightarrow$$

$$\text{найдется } k, \text{ такое что } (|A(k, \vec{m})|_M = 1 \text{ и } |B(\vec{m})|_M = 1).$$

Но условие  $|B(\vec{m})|_M = 1$  не зависит от  $k$ . Поэтому

$$\text{найдется } k, \text{ такое что } (|A(k, \vec{m})|_M = 1 \text{ и } |B(\vec{m})|_M = 1) \Leftrightarrow$$

$$(\text{найдется } k, \text{ такое что } |A(k, \vec{m})|_M = 1) \text{ и } |B(\vec{m})|_M = 1 \Leftrightarrow$$

$$|\exists x A(x, \vec{m})|_M = 1 \text{ и } |B(\vec{m})|_M = 1 \Leftrightarrow |\exists x A(x, \vec{m}) \wedge B(\vec{m})|_M = 1.$$

Таким образом,  $(*)$  выполняется.

(8) Рассмотрим случай  $\mathcal{Y} = \exists$ . Запишем  $A$  как  $A(a, \vec{e})$ , где  $\vec{e}$  — список всех параметров, кроме  $a$ . По определению истинности, в модели  $M$  для любого  $\vec{m}$

$$|\exists x A(x, \vec{m})|_M = \max_{k \in M} |A(k, \vec{m})|_M.$$

По тому же определению,

$$|\exists y A(y, \vec{m})|_M = \max_{k \in M} |A(k, \vec{m})|_M.$$

Т.е. первая равносильность из (8) очевидна.

Вторая равносильность тоже очевидна, т.к. выражения  $[y/a]A$  и  $[y/b][b/a]A$  совпадают: если заменить в  $A$  все вхождения  $a$  на новую букву  $b$ , а потом все вхождения  $b$  — на  $y$ , то это все равно, что сразу заменить все  $a$  на  $y$ .

Остальные утверждения леммы проверяются достаточно легко. ■

## Предваренная нормальная форма

**Определение 48.** *Предваренная нормальная форма (ПНФ)* — это формула вида

$$\mathcal{Y}_1 x_1 \dots \mathcal{Y}_n x_n [x_1, \dots, x_n / a_1, \dots, a_n] A,$$

где  $\mathcal{Y}_1, \dots, \mathcal{Y}_n$  — кванторы,  $A$  — формула без кванторов,  $a_1, \dots, a_n$  — (различные) свободные переменные,  $x_1, \dots, x_n$  — (различные) связанные переменные, не входящие в  $A$ . Формула без кванторов тоже считается ПНФ.



Мы докажем, что всякая формула первого порядка равносильна некоторой ПНФ. Начнем со вспомогательного преобразования формул.

**Определение 49.** *Формула с тесными отрицаниями (ТО)* — это формула, построенная из литералов (т.е. атомарных формул и их отрицаний) с помощью конъюнкции, дизъюнкции и кванторов.

Точное определение — индуктивное:

- Если  $A$  — атомарная формула, то  $A$  и  $\neg A$  — ТО-формулы.
- Если  $A, B$  — ТО-формулы, то  $(A \wedge B)$  и  $(A \vee B)$  — ТО-формулы.
- Если  $A$  — ТО-формула,  $a \in FVar$ ,  $x \in BVar$ ,  $x$  не входит в  $A$ , то  $\forall x[x/a]A$  и  $\exists x[x/a]A$  — ТО-формулы.

**Лемма 10.1.** *Всякая формула первого порядка равносильна некоторой ТО-формуле.*

**Доказательство** Идея доказательства состоит в том, что импликацию можно выразить через отрицание и дизъюнкцию, а все отрицания можно задвинуть вглубь, используя законы Де Моргана и лемму 9.10 (2),(3).

Аккуратное доказательство проводится по индукции: именно, индукцией по длине формулы  $A$ , доказываем, что  $A$  равносильна ТО-формуле, в которую входят те же переменные<sup>21</sup>.

Предположим, что утверждение доказано для всех формул, которые короче, чем  $A$ . По лемме 6.1, возможны следующие случаи.

(1)  $A$  — атомарная. Тогда  $A$  — ТО-формула, и доказывать нечего.

(2)  $A = (B \circ C)$ , где  $\circ$  — это  $\wedge$  или  $\vee$ . Формулы  $B, C$  — короче, и по предположению индукции, найдутся ТО-формулы  $B_1, C_1$ , такие что  $B \sim B_1, C \sim C_1$ . Тогда, по лемме 9.10 (6),  $A \sim (B_1 \circ C_1)$ , а по определению 49,  $(B_1 \circ C_1)$  — ТО-формула. Переменные в ней — те же, что в  $A$ , т.к. по предположению индукции, они не изменяются при переходе от  $B$  к  $B_1$  и от  $C$  к  $C_1$ .

(3)  $A = (B \rightarrow C)$ . Из логики высказываний (лемма 9.10 (1)) получаем  $A \sim (\neg B \vee C)$ . Формулы  $\neg B, C$  — короче, чем  $A$ , и тогда найдутся ТО-формулы  $B_1, C_1$ , такие что  $\neg B \sim B_1, C \sim C_1$ . По лемме 9.10 (6),(9),  $A \sim (B_1 \vee C_1)$ , и  $(B_1 \vee C_1)$  — ТО-формула. Переменные не меняются — по предположению индукции (как и в случае (2)).

(4)  $A = \mathcal{M}x[x/a]B$ ,  $x$  не входит в  $B$ . По предположению индукции,  $B \sim B_1$  для некоторой ТО-формулы  $B_1$  с теми же переменными. Поэтому  $x$  не входит в  $B_1$ , и, по лемме 9.10 (7),  $A \sim \mathcal{M}x[x/a]B_1$ . Ясно, что  $\mathcal{M}x[x/a]B_1$  — ТО-формула, и переменные из  $A$  в ней сохраняются.

(5)  $A = \neg B$ . Тогда рассмотрим все возможности для  $B$ .

(5.1)  $B$  — атомарная. Тогда  $A$  — ТО-формула, и доказывать нечего.

(5.2)  $B = (C \vee D)$ . Из логики высказываний (закон Де Моргана) имеем:  $A \sim (\neg C \wedge \neg D)$ . Формулы  $\neg C, \neg D$  — короче, поэтому найдутся ТО-формулы  $C_1, D_1$ , для которых  $\neg C \sim C_1, \neg D \sim D_1$ . По лемме 9.10,  $A \sim (C_1 \wedge D_1)$ , и снова получаем ТО-формулу. Переменные, как и раньше, сохраняются.

(5.3)  $B = (C \wedge D)$ . Этот случай аналогичен (5.2).

(5.4)  $B = (C \rightarrow D)$ . Из логики высказываний,  $A = \neg(C \rightarrow D) \sim (C \wedge \neg D)$ . Т.к.  $C, \neg D$  — короче, чем  $A$ , имеем ТО-формулы  $C_1, D_1$ , для которых  $C \sim C_1, \neg D \sim D_1$ . По лемме 9.10 (6),  $A \sim (C_1 \wedge D_1)$ .

(5.5)  $B = \forall x[x/a]C$ ,  $x$  не входит в  $C$ . По лемме 9.10 (2),  $A = \neg B \sim \exists x[x/a]\neg C$ . Т.к.  $\neg C$  — короче, чем  $A$ , имеется ТО-формула  $C_1$ , такая что  $\neg C \sim C_1$ . Из-за сохранения переменных,  $x$  не входит в  $C_1$ . По лемме 9.10 (7),

$$\exists x[x/a]\neg C \sim \exists x[x/a]C_1.$$

Итак,  $A$  равносильна ТО-формуле  $\exists x[x/a]C_1$  с теми же переменными.

(5.6)  $B = \exists x[x/a]C$ . Этот случай аналогичен (5.5).

(5.7)  $B = \neg C$ . По логике высказываний,  $A = \neg\neg C \sim C$ . По предположению индукции, имеем ТО-формулу  $C_1 \sim C$ . Итак,  $A \sim C_1$ . ■

<sup>21</sup>Последнее дополнение — техническое, оно понадобится далее в случаях (4), (5.5); в лекции оно не упоминалось.

**Теорема 10.2.** Любая формула первого порядка равносильна некоторой ПНФ.

**Доказательство** Благодаря лемме 10.1, достаточно доказать это для ТО-формул. Т.е. индукцией по длине ТО-формулы  $A$  доказываем, что  $A$  равносильна ПНФ. По лемме 6.1, возникают такие случаи.

(1)  $A$  — литерал. Тогда  $A$  — ПНФ, по определению.

(2)  $A = (B \circ C)$ , где  $\circ$  — это  $\vee$  или  $\wedge$ . По предположению индукции,  $B \sim B'$ ,  $C \sim C'$  для некоторых ПНФ  $B', C'$ . Тогда, по лемме 9.10,  $A = (B \circ C) \sim (B' \circ C')$ . Теперь нужна еще одна лемма.

**Лемма 10.3.** Если  $A, B$  — ПНФ,  $\circ = \vee$  или  $\wedge$ , то формула  $(A \circ B)$  равносильна ПНФ.

**Доказательство** Доказываем индукцией по числу кванторов в  $(A \circ B)$ .

Если кванторов нет, то это уже ПНФ, и доказывать нечего.

Если есть кванторы, то мы можем считать, что они есть в  $A$ : если они есть только в  $B$ , можно переставить  $A$  и  $B$  — т.к.  $(A \circ B) \sim (B \circ A)$  (логика высказываний).

Итак, пусть  $A = \mathcal{Y}x[x/a]A_1$ .

Случай 1.  $a, x$  не входят в  $B$ .

По лемме 9.10,

$$(A \circ B) = (\mathcal{Y}x[x/a]A_1 \circ B) \sim \mathcal{Y}x[x/a](A_1 \circ B).$$

Число кванторов в  $A_1 \circ B$  меньше, чем в  $A \circ B$ , и, по предположению индукции,  $(A_1 \circ B) \sim C$  для некоторой ПНФ  $C$ .

(1.1) Если  $x$  не входит в  $C$ , то, опять по лемме 9.10,

$$\mathcal{Y}x[x/a](A_1 \circ B) \sim \mathcal{Y}x[x/a]C.$$

Таким образом,  $(A \circ B)$  равносильна ПНФ  $\mathcal{Y}x[x/a]C$ .

(1.2) Если  $x$  входит в  $C$ , то возьмем новую связанную переменную  $y$ , которой нет в  $A_1, B, C$ . По лемме 9.10,  $A = \mathcal{Y}x[x/a]A_1 \sim \mathcal{Y}y[y/a]A_1$ , и далее  $(A \circ B) \sim (\mathcal{Y}y[y/a]A_1 \circ B)$ . Теперь, как в (1.1):

$$(\mathcal{Y}y[y/a]A_1 \circ B) \sim \mathcal{Y}y[y/a]C.$$

Случай 2.  $a$  или  $x$  входит в  $B$ .

Тогда можно эти переменные переименовать. А именно, выберем  $b \in FVar$ ,  $y \in BVar$ , которые не входят в  $B$ . По лемме 9.10,

$$A = \mathcal{Y}x[x/a]A_1 \sim \mathcal{Y}y[y/b][b/a]A_1.$$

Формула  $\mathcal{Y}y[y/b][b/a]A_1$  равносильна ПНФ, согласно случаю 1 (где вместо  $A_1$  надо использовать  $[b/a]A_1$ ). ■

Возвращаемся к доказательству теоремы 10.2, случай (2). По лемме 10.3 получаем, что  $(B' \circ C')$  равносильна ПНФ, поэтому и  $A$  равносильна ПНФ.

(3)  $A = \mathcal{Y}x[x/a]B$ .

По предположению индукции, имеется ПНФ  $B'$ , равносильная  $B$ . Выберем какую-нибудь связанную переменную  $y$ , не входящую ни в  $B$ , ни в  $B'$ . По лемме 9.10 получаем:

$$A = \mathcal{Y}x[x/a]B \sim \mathcal{Y}y[y/a]B \sim \mathcal{Y}y[y/a]B'.$$

Формула  $\mathcal{Y}y[y/a]B'$  — ПНФ. ■

Пример Рассмотрим формулу  $\forall xP(x) \vee \exists xQ(x)$ . Она приводится к ПНФ следующим образом:

$$(\forall xP(x) \vee \exists xQ(x)) \sim (\forall xP(x) \vee \exists yQ(y)) \sim \forall x(P(x) \vee \exists yQ(y)) \sim \forall x\exists y(P(x) \vee Q(y)).$$

Подробнее, это происходит так:

$$(\forall x[x/a]P(a) \vee \exists x[x/a]Q(a)) \sim (\forall x[x/a]P(a) \vee \exists y[y/b]Q(b))$$

$$\sim \forall x [x/a](P(a) \vee \exists y [y/b]Q(b)) \sim \forall x \exists y [x, y/a, b](P(a) \vee Q(b)).$$

Замечание В логике высказываний мы можем выяснить, является ли данная формула тавтологией, приведя ее к СДНФ. В логике предикатов аналогичный метод не работает: у одной и той же формулы могут быть несколько совершенно разных ПНФ. И по данной ПНФ непонятно, как установить общезначимость. В частности, неверно, что

$$\models \mathcal{M}x_1 \dots \mathcal{M}x_n [x_1, \dots, x_n/a_1, \dots, a_n]A \Rightarrow \models A.$$

Например, формула  $\exists x \forall y (P(x) \rightarrow P(y))$  общезначима, т.к.

$$\begin{aligned} \exists x \forall y (P(x) \rightarrow P(y)) &\sim \exists x \forall y (\neg P(x) \vee P(y)) \sim \\ \exists x (\neg P(x) \vee \forall y P(y)) &\sim (\exists x \neg P(x) \vee \forall y P(y)) \sim (\neg \forall x P(x) \vee \forall y P(y)) \\ &\sim (\neg \forall x P(x) \vee \forall x P(x)). \end{aligned}$$

При этом  $P(x) \rightarrow P(y)$  — совсем не общезначима.

## Лекция 11

### Исчисление предикатов

*Исчисление предикатов в сигнатуре  $\Omega$*  — это аксиоматическая система гильбертовского типа. Она обозначается через  $PC_\Omega$  и задается следующими аксиомами и правилами вывода.

I. 10 схем аксиом исчисления высказываний  $CL$  (см. лекцию 4). Но теперь  $A, B, C$  могут быть любыми формулами сигнатуры  $\Omega$ .

II. Предикатные аксиомы

- (1)  $\forall x [x/a]A \rightarrow [t/a]A$ .
- (2)  $[t/a]A \rightarrow \exists x [x/a]A$ .
- (3)  $\forall x [x/a](A \rightarrow B) \rightarrow (A \rightarrow \forall x [x/a]B)$ .
- (4)  $\forall x [x/a](B \rightarrow A) \rightarrow (\exists x [x/a]B \rightarrow A)$ .

Здесь  $A, B$  — произвольные формулы,  $t$  — произвольный терм,  $a$  — свободная переменная,  $x$  — связанная переменная. Формула  $[t/a]A$  получается из  $A$  заменой всех вхождений  $a$  на  $t$ .<sup>22</sup>

Ограничения Переменная  $x$  не должна входить в  $A$  и  $B$ . В аксиомах 3, 4 переменная  $a$  не должна входить в  $A$ .

III. Правила вывода.

*Modus Ponens (MP)*

$$\frac{A, A \rightarrow B}{B},$$

*Gen* (правило обобщения)

$$\frac{A}{\forall x [x/a]A}.$$

Здесь предполагается, что  $x$  не входит в  $A$ .

Определение вывода в исчислении предикатов аналогично исчислению высказываний, но здесь добавляется еще правило *Gen*.

**Определение 50.** Пусть  $\Gamma$  — некоторое множество формул сигнатуры  $\Omega$ . *Вывод формулы  $A$  в  $PC_\Omega$  из  $\Gamma$*  — это конечная последовательность формул, каждая из которых — аксиома или принадлежит  $\Gamma$  или получается из предыдущих по правилу MP или Gen, а последняя формула есть  $A$ .

Т.е. это последовательность формул  $A_1, \dots, A_n = A$ , где для всех  $k$  выполняется одно из условий:

<sup>22</sup>Формально  $[t/a]A$  надо определять индукцией по длине  $A$  и доказывать, что получается формула.

- $A_k$  — аксиома,
- $A_k \in \Gamma$ ,
- существуют  $i, j < k$ , для которых  $A_j = A_i \rightarrow A_k$ ,
- существует  $i < k$  и переменные  $x, a$  такие, что  $A_k = \forall x[x/a]A_i$ .

Формула  $A$  выводима из  $\Gamma$ , если существует ее вывод из  $\Gamma$ ; обозначение:  $\Gamma \vdash_{PC_\Omega} A$ .

Для этой выводимости сохраняется лемма 4.2 с тем же доказательством:

**Лемма 11.1.**

- (1) Если  $\Delta \subseteq \Gamma$  и  $\Delta \vdash A$ , то  $\Gamma \vdash A$ .
- (2) Если  $\Gamma \vdash A$ , то существует конечное  $\Delta \subseteq \Gamma$ , для которого  $\Delta \vdash A$ .
- (3) Если  $\Delta \vdash \Gamma$  и  $\Gamma \vdash A$ , то  $\Delta \vdash A$ .

**Лемма 11.2.** Пусть  $A$  — пропозициональная формула,  $SA$  — ее подстановочный пример в сигнатуре  $\Omega$ . Если  $\vdash_{CL} A$ , то  $\vdash_{PC_\Omega} SA$ .

Поскольку теоремы  $CL$  — это в точности тавтологии (лекция 5), то лемму можно сформулировать так: все подстановочные примеры тавтологий выводимы в исчислении предикатов.

**Доказательство** Индукция по длине вывода  $A$  в  $CL$ .

1. Если  $A$  — аксиома, то  $SA$  — аксиома того же вида. Это получается из того, что подстановка  $S$  дистрибутивна относительно логических связок. Например, если  $A$  — аксиома 1:

$$A = B \rightarrow (C \rightarrow B),$$

то

$$SA = SB \rightarrow (SC \rightarrow SB),$$

и это аксиома I.1 (в исчислении предикатов). Аналогично для других аксиом.

2. Пусть  $A$  получается по правилу  $MP$  из  $B$  и  $B \rightarrow A$ . По предположению индукции, в  $PC_\Omega$  выводимы  $SB$  и  $S(B \rightarrow A)$ . Но  $S(B \rightarrow A) = SB \rightarrow SA$ . Применяв  $MP$  в исчислении предикатов, получим  $\vdash_{PC_\Omega} SA$ . ■

**Лемма 11.3.** Некоторые теоремы и допустимые правила в  $PC_\Omega$ :

- (1)  $\forall x[x/a]A \rightarrow A$  ( $x$  не входит в  $A$ ).
- (2)  $A \rightarrow \exists x[x/a]A$  ( $x$  не входит в  $A$ ).

$$(3) \frac{A \rightarrow B}{A \rightarrow \forall x[x/a]B}.$$

$$(4) \frac{B \rightarrow A}{\exists x[x/a]B \rightarrow A}.$$

В двух последних правилах переменная  $x$  не входит в  $A, B$ ; переменная  $a$  не входит в  $A$ .

Правила (3), (4) называются ослабленными правилами Бернайса. В исходной (не ослабленной) форме  $x$  может входить в  $A$ ; этот вариант разберем чуть позже.

**Доказательство** (1), (2) Тривиальные случаи аксиом II.1, II.2 для  $t = x$ .

(3) (Мы опускаем индекс при  $\vdash$ .) Рассматриваем выводы из некоторого множества гипотез  $\Gamma$ .

Пусть  $\Gamma \vdash A \rightarrow B$ . По правилу  $Gen$  тогда  $\Gamma \vdash \forall x[x/a](A \rightarrow B)$ . По аксиоме II.3,  $\Gamma \vdash \forall x[x/a](A \rightarrow B) \rightarrow (A \rightarrow \forall x[x/a]B)$ . Теперь  $\Gamma \vdash A \rightarrow \forall x[x/a]B$  по  $MP$ .

(4) Аналогичное рассуждение с аксиомой II.4. (Упражнение.) ■

**Лемма 11.4.**  $\vdash_{PC_\Omega} \forall y[y/a]A \rightarrow \forall x[x/a]A$ ,  
где  $\forall$  – квантор, а переменные  $x, y$  не входят в  $A$ .

**Доказательство** Рассмотрим случай  $\forall = \forall$ .

$\vdash \forall y[y/a]A \rightarrow [x/a]A$  – аксиома П.1. Тогда  $\vdash \forall y[y/a]A \rightarrow \forall x[x/a]A$  по правилу Бернайса.

Случай  $\forall = \exists$  разбирается аналогично (упражнение). ■

**Лемма 11.5** (Ослабленная теорема дедукции). Если  $\Gamma, A \vdash_{PC_\Omega} B$  без применения правила *Gen*, то  $\Gamma \vdash_{PC_\Omega} A \rightarrow B$ .

**Доказательство** Доказательство – такое же, как для теоремы дедукции в *CL* (см. лекцию 4). ■

**Лемма 11.6.** В исчислении предикатов допустимо правило силлогизма

$$\frac{A \rightarrow B, B \rightarrow C}{A \rightarrow C}.$$

**Доказательство** Из теоремы дедукции следует, что это правило – производное. См. лекцию 4. ■

**Лемма 11.7.** В  $PC_\Omega$  в выводах из гипотез допустимы правила Бернайса:

$$(1) \frac{A \rightarrow B}{A \rightarrow \forall x[x/a]B}.$$

$$(2) \frac{B \rightarrow A}{\exists x[x/a]B \rightarrow A}.$$

где  $x$  не входит в  $B$ ; переменная  $a$  не входит в  $A$ .

**Доказательство** Докажем допустимость 1-го правила; второе рассматривается аналогично.

Пусть  $\Gamma \vdash A \rightarrow B$ . Выберем переменную  $y$ , не входящую ни в  $A$ , ни в  $B$ . Тогда по лемме 10.3

$$\Gamma \vdash A \rightarrow \forall y[y/a]B.$$

По лемме 11.4,

$$\vdash \forall y[y/a]B \rightarrow \forall x[x/a]B.$$

Отсюда по правилу силлогизма

$$\Gamma \vdash A \rightarrow \forall x[x/a]B.$$

**Теорема 11.8** (Теорема дедукции). Если  $A$  – замкнутая формула, то

$$\Gamma, A \vdash_{PC_\Omega} B \Leftrightarrow \Gamma \vdash_{PC_\Omega} A \rightarrow B.$$

**Доказательство** Утверждение ( $\Leftarrow$ ) легко получается по *MP* (для любой  $A$ ); см. лекцию 4.

( $\Rightarrow$ ) доказываем по индукции. Доказательство – как в лекции 4 и лемме 11.5, но еще надо рассмотреть случай, когда  $B$  получается по правилу *Gen*.

Итак, пусть  $B = \forall x[x/a]C$  и  $\Gamma, A \vdash C$ . По предположению индукции  $\Gamma \vdash A \rightarrow C$ . Тогда по правилу Бернайса (поскольку  $A$  замкнута) получаем

$$\Gamma \vdash A \rightarrow \forall x[x/a]C, \text{ т.е. } \Gamma \vdash A \rightarrow B. \quad \blacksquare$$

**Следствие 11.9.** Для любой конечной теории  $T$  и формулы  $A$  сигнатуры  $\Omega$

$$T \vdash_{PC_\Omega} A \Leftrightarrow \vdash_{PC_\Omega} (\bigwedge T) \rightarrow A.$$

Здесь  $\bigwedge T$  обозначает конъюнкцию всех формул из  $T$ .<sup>23</sup>

<sup>23</sup> Не имеет значения, в каком порядке берутся формулы и расставляются скобки в конъюнкции: утверждение от этого не зависит.

**Доказательство** (Мы опять опускаем индекс при  $\vdash$ .) По теореме дедукции

$$(*) \quad \bigwedge T \vdash A \Leftrightarrow \vdash (\bigwedge T) \rightarrow A.$$

Заметим также, что

$$(**) \quad T \vdash A \Leftrightarrow \bigwedge T \vdash A.$$

Действительно,  $T \vdash \bigwedge T$  — по допустимому правилу введения  $\wedge$  (см. лекцию 5); его надо применить несколько раз. Поэтому из  $\bigwedge T \vdash A$  по транзитивности (лемма 10.1(3)) следует  $T \vdash A$ .

Обратно,  $\bigwedge T \vdash T$  по аксиомам I.3, I.4 и MP. Поэтому из  $T \vdash A$  по транзитивности следует  $\bigwedge T \vdash A$ . Утверждение следствия получается из (\*) и (\*\*). ■

## Корректность исчисления предикатов

**Теорема 11.10** (Теорема о корректности исчисления предикатов).

(1) Пусть  $T$  — теория 1-го порядка в сигнатуре  $\Omega$ . Тогда для любой формулы  $A$  этой сигнатуры

$$T \vdash_{PC_\Omega} A \quad \Rightarrow \quad T \models \bar{\forall}A.$$

(2) Для любой формулы  $A$  сигнатуры  $\Omega$

$$\vdash_{PC_\Omega} A \quad \Rightarrow \quad \models A,$$

т.е. все теоремы исчисления предикатов общезначимы.

**Доказательство** Очевидно, что (2) следует из (1): надо взять  $T = \emptyset$  и вспомнить, что по определению общезначимость  $A$  равносильна общезначимости  $\bar{\forall}A$  (лекция 9).

(1) доказывается индукцией по длине вывода  $A$  в  $T$  аналогично теореме корректности для исчисления высказываний (теорема 4.5).

(1.1) Если  $A \in T$ , то доказывать нечего:  $A$  истинна во всех моделях  $T$  и  $\bar{\forall}A = A$ , т.к.  $A$  замкнута.

(1.2) Все аксиомы группы I — подстановочные примеры аксиом  $CL$ . Например, предикатная формула  $A \rightarrow (B \rightarrow A)$  — пример пропозициональной аксиомы  $P_1 \rightarrow (P_2 \rightarrow P_1)$  и т.д. Аксиомы  $CL$  — тавтологии (теорема корректности 4.5). Поэтому аксиомы группы I общезначимы по лемме о тавтологиях (лемма 9.5).

(1.3) Пусть  $A$  получается по  $MP$  из  $B$  и  $B \rightarrow A$ . Выводы этих формул короче, и по предположению индукции

$$T \models \bar{\forall}B, \quad T \models \bar{\forall}(B \rightarrow A).$$

Рассмотрим любую модель  $M$  теории  $T$  и докажем, что  $M \models \bar{\forall}A$ . По лемме 8.3 для этого надо заменить свободные переменные из  $A$  (обозначим их список  $\vec{a}$ ) на произвольные элементы из  $M$  (обозначим этот список  $\vec{m}$ ) и доказать, что полученная оцененная формула (обозначим ее  $A_1$ ) истинна в  $M$ .

Заметим, что при замене  $\vec{a}$  на  $\vec{m}$  в формуле  $B$  могут остаться еще какие-то свободные переменные; заменим их тоже на элементы из  $M$  (как угодно), и получим оцененную формулу  $B_1$ . Поскольку  $T \models \bar{\forall}B$  и  $M \models T$ , имеем  $M \models \bar{\forall}B$ , и по лемме 8.3,  $M \models B_1$ .

Аналогично  $M \models \bar{\forall}(B \rightarrow A)$ , откуда  $M \models B_1 \rightarrow A_1$  по лемме 8.3. Теперь из истинности  $B_1 \rightarrow A_1$  и  $B_1$  следует истинность  $A_1$  (по определению значения импликации; см. лекцию 7).

(1.4) Пусть  $A$  получается по правилу  $Gen$ , т.е.  $A = \forall x[x/a]B$ ,  $T \vdash B$ . Вывод  $B$  короче, и по предположению индукции  $T \models \bar{\forall}B$ .

Случай 1 Если  $a$  входит в  $B$ , то  $\bar{\forall}B$  и  $\bar{\forall}\forall x[x/a]B$  могут отличаться только порядком кванторов. Из леммы 8.3 следует, что эти формулы равносильны. Поэтому  $T \models \bar{\forall}A$ .

Случай 2  $a$  не входит в  $B$ . В этом случае тоже из  $M \models \bar{\forall}B$  следует  $M \models \bar{\forall}A$ .

В самом деле, пусть  $B = B(\vec{b})$ ,  $a$  не входит в  $\vec{b}$ . Допустим, что  $M \models \bar{\forall}B$ . Тогда для всех наборов  $\vec{m}$  элементов из  $M$  (той же длины, что  $\vec{b}$ )  $M \models B(\vec{m})$ .

В формуле  $A = \forall x[x/a]B(\vec{b})$  остаются все те же свободные переменные  $\vec{b}$ . Поэтому  $M \models \forall x[x/a]B(\vec{b})$  означает, что для всех  $\vec{m}$  из  $M$

$$M \models \forall x[x/a]B(\vec{m}).$$

Но это — то же, что  $M \models B(\vec{m})$ : т.к. переменная  $a$  в  $B(\vec{m})$  не входит, любая ее замена оказывается фиктивной. Итак,  $M \models \forall A$ .

(1.5)  $A$  — аксиома II.3:

$$A = \forall x[x/a](C \rightarrow B) \rightarrow (C \rightarrow \forall x[x/a]B),$$

где  $x$  не входит в  $C$  и  $B$ ,  $a$  не входит в  $C$ . Докажем общезначимость этой формулы. Выберем модель  $M$  и возьмем произвольную замену свободных переменных на элементы из  $M$ . Получим оцененную формулу

$$A_1 = \forall x[x/a](C_1 \rightarrow B_1) \rightarrow (C_1 \rightarrow \forall x[x/a]B_1).$$

Т.к.  $a$  не входит в  $C$ , здесь  $C_1$  — замкнутая (т.е. тоже оцененная) формула, а  $B_1$  может содержать только одну свободную переменную  $a$  (поскольку формула  $\forall x[x/a]B_1$  замкнута). Запишем  $B_1$  как  $B_1(a)$  и соответственно

$$A_1 = \forall x(C_1 \rightarrow B_1(x)) \rightarrow (C_1 \rightarrow \forall x B_1(x)).$$

Докажем, что  $M \models A_1$ . Предположим

$$M \models \forall x(C_1 \rightarrow B_1(x))$$

и проверим, что  $M \models C_1 \rightarrow \forall x B_1(x)$ . В свою очередь, для этого предположим

$$M \models C_1$$

и докажем  $M \models \forall x B_1(x)$ . Возьмем любое  $m \in M$ . Из  $M \models \forall x(C_1 \rightarrow B_1(x))$  следует

$$M \models C_1 \rightarrow B_1(m).$$

Тогда из  $M \models C_1$  следует  $M \models B_1(m)$ . Поскольку  $m$  произвольно, получаем  $M \models \forall x B_1(x)$ , что и требовалось.

(1.6)  $A$  — аксиома II.4. Этот случай аналогичен предыдущему. Доказательство — упражнение.

Оставшиеся аксиомы II.1, II.2 будут рассмотрены на следующей лекции. ■

## Лекция 12

### Корректность исчисления предикатов (окончание)

Для завершения доказательства теоремы корректности 11.10 осталось проверить общезначимость аксиом II.1 и II.2. Рассмотрим II.1 (II.2 проверяется аналогично — упражнение).

Рассуждаем как в случае II.3 (лекция 11). Нам надо доказать общезначимость формулы

$$A(a, \vec{b}) := \forall x[x/a]B \rightarrow [t/a]B,$$

где  $\vec{b}$  — список дополнительных параметров (кроме  $a$ ).<sup>24</sup> Тогда запишем  $B$  как  $B(a, \vec{b})$ ,  $t$  — как  $t(a, \vec{b})$ .

Рассмотрим модель  $M$  и заменим набор параметров  $a, \vec{b}$  на набор произвольных элементов  $q, \vec{m}$  из  $M$ . Получим оцененную формулу

$$A(q, \vec{m}) = \forall x[x/a]B(a, \vec{m}) \rightarrow [t(q, \vec{m})/a]B(a, \vec{m}).$$

Обозначим

$$B_1(a) := B(a, \vec{m}), \quad t_1 := t(q, \vec{m})$$

<sup>24</sup>Переменная  $a$  в формулу  $A$  может попасть из термина  $t$ . Если она не входит в  $t$  (и в  $A$ ), рассуждение не меняется.

и перепишем формулу  $A(q, \vec{m})$ :

$$A(q, \vec{m}) = \forall x[x/a]B_1(a) \rightarrow B_1(t_1).$$

Здесь  $B_1(t_1)$  обозначает  $[t_1/a]B_1(a)$ .

Нам надо доказать, что  $M \models A(q, \vec{m})$ . Для этого предположим

$$M \models \forall x[x/a]B_1(a)$$

и докажем

$$M \models B_1(t_1).$$

Достаточно будет установить следующий факт:

**Лемма 12.1.** Пусть  $B_1(a) \in Fm_{\Omega \cup M}$ ,  $r(a) \in Tm_{\Omega \cup M}$ ,  $t_1 \in CTm_{\Omega \cup M}$ . Тогда

$$(1) |r(t_1)|_M = |r(|t_1|_M)|_M,$$

$$(2) |B_1(t_1)|_M = |B_1(|t_1|_M)|_M.$$

(Здесь  $r(t_1)$  обозначает  $[t_1/a]r(a)$ .)

Из утверждения (2) получаем  $M \models B_1(t_1)$  (в предположении  $M \models \forall x[x/a]B_1(a)$ ), поскольку из  $M \models \forall x[x/a]B_1(a)$  следует  $M \models B_1(|t_1|_M)$ .

**Доказательство** (леммы). Индекс  $M$  при  $|\dots|$  не пишем. С некоторыми изменениями повторяется доказательство теоремы 7.4.

(1) Индукция по длине  $r$ .

(1.1) (базис индукции).  $r = c$ , для  $c \in Const_{\Omega}$ . Тогда  $a$  не входит в  $r$ , и доказывать нечего.

(1.2) (базис индукции).  $r = m$ , для  $m \in \underline{M}$ . Опять  $a$  не входит в  $r$ , и все очевидно.

(1.3) (базис индукции).  $r = a$ . Тогда

$$r(t_1) = t_1, \quad r(|t_1|) = |t_1|,$$

и также

$$|t_1| = ||t_1||,$$

по определению значения оцененного термина (лекция 7, опр. 4):  $|m| = m$  для всех  $m \in M$ .

(1.3) (шаг индукции).  $r(a) = f(r_1(a), \dots, r_n(a))$ . Тогда

$$r(t_1) = f(r_1(t_1), \dots, r_n(t_n)), \quad r(|t_1|) = f(r_1(|t_1|), \dots, r_n(|t_n|)),$$

и

$$(*) \quad |r(t_1)| = f_M(|r_1(t_1)|, \dots, |r_n(t_n)|), \quad |r(|t_1|)| = f_M(|r_1(|t_1|)|, \dots, |r_n(|t_n|)|).$$

Но по предположению индукции для термов  $r_i$

$$|r_i(t_1)| = |r_i(|t_1|)|.$$

Поэтому из (\*) имеем:

$$|r(t_1)| = |r(|t_1|)|.$$

(2) Индукция по числу связей и кванторов в  $B_1(a)$ .

(2.1) (базис индукции)  $B_1(a) = P(r_1(a), \dots, r_n(a))$  — атомарная. Доказательство аналогично (1.3) — упражнение.

(2.2) (шаг индукции)  $B_1$  получается применением  $\wedge, \vee, \rightarrow$  или  $\neg$ . Эти случаи почти очевидны — упражнение.

(2.3) (шаг индукции)  $B_1(a) = \exists x[x/b]C(a, b)$ .



Тогда

$$(**) \quad |B_1(t_1)| = |\exists x[x/b]C(t_1, b)| = \max_{l \in M} |C(t_1, l)|, \quad |B_1(|t_1|)| = |\exists x[x/b]C(|t_1|, b)| = \max_{l \in M} |C(|t_1|, l)|.$$

По предположению индукции, примененному к формуле  $C(a, l)$ ,

$$|C(t_1, l)| = |C(|t_1|, l)|$$

для каждого  $l \in M$ . Теперь из  $(**)$  получаем

$$|B_1(t_1)| = |B_1(|t_1|)|.$$

$$(2.4) \text{ (шаг индукции)} \quad B_1(a) = \forall x[x/b]C(a, b).$$

Доказательство аналогично (2.3):  $\exists$  заменяется на  $\forall$ , а  $\max$  — на  $\min$ . ■

## Исчисление предикатов с равенством

**Определение 51.** Пусть  $\Omega$  — сигнатура, содержащая предикатный символ равенства  $=$ . *Исчисление предикатов с равенством* в сигнатуре  $\Omega$  получается из обычного исчисления предикатов  $PC_\Omega$  добавлением аксиом стандартной теории равенства  $Eq_\Omega$  (см. лекцию 8).

Для теорий в такой сигнатуре можно рассматривать нормальные модели и логическое следование на них:  $T \vDash_{\text{норм}} A$  означает, что (замкнутая) формула  $A$  истинна во всех нормальных моделях теории  $T$ .

Также можно определить нормальную общезначимость: формула  $A$  *нормально общезначима*, если ее универсальное замыкание  $\bar{\forall}A$  истинно во всех нормальных моделях данной сигнатуры.

**Теорема 12.2** (Теорема о корректности исчисления предикатов с равенством).

(1) Пусть  $T$  — теория 1-го порядка с равенством в сигнатуре  $\Omega$ . Тогда для любой замкнутой формулы  $A$  этой сигнатуры

$$T \vdash_{PC_\Omega} A \Rightarrow T \vDash_{\text{норм}} A.$$

(2) Для любой формулы  $A$  сигнатуры  $\Omega$

$$\vdash_{PC_\Omega} A \Rightarrow \vDash_{\text{норм}} A,$$

т.е. все теоремы исчисления предикатов с равенством нормально общезначимы.

**Доказательство** (1) Пусть  $T \vdash_{PC_\Omega} A$ . По определению, это означает  $T \cup Eq_\Omega \vdash_{PC_\Omega} A$ . По теореме корректности 11.10

$$T \cup Eq_\Omega \vDash A.$$

Если  $M \vDash T$  и  $M$  нормальна, то  $M \vDash Eq_\Omega$  (лемма 8.4). Тогда  $M \vDash A$ .

(2) Как и в теореме 11.10, рассмотрим  $T = \emptyset$  и применим (1) для  $\bar{\forall}A$ . ■

## Непротиворечивость

**Определение 52.** Теория  $T$  в сигнатуре  $\Omega$  называется *противоречивой*, если для некоторой формулы  $A$  в этой сигнатуре

$$T \vdash_{PC_\Omega} A \text{ и } T \vdash_{PC_\Omega} \neg A.$$

Аналогично, теория  $T$  в сигнатуре  $\Omega$  с равенством *противоречива*, если  $T \vdash_{PC_\Omega} A$  и  $T \vdash_{PC_\Omega} \neg A$  для некоторой формулы  $A$  сигнатуры  $\Omega$ .

**Лемма 12.3.** Если теория  $T$  в сигнатуре  $\Omega$  противоречива, то  $T \vdash_{PC_\Omega} B$  для любой формулы сигнатуры  $B$ ; аналогично — для теорий с равенством.

**Доказательство** См. лемму 5.4 (2). ■

**Следствие 12.4.** (1) Если теория 1-го порядка выполнима, то она непротиворечива.

(2) Если теория 1-го порядка с равенством нормально выполнима (т.е. имеет нормальную модель), то она непротиворечива.

**Доказательство** (1) Предположим, что теория  $T$  в сигнатуре  $\Omega$  противоречива. Предположим, что  $M \models T$ . Возьмем какую-нибудь замкнутую формулу  $B$ , истинную в  $M$  (например, формулу вида  $A \rightarrow A$ ). По лемме 12.3,  $T \vdash_{PC\Omega} \neg B$ . Тогда по теореме корректности 11.10,  $T \models \neg B$ . Следовательно,  $M \models \neg B$ , что противоречит выбору  $B$ .

(2) Аналогично, с использованием  $PC\Omega^-$ . ■

### Пример: арифметика Пеано

*Арифметика Пеано* (PA) — это теория 1-го порядка в сигнатуре  $\{0, 1, +, \cdot, =\}$  (см. лекцию 6) со следующими аксиомами:

- (1)  $\forall x (x + 1 \neq 0)$ .
- (2)  $\forall x \forall y (x + 1 = y + 1 \rightarrow x = y)$ .
- (3)  $\forall x (x \neq 0 \rightarrow \exists y (y + 1 = x))$ .
- (4)  $\forall x (x + 0 = x)$ .
- (5)  $\forall x (x + (y + 1) = (x + y) + 1)$ .
- (6)  $\forall x (x \cdot 0 = 0)$ .
- (7)  $\forall x \forall y (x \cdot (y + 1) = x \cdot y + x)$ .
- (8)  $\bar{\forall} (A(0) \wedge \forall x (A(x) \rightarrow A(x + 1)) \rightarrow \forall x A(x))$ .

Здесь (1)–(7) — конкретные формулы, а (8) — схема, т.е. бесконечное множество аксиом определенного вида. Предполагается, что  $A$  — формула с несколькими свободными переменными, т.е.  $A = A(a, \dots)$ .  $A(0)$ ,  $A(x)$  обозначают соответственно  $[0/a]A$ ,  $[x/a]A$ ;  $\forall x (A(x) \rightarrow A(x + 1))$  — это формула  $\forall x [x/a](A \rightarrow [a + 1/a]A)$ .

(8) называется *схемой аксиом индукции*. Она выражает принцип математической индукции: если какое-то свойство  $A$  верно для 0 и из истинности  $A$  для  $x$  следует истинность для  $x + 1$ , то  $A$  верно для всех  $x$ . Однако в теории PA индукция постулируется только для тех свойств, которые можно записать формулами в данной сигнатуре.

Хотя теория PA и называется “арифметика Пеано”, она отличается от той, которую рассматривал сам Пеано: в его теории индукция применима ко всем свойствам натуральных чисел. Теория Пеано (в современном понимании) соответствует арифметике 2го порядка, которая в нашем курсе не изучается.

**Теорема PA** непротиворечива.

“Доказательство”. PA имеет *стандартную модель*  $\mathbb{N}$ : множество натуральных чисел (включая 0), где  $+$  интерпретируется как операция сложения,  $\cdot$  — как операция умножения, константа 0 — как число ноль, константа 1 — как число единица. Все аксиомы PA верны в этой модели. По следствию 12.4, PA непротиворечива.

Это — метаматематическое рассуждение; в нем предполагается известным, что такое натуральные числа и какие у них свойства. Чтобы дать строгое математическое доказательство, нужна формальная теория, где мы можем определить множество натуральных чисел. Это делается в аксиоматической теории множеств, о чем будет сказано кратко в лекции 14.

## Модальное исчисление S5

Некоторые части логики предикатов можно превратить в логики высказываний — так называемые *модальные логики*. В модальных логиках к обычным булевым связкам добавляются модальные связки, в простейшем случае — одноместная связка “необходимо” ( $\Box$ ).

В отличие от булевых связок, логические свойства связки  $\Box$  не очевидны и допускают много вариаций. Первые модальные исчисления были построены К.Льюисом (1918) и названы им S1, ..., S5. А вообще имеется огромное число (континуум) различных модальных логик.

В этом курсе мы рассмотрим только исчисление S5. Современная формулировка его была дана Гёделем (1933).

**Определение 53.** Множество модальных формул  $MFm$  строится по следующим правилам:

- Если  $A \in Var$ , то  $A \in MFm$ .
- Если  $A, B \in MFm$ , то  $(A \wedge B) \in MFm$ .
- Если  $A, B \in MFm$ , то  $(A \vee B) \in MFm$ .
- Если  $A, B \in MFm$ , то  $(A \rightarrow B) \in MFm$ .
- Если  $A \in MFm$ , то  $\neg A \in MFm$ .
- Если  $A \in MFm$ , то  $\Box A \in MFm$ .

Также будем использовать связку “возможно” ( $\Diamond$ ), которая определяется как сокращение:

$$\Diamond := \neg \Box \neg$$

### Схемы аксиом S5

(I) Схемы (1)–(10) из  $CL$ , но для модальных формул.

(II)

$$(AK) \quad \Box(A \rightarrow B) \rightarrow (\Box A \rightarrow \Box B),$$

$$(AT) \quad \Box A \rightarrow A,$$

$$(A4) \quad \Box A \rightarrow \Box \Box A,$$

$$(A5) \quad \Diamond \Box A \rightarrow \Box A.$$

### Правила вывода S5

Modus Ponens (MP),

Правило добавления  $\Box$  (Nec):  $\frac{A}{\Box A}$

Понятия вывода и выводимости в S5 определяются аналогично  $CL$  (с учетом дополнительного правила), точное определение оставляется читателю.

## Семантика Крипке для S5

**Определение 54.** Пусть  $W \neq \emptyset$  — множество. *Оценка* (пропозициональных переменных) на  $W$  — это отображение  $Var \rightarrow \mathcal{P}(W)$ . *Модель Крипке*<sup>25</sup> на  $W$  — это пара  $(W, \theta)$ , где  $\theta$  — оценка на  $W$ .  $W$  называется *множеством (возможных) миров* этой модели.

**Определение 55.** Для модели Крипке  $M = (W, \theta)$ , мира  $u \in W$  и модальной формулы  $A$  определяем *значение*  $A$  в  $u$ ; оно обозначается  $|A|_u^M$ . Определение дается индукцией по длине  $A$  сразу для всех миров  $u$ :

- $|P_i|_u^M = 1 \Leftrightarrow u \in \theta(P_i)$  для каждой переменной  $P_i$ ,

<sup>25</sup>Иногда говорят: модель Крипке – Лейбница

- $|A \wedge B|_u^M = \min(|A|_u^M, |B|_u^M)$ ,
- $|A \vee B|_u^M = \max(|A|_u^M, |B|_u^M)$ ,
- $|\neg A|_u^M = 1 - |A|_u^M$ ,
- $|A \rightarrow B|_u^M = \max(1 - |A|_u^M, |B|_u^M)$ ,
- $|\Box A|_u^M = \min_{v \in W} |A|_v^M$ .

Чтобы доказать корректность этого определения, нужна лемма об однозначном анализе формул, аналогичная лемме 1.1. См. лекцию 1.

Вместо  $|A|_u^M = 1$  пишут также  $M, u \models A$  и говорят, что формула  $A$  истинна в модели  $M$  в мире  $u$ . В этих обозначениях определение 55 записывается так:

- $M, u \models P_i \Leftrightarrow u \in \theta(P_i)$ ,
- $M, u \models A \wedge B \Leftrightarrow M, u \models A$  и  $M, u \models B$ ,
- $M, u \models A \vee B \Leftrightarrow M, u \models A$  или  $M, u \models B$ ,
- $M, u \models \neg A \Leftrightarrow M, u \not\models A$ ,
- $M, u \models A \rightarrow B \Leftrightarrow M, u \not\models A$  или  $M, u \models B$ ,
- $M, u \models \Box A \Leftrightarrow \forall v \in W M, v \models A$ .

Из определения сразу получаем:

$$M, u \models \Diamond A \Leftrightarrow \exists v \in W M, v \models A.$$

Таким образом, в семантике Крипке “необходимо” ( $\Box$ ) понимается как истинность во всех мирах (“всегда”), а “возможно” ( $\Diamond$ ) — как истинность в некоторых мирах (“иногда”).

**Определение 56.** Модальная формула  $A$  *общезначима* на (непустом) множестве  $W$ , если она истинна во всех мирах в любой модели Крипке на  $W$ .

Общезначимость  $A$  на  $W$  обозначается  $W \models A$ .

**Теорема 12.5** (Теорема корректности для  $S5$ ). *Если  $\vdash_{S5} A$ , то  $W \models A$  для любого  $W \neq \emptyset$ .*

Это утверждение можно доказать индукцией по длине вывода  $A$ . У нас оно получится как следствие другой теоремы на следующей лекции.

## Стандартный перевод модальных формул

**Определение 57.** Рассмотрим сигнатуру со счетным множеством одноместных предикатных символов:  $P_1^1, P_2^1, \dots$ . *Стандартный перевод* (или перевод Вайсберга)  $A \mapsto A^*$  модальных формул в формулы 1-го порядка в этой сигнатуре определяется по индукции:

- $P_i^* := P_i^1(a)$ ,
- $(A \circ B)^* := (A^* \circ B^*)$  для  $\circ = \vee, \rightarrow, \wedge$ ,
- $(\neg A)^* := \neg A^*$ ,
- $(\Box A)^* := \forall x [x/a]A^*$ , где  $x$  — первая связанная переменная (в общем списке  $BVar$  — см. лекцию 6), не входящая в  $A^*$ .<sup>26</sup>

Таким образом,  $A^*$  — формула с одной свободной переменной  $a$  или замкнутая.

<sup>26</sup>Можно взять и любую другую переменную, не попавшую в  $A$ , но мы выбираем первую для единообразия.

**Определение 58.** Каждой модели Крипке  $M = (W, \theta)$  поставим в соответствие модель  $M^*$  сигнатуры  $\{P_1^1, P_2^1, \dots\}$  с носителем  $W$ . А именно, полагаем для каждого  $u \in W$

$$M^* \models P_i^1(u) \Leftrightarrow M, u \models P_i.$$

Это можно записать и так:

$$|P_i^1(u)|_{M^*} := |P_i|_u^M.$$

**Лемма 12.6.** Для любой модальной формулы  $A$

$$|A^*(u)|_{M^*} = |A|_u^M.$$

**Доказательство** Индукцией по длине  $A$  доказываем утверждение для всех  $u$ .

Если  $A$  — переменная, утверждение следует из определений 57, 58.

Если  $A$  имеет вид отрицания, конъюнкции, дизъюнкции или импликации, утверждение легко следует из определений истинности для модальных формул и формул 1-го порядка — упражнение.

Пусть  $A = \Box B$ . Тогда по определению 5 лекции 7 и опр. 55 выше,

$$|A^*(u)|_{M^*} = |(\forall x [x/a]B^*)(u)|_{M^*} = \min_{v \in W} |B^*(v)|_{M^*},$$

$$|A|_u^M = \min_{v \in W} |B|_v^M.$$

По предположению индукции,  $|B^*(v)|_{M^*} = |B|_v^M$ . Поэтому утверждение верно для  $A$ . ■

**Лемма 12.7.** <sup>27</sup> Для любой модальной формулы  $A$  и непустого  $W$

$$W \models \forall x [x/a]A^* \text{ в классической логике} \Leftrightarrow W \models A \text{ в модальной логике}.$$

**Доказательство** ( $\Rightarrow$ ) Доказываем от противного. Пусть  $W \not\models A$ , тогда для некоторой модели Крипке  $M$  на  $W$  и какого-то мира  $u \in W$

$$M, u \not\models A.$$

Отсюда по лемме 12.6

$$M^* \not\models A^*(u),$$

следовательно,

$$M^* \not\models \forall x [x/a]A^*,$$

и потому

$$W \not\models \forall x [x/a]A^*.$$

( $\Leftarrow$ ) Тоже рассуждаем от противного. Пусть

$$W \not\models \forall x [x/a]A^*.$$

Тогда найдется модель  $\mu$  нашей сигнатуры (с одноместными предикатами) с носителем  $W$  такая, что

$$\mu \not\models \forall x [x/a]A^*.$$

т.е. для некоторого  $u \in W$

$$(\#) \quad \mu \not\models A^*(u).$$

Но  $\mu = M^*$  для некоторой модели Крипке  $M$  на  $W$ : она однозначно задается равенствами

$$|P_i|_v^M = |P_i^1(v)|_\mu$$

для всех  $v, i$ . Поэтому из (#) по лемме 12.6 получаем

$$M, u \not\models A.$$

Таким образом,  $W \not\models A$ . ■

<sup>27</sup>На лекции в формулировке этой леммы была допущена неточность: запись  $\forall u A^*(u)$  неправомерна.

# Лекция 13

## Свойства исчисления S5

На прошлой лекции мы для каждой модальной формулы  $A$  построили перевод  $A^*(a)$  — формулу в сигнатуре с одноместными предикатами.

**Теорема 13.1.** *Следующие утверждения эквивалентны:*

- (1)  $\vdash_{S5} A$ ,
- (2)  $\vdash_{PC} A^*$ ,
- (3)  $\vDash A^*$ ,
- (4)  $W \vDash A^*$  на всех конечных  $W$ ,
- (5)  $W \vDash A$  на всех  $W$ ,
- (6)  $W \vDash A$  на всех конечных  $W$ .

Здесь  $PC$  понимается как исчисление предикатов в сигнатуре с одноместными предикатами  $P_i^1$  и без равенства.

### Доказательство

Доказывать будем следующие импликации:

$$\begin{array}{ccc}
 1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4 & & \\
 \uparrow & \downarrow & \downarrow \\
 6 & 5 \Rightarrow 6 & 
 \end{array}$$

(1  $\Rightarrow$  2). Индукция по длине вывода  $A$  в  $S5$ .

- Если  $A$  — аксиома группы (I), то  $A^*$  — аксиома  $PC$  того же вида (из группы I). Например, если  $A = (B \wedge C) \rightarrow B$ , то  $A^* = (B^* \wedge C^*) \rightarrow B^*$  и т.д.
- Пусть

$$A = (\Box(C \rightarrow B) \rightarrow (\Box C \rightarrow \Box B)).$$

Тогда

$$A^* = (\forall x(C^*(x) \rightarrow B^*(x)) \rightarrow (\forall x C^*(x) \rightarrow \forall x B^*(x))).$$

Тогда  $\vdash_{PC} A^*$  получим по теореме дедукции (она применима, т.к. все гипотезы — замкнутые) из следующей выводимости:

$$\forall x(C^*(x) \rightarrow B^*(x)), \forall x C^*(x) \vdash \forall x B^*(x).$$

А это доказывается непосредственно:

1.  $\forall x(C^*(x) \rightarrow B^*(x))$  — гипотеза.
2.  $\forall x(C^*(x) \rightarrow B^*(x)) \rightarrow (C^*(a) \rightarrow B^*(a))$  — аксиома II.1 из  $PC$ .
3.  $C^*(a) \rightarrow B^*(a)$  — 1, 2, МР.
4.  $\forall x C^*(x)$  — гипотеза.
5.  $\forall x C^*(x) \rightarrow C^*(a)$  — аксиома II.1 из  $PC$ .
6.  $C^*(a)$  — 4, 5, МР.
7.  $B^*(a)$  — 3, 6, МР.
8.  $\forall x B^*(x)$  — 7, Gen.

- Пусть  $A = (\Box B \rightarrow B)$ . Тогда  $A^* = \forall x B^*(x) \rightarrow B^*(a)$  — аксиома.
- $A = (\Box B \rightarrow \Box \Box B)$ . Тогда  $A^* = (\forall x B^*(x) \rightarrow \forall y \forall x B^*(x))$  получается с помощью правила Бернаиса из  $\forall x B^*(x) \rightarrow \forall x B^*(x)$  (примера тавтологии — см. лемму 11.2).
- $A = (\Diamond \Box B \rightarrow \Box B)$ . Тогда  $A^* = (\exists y \forall x B^*(x) \rightarrow \forall x B^*(x))$  получается из  $\forall x B^*(x) \rightarrow \forall x B^*(x)$  с помощью второго правила Бернаиса.
- $A$  получается по  $MP$  из  $B, B \rightarrow A$ . По предположению индукции,

$$\vdash_{PC} B^*, B^* \rightarrow A^*.$$

Тогда  $\vdash_{PC} A^*$  по  $MP$ .

- $A = \Box B$  получается по  $Nec$  из  $B$ . Тогда  $A^* = \forall x B^*(x)$ . По предположению индукции,  $\vdash_{PC} B^*(a)$ . Отсюда  $\vdash_{PC} A^*$  по  $Gen$ .

(2  $\Rightarrow$  3). Это следует из теоремы корректности для  $PC$ .

(3  $\Rightarrow$  4), (5  $\Rightarrow$  6) очевидны.

(4  $\Rightarrow$  6). Получается из леммы 12.7.<sup>28</sup>

(3  $\Rightarrow$  5). Получается из леммы 12.7.

(6  $\Rightarrow$  1). Это — теорема о полноте  $S5$  относительно конечных моделей Крипке. Ее доказательство занимает всю оставшуюся часть лекции.

**Определение 59.** Модальные формулы  $A, B$  доказуемо эквивалентны в  $S5$ , если  $\vdash_{S5} A \leftrightarrow B$ . Обозначение:  $A \equiv_{S5} B$ .

Далее мы будем опускать индекс  $S5$ .

**Лемма 13.2** (Некоторые синтаксические свойства  $S5$ ). (1) Допустимы правила монотонности

$$\frac{A \rightarrow B}{\Box A \rightarrow \Box B}, \quad \frac{A \rightarrow B}{\Diamond A \rightarrow \Diamond B}.$$

(2)  $\equiv$  задает отношение эквивалентности на  $MFT$ .

(3)  $\equiv$  согласовано со всеми связками:

если  $A \equiv A'$ , то  $\Box A \equiv \Box A'$ ,  $\neg A \equiv \neg A'$ ;

если  $A \equiv A'$  и  $B \equiv B'$ , то  $(A \circ B) \equiv (A' \circ B')$  для  $\circ = \vee, \wedge, \rightarrow$ .

(4) Если  $A$  — подформула формулы  $B$  и  $A \equiv A'$ , то замена вхождения  $A$  на  $A'$  в  $B$  даст эквивалентную формулу:  $B(\dots A \dots) \equiv B(\dots A' \dots)$ .

(5)  $\Diamond(A \vee B) \equiv \Diamond A \vee \Diamond B$ .

(6)  $\Diamond(A \wedge \Diamond B) \equiv \Diamond A \wedge \Diamond B$ .

(7)  $\Diamond(A \wedge \Box B) \equiv \Diamond A \wedge \Box B$ .

(8)  $\Box(A \wedge B) \equiv \Box A \wedge \Box B$ .

Доказательство (не слишком трудное) опускаем.

**Определение 60.** Модальные формулы глубины 1 определяются по индукции:

- $P_i$  — глубины 1,
- если  $A$  — глубины 1, то  $\neg A$  — глубины 1,

<sup>28</sup> $W \vDash A^*$  означает то же, что  $W \vDash \forall x[x/a]A^*(a)$ .

- если  $A, B$  — глубины 1, то  $A \circ B$  — глубины 1 для  $\circ = \vee, \wedge, \rightarrow$ .
- если  $A \in Fm$  (классическая формула), то  $\diamond A$  — глубины 1.

**Лемма 13.3** (О нормальной форме для формул глубины 1). *Если  $A$  — глубины 1, то  $A \equiv \bigvee_i A_i$ , где  $A_i$  — вида  $\bigwedge_j Q_{ij}$ , а каждое  $Q_{ij}$  — либо литерал, либо формула вида  $\diamond D$  или  $\neg \diamond D$ , где  $D$  — классическая.*

**Доказательство** Из определения 60 следует, что формула  $A$  имеет вид  $B(P_1, \dots, P_n, \diamond C_1, \dots, \diamond C_m)$ , где  $B(P_1, \dots, P_n, P_{n+1}, \dots, P_{n+m})$  и  $C_1, \dots, \diamond C_m$  — классические формулы. (Это легко доказывается по индукции.)

Формулу  $B$  можно привести к СДНФ:  $B \sim \bigvee_i B_i$ , где  $B_i$  — элементарные конъюнкции. По теореме полноты для  $CL$  тогда

$$\vdash_{CL} B \leftrightarrow \bigvee_i B_i.$$

Тогда, подставив формулы  $\diamond C_1, \dots, \diamond C_m$  вместо  $P_{n+1}, \dots, P_{n+m}$  в этот вывод, получим

$$\vdash_{S5} A \leftrightarrow \bigvee_i A_i,$$

где  $A_i = B_i(P_1, \dots, P_n, \diamond C_1, \dots, \diamond C_m)$ . Поскольку  $B_i$  — элементарная конъюнкция,  $A_i$  окажется конъюнкцией формул  $P_1, \dots, P_n, \diamond C_1, \dots, \diamond C_m$  или их отрицаний, что и требовалось. ■

**Лемма 13.4.** *Существует лишь конечное число попарно не эквивалентных формул глубины 1 от переменных  $P_1, \dots, P_n$ .*

**Доказательство** Достаточно рассмотреть нормальные формы из предыдущей леммы.

С точностью до  $\equiv$ , имеется конечное число конъюнкций  $A_i$ . Действительно, каждая из них содержит литералы от  $P_1, \dots, P_n$  и формулы вида  $\diamond D, \neg D$ , где  $D$  — классическая формула от  $P_1, \dots, P_n$ . Такие формулы  $D$  приводятся к СДНФ в  $CL$ , и тем более, в  $S5$ . И если  $D \equiv D'$ , то  $\diamond D \equiv \diamond D'$ ,  $\neg \diamond D \equiv \neg \diamond D'$  — по лемме 13.2.

Из конечного числа  $A_i$  можно построить лишь конечное число их дизъюнкций с точностью до  $\equiv$  (здесь снова пользуемся леммой 13.2). ■

**Лемма 13.5.** *В  $S5$  всякая формула эквивалентна формуле глубины 1 (от тех же переменных).*

**Доказательство** Запишем эквивалентную формулу, используя связку  $\diamond$  вместо  $\square$  (это можно сделать, т.к.  $\square A \equiv \neg \diamond \neg A$ ). Далее рассуждаем индукцией по длине формулы.

Нетривиален только шаг индукции для формулы вида  $\diamond A$ . По предположению индукции,  $A$  эквивалентна формуле глубины 1, и значит, нормальной форме из леммы 13.3. Тогда  $\diamond A \equiv \bigvee_i \diamond A_i$  (лемма 13.2 (5),(3)).

Рассмотрим  $\diamond A_i = \diamond \bigwedge_j Q_{ij}$ . Используя лемму 13.2 (6),(7) (и эквивалентность  $\neg \diamond D \equiv \square \neg D$ ), преобразуем эту формулу в конъюнкцию формул вида  $\diamond P_k, \diamond D, \square D$  (где  $D$  — классическая), т.е. в формулу глубины 1. ■

Из лемм 13.4, 13.5 получаем

**Предложение 13.6.** *(о локальной табличности  $S5$ )*

*Существует конечное число формул от переменных  $P_1, \dots, P_n$ , попарно не эквивалентных в  $S5$ .*

Упражнение Оцените количество этих формул в зависимости от  $n$ .

**Определение 61.** Для множества модальных формул  $\Gamma$  *выводимость* формулы  $A$ , (обозначение:  $\Gamma \vdash_{S5} A$ ) означает, что существует вывод  $A$  с использованием формул из  $\Gamma$ , аксиом  $S5$  и правила  $MP$  (но не  $Gen$ ).

$\Gamma$  *противоречиво* в  $S5$ , если  $\Gamma \vdash_{S5} A, \neg A$  для некоторой формулы  $A$ .



Легко видеть, что для этой выводимости сохраняются лемма 5.4 и теорема дедукции 4.4.

Пусть  $\Phi$  — множество всех модальных формул от  $P_1, \dots, P_n$ . Рассматриваем непротиворечивые (в  $S5$ ) подмножества  $\Phi$ .

**Определение 62.** Множество  $\Gamma \subseteq \Phi$  называется *максимальным*, если оно непротиворечиво, а всякое его собственное расширение внутри  $\Phi$  противоречиво.

**Лемма 13.7.** *Всякое непротиворечивое множество содержится в максимальном.*

**Доказательство** Если  $\Gamma$  непротиворечиво, но не максимально, то найдется  $A$  такая, что  $\Gamma \cup \{A\}$  непротиворечиво. Тогда и  $\Gamma \cup \{A' \in \Phi \mid A' \equiv A\}$  непротиворечиво. Действительно, если противоречие выводится из

$\Gamma, A, A'_1, \dots, A'_k$  и все  $A'_i$  эквивалентны  $A$ , то оно выводится уже из  $\Gamma \cup \{A\}$  — поскольку  $\vdash_{S5} A \rightarrow A'_i$ , а тогда  $\Gamma \cup \{A\} \vdash A'_i$  (по МР).

Если же мы будем расширять  $\Gamma$ , добавляя вместе с каждой формулой все эквивалентные ей, то за конечное число шагов мы получим все  $\Phi$  — это следует из локальной табличности  $S5$ . Значит, за (меньшее) конечное число таких шагов мы можем получить максимальное множество. ■

**Лемма 13.8** (Свойства максимальных множеств). *Для максимального  $\Gamma$  сохраняются свойства из леммы 5.6:*

- (0)  $\Gamma \vdash B \Rightarrow B \in \Gamma$  (для  $B \in \Phi$ );
- (1)  $\neg B \in \Gamma \Leftrightarrow B \notin \Gamma$ ;
- (2)  $(B \wedge C) \in \Gamma \Leftrightarrow (B \in \Gamma \text{ и } C \in \Gamma)$ ;
- (3)  $(B \vee C) \in \Gamma \Leftrightarrow (B \in \Gamma \text{ или } C \in \Gamma)$ ;
- (4)  $(B \rightarrow C) \in \Gamma \Leftrightarrow (B \notin \Gamma \text{ или } C \in \Gamma)$ .

**Определение 63.** Определим отношение достижимости на максимальных множествах:

$$\Gamma R \Delta := \forall A (\Box A \in \Gamma \Rightarrow A \in \Delta).$$

**Лемма 13.9.**  $R$  — отношение эквивалентности.

**Доказательство**

- Рефлексивность.

Пусть  $\Box A \in \Gamma$ . Т.к.  $\Box A \rightarrow A$  — аксиома  $S5$ , она лежит в  $\Gamma$  (лемма 13.8 (0)). Тогда  $\Gamma \vdash A$  по МР, а потому  $A \in \Gamma$  (опять по 13.8 (0)). По определению  $R$  имеем  $\Gamma R \Gamma$ .

- Транзитивность.

Предположим  $\Gamma R \Delta R \Xi$  и докажем  $\Gamma R \Xi$ .

Пусть  $\Box A \in \Gamma$ . Т.к.  $\Box A \rightarrow \Box \Box A$  — аксиома  $S5$ , она лежит в  $\Gamma$ . Тогда  $\Gamma \vdash \Box \Box A$  по МР, а потому  $\Box \Box A \in \Gamma$ . Теперь из  $\Gamma R \Delta$  получаем, что  $\Box A \in \Delta$ . И из  $\Delta R \Xi$  — что  $A \in \Xi$ .

- Симметричность.

Предположим  $\Gamma R \Delta$  и докажем  $\Delta R \Gamma$ .

Пусть  $\Box A \in \Delta$ . Тогда  $\Diamond \Box A = \neg \Box \neg \Box A \in \Gamma$ . В самом деле, иначе  $\Box \neg \Box A \in \Gamma$  (лемма 13.8(1)). А тогда  $\neg \Box A \in \Delta$  (т.к.  $\Gamma R \Delta$ ), что дает противоречие в  $\Delta$ .

Таким образом,  $\Diamond \Box A \in \Gamma$ . Кроме того,  $(\Diamond \Box A \rightarrow A) \in \Gamma$  — это аксиома  $S5$ . Отсюда по МР и 13.8(0) получаем  $A \in \Gamma$ , что и требовалось. ■

Доказываем теперь импликацию  $6 \Rightarrow 1$  из теоремы 13.1: для данной формулы  $A$ , не выводимой в  $S5$ , построим опровергающую конечную модель Крипке.

Т.к.  $\not\vdash_{S5} A$ , множество  $\{\neg A\}$  непротиворечиво. По лемме 13.7 построим максимальное множество  $\Gamma$ , содержащее  $\neg A$ . Пусть

$$W := \{\Delta \mid \Gamma R \Delta\}.$$

Из предложения 13.6 и леммы 13.8 следует, что  $W$  конечно. Зададим оценку на  $W$ :

$$\theta(P_i) := \{\Delta \mid P_i \in \Delta\}$$

и рассмотрим модель Крипке  $M := (W, \theta)$ .

**Лемма 13.10** (Основная лемма).

$$M, \Delta \vDash B \Leftrightarrow B \in \Delta$$

для всех  $B(P_1, \dots, P_n)$  и  $\Delta \in W$ .

**Доказательство** Индукция по длине  $B$ .

- $B$  — переменная. Тогда утверждение верно по определению  $\theta$ .
- $B = (C \vee D)$ . Тогда по определению 5 лекции 12, предположению индукции и лемме 13.8 (3)

$$\begin{aligned} M, \Delta \vDash B &\Leftrightarrow (M, \Delta \vDash C \text{ или } M, \Delta \vDash D) \Leftrightarrow (C \in \Delta \text{ или } D \in \Delta) \\ &\Leftrightarrow (C \vee D) \in \Delta, \end{aligned}$$

что и требовалось.

- Случаи связок  $\wedge, \rightarrow, \neg$  разбираются аналогично (упражнение).
- $B = \Box C$ . Проверим эквивалентность

$$M, \Delta \vDash \Box C \Leftrightarrow \Box C \in \Delta.$$

( $\Leftarrow$ ) Пусть  $\Box C \in \Delta$ . Чтобы доказать  $M, \Delta \vDash \Box C$ , рассмотрим  $\Psi \in W$ . Поскольку  $R$  — отношение эквивалентности и  $\Gamma R \Delta$ ,  $\Gamma R \Psi$ , получаем  $\Delta R \Psi$ . Тогда  $C \in \Psi$  (по определению  $R$ ). Отсюда  $M, \Psi \vDash C$ , по предположению индукции.

( $\Rightarrow$ ) Предположим  $\Box C \notin \Delta$  и докажем  $M, \Delta \not\vDash \Box C$ . Для этого надо построить  $\Psi \in W$  такое, что  $M, \Psi \not\vDash C$ .

Рассмотрим множество

$$V := \{D \mid \Box D \in \Delta\} \cup \{\neg C\}.$$

Покажем, что  $V$  непротиворечиво. Действительно, иначе бы (по лемме 5.4)

$$D_1, \dots, D_k \vdash_{S5} C$$

для некоторых  $D_1, \dots, D_k$ , где  $\Box D_1, \dots, \Box D_k \in \Delta$ . Тогда по теореме дедукции

$$\vdash_{S5} \bigwedge_i D_i \rightarrow C,$$

откуда по правилу монотонности

$$(*) \quad \vdash_{S5} \Box(\bigwedge_i D_i) \rightarrow \Box C.$$

Но по лемме 13.2 (8) (многократно)

$$\Box(\bigwedge_i D_i) \equiv \bigwedge_i \Box D_i.$$

Вспомогая, что  $\Box D_i \in \Delta$ , получаем  $(\bigwedge_i \Box D_i) \in \Delta$  по лемме 13.8. Из той же леммы следует, что максимальное множество содержит вместе с каждой формулой и все ей эквивалентные. Поэтому  $\Box(\bigwedge_i D_i) \in \Delta$ , и из (\*) по МР следует  $\Box C \in \Delta$ . Это противоречит исходному предположению.

Итак,  $V$  непротиворечиво. Выберем максимальное  $\Psi$ , содержащее  $V$ . Из определения  $V$  получается:  $\Delta R \Psi$ ,  $C \notin \Psi$  (т.к.  $\neg C \in \Psi$ ). Тогда:

$\Gamma R \Psi$  по транзитивности  $R$  (т.е.  $\Psi \in W$ ),

$M, \Psi \not\vdash C$  по предположению индукции, т.к.  $C \notin \Psi$ .

■

Наконец, из леммы 13.10 следует  $W \not\vdash A$ , что и требовалось. ■

## Лекция 14

### Полнота исчисления предикатов и ее следствия

Мощностью сигнатуры  $\Omega$  (обозначение:  $|\Omega|$ ) назовем мощность<sup>29</sup> множества всех ее символов, т.е. множества  $Pred_\Omega \cup Const_\Omega \cup Fun_\Omega$ .

**Теорема 14.1** (О существовании модели). (1) Пусть  $T$  — непротиворечивая теория без равенства в сигнатуре  $\Omega$ . Тогда  $T$  имеет модель мощности  $|\Omega|$  или счетную, если  $\Omega$  конечна.

(2) Пусть  $T$  — непротиворечивая теория с равенством в сигнатуре  $\Omega$ . Тогда  $T$  имеет нормальную модель мощности  $\leq |\Omega|$  или не более, чем счетную, если  $\Omega$  конечна.

**Доказательство** Утверждение (1) в этом курсе не доказывается.

(2) получается из (1) следующим образом.

Напомним, что непротиворечивость теории с равенством  $T$  понимается относительно  $PC_\Omega^=$ , т.е. как непротиворечивость теории  $T \cup Eq_\Omega$  относительно  $PC_\Omega$ . Согласно (1),  $T \cup Eq_\Omega$  имеет модель  $M$  мощности  $|\Omega|$  (или счетную). По лемме о нормализации (теорема 8.5),  $M \equiv \widetilde{M}$ , где  $\widetilde{M}$  — нормальная модель с носителем  $\underline{M}/\approx$ . Тогда  $|\widetilde{M}| \leq |M|$ .<sup>30</sup> Таким образом,  $\widetilde{M}$  — модель  $T$  нужной мощности. ■

**Теорема 14.2** (Теорема Гёделя о полноте исчисления предикатов (с равенством)).

(1) Для теории  $T$  и замкнутой формулы  $A$  сигнатуры  $\Omega$

$$T \vDash A \Rightarrow T \vdash_{PC_\Omega} A.$$

(2) Для любой формулы  $A$  сигнатуры  $\Omega$

$$\vDash A \Rightarrow \vdash_{PC_\Omega} A.$$

(1<sup>=</sup>) Для теории с равенством  $T$  и замкнутой формулы  $A$  сигнатуры  $\Omega$

$$T \vDash_{\text{норм}} A \Rightarrow T \vdash_{PC_\Omega^=} A.$$

(2<sup>=</sup>) Для любой формулы  $A$  сигнатуры с равенством  $\Omega$

$$\vDash_{\text{норм}} A \Rightarrow \vdash_{PC_\Omega^=} A.$$

<sup>29</sup>Пока что мы опираемся на интуитивное представление о мощности; некоторое уточнение будет дано в конце лекции.

<sup>30</sup>Это один из вариантов аксиомы выбора, о чем упомянем в конце лекции.

**Доказательство** (Не пишем индексы при  $\vdash$ .) (1) Если  $T \not\vdash A$ , то  $T \cup \{\neg A\}$  непротиворечива (по лемме 5.4; она переносится на предикатный случай). По теореме 14.1 эта теория выполнима, и значит,  $T \not\vdash A$ .

(2) По определению  $\vDash A$  означает  $\vDash \bar{\forall}A$ . А в силу (1) для  $T = \emptyset$  из  $\vDash \bar{\forall}A$  следует  $\vdash \bar{\forall}A$ . Наконец,  $\vdash \bar{\forall}A \rightarrow A$  (по аксиоме II.1 и правилу силлогизма). Тогда по МР получаем  $\vdash A$ .

(1<sup>=</sup>) Аналогично (1). Если  $T \not\vdash A$ , то  $T \cup \{\neg A\}$  непротиворечива в  $PC_{\bar{\Omega}}$ , а потому нормально выполнима по теореме 14.1. Следовательно,  $T \not\vdash_{\text{норм}} A$ .

(2<sup>=</sup>) получается из (1<sup>=</sup>) аналогично (2). ■

Далее мы рассматриваем опять только теории с равенством и нормальные модели.

**Теорема 14.3** (Гёделя — Мальцева о компактности). *Если любое конечное подмножество теории  $T$  выполнимо, то и  $T$  выполнима.*

**Доказательство** Если все конечные подмножества  $T$  выполнимы, то они непротиворечивы (следствие 12.4). Тогда  $T$  непротиворечива (лемма 10.1) и следовательно, выполнима (теорема 14.1). ■

**Теорема 14.4** (Лёвенгейма — Сколема о понижении мощности). *Если теория в сигнатуре  $\Omega$  выполнима, то она имеет модель мощности  $\leq \max(|\Omega|, \aleph_0)$ .*

**Доказательство** Если теория выполнима, то она непротиворечива (следствие 12.4). Тогда по теореме 14.1 она имеет модель нужной мощности. ■

**Теорема 14.5** (О повышении мощности). (1) *Если теория имеет конечные модели неограниченной мощности, то она имеет и бесконечную модель.*

(2) *Если теория в сигнатуре  $\Omega$  имеет бесконечную модель, то она имеет модели любой бесконечной мощности  $k \geq |\Omega|$ .*

**Доказательство** (1) Пусть  $T$  — данная теория. Согласно условию, для любого натурального  $n$  теория  $T$  имеет конечную модель мощности больше  $n$ .

Рассмотрим сигнатуру  $\Omega^+$ , которая получается из  $\Omega$  добавлением счетного множества новых констант  $\{c_1, c_2, \dots\}$ . В этой сигнатуре построим теорию

$$T^+ := T \cup \{c_i \neq c_j \mid i < j\}.$$

Докажем, что  $T^+$  выполнима. По теореме компактности достаточно доказать, что любая конечная  $T' \subset T$  выполнима. В самом деле,

$$T' \subset T \cup \{c_i \neq c_j \mid 1 \leq i < j \leq n\}$$

для некоторого  $n$ . Пусть  $M$  — модель теории  $T$  мощности  $> n$ . Превратим ее в модель  $M'$  сигнатуры  $\Omega^+$ , добавив интерпретацию констант  $c_1, \dots, c_n$  какими-нибудь различными элементами, а остальных новых констант — как угодно. Тогда  $M' \vDash T \cup \{c_i \neq c_j \mid 1 \leq i < j \leq n\}$ , и подавно  $M' \vDash T'$ .

Итак,  $T^+$  выполнима. Если  $M^+ \vDash T^+$ , то  $M^+ \vDash T$ , и она бесконечна, т.к. все ее элементы  $(c_i)_{M^+}$  различны. Рассматривая  $M^+$  в сигнатуре  $\Omega$ , получаем бесконечную модель теории  $T$ .

(2) Аналогично (1), рассмотрим сигнатуру  $\Omega^+$  с множеством новых констант  $\{c_i \mid i \in k\}$ , где  $k$  — данная бесконечная мощность. В этой сигнатуре построим теорию

$$T^+ := T \cup \{c_i \neq c_j \mid i, j \in k; i \neq j\}.$$

Любая конечная  $T' \subset T^+$  содержится в некоторой теории

$$T \cup \{c_i \neq c_j \mid i, j \in I\},$$

где  $I$  — конечное подмножество  $k$ . Последняя теория выполнима в бесконечной модели теории  $T$ , с интерпретацией констант  $c_i$  для  $i \in I$  какими-нибудь различными элементами, а остальных новых констант — произвольно. Тогда по теореме компактности  $T^+$  выполнима.

Из теории множеств следует, что  $|\Omega^+| = k$ .<sup>31</sup> По теореме 14.4  $T^+$  имеет модель  $M^+$  мощности  $\leq k$ . В этой модели интерпретации всех констант  $c_i$  различны (см. определение  $T^+$ ), поэтому ее мощность  $\geq k$ . Значит,  $|M^+| = k$ . Рассматривая  $M^+$  в сигнатуре  $\Omega$ , получим модель  $T$  мощности  $k$ . ■

<sup>31</sup>Здесь мы используем следующий факт: если  $|X| \leq |Y|$ , то  $|X \cup Y| = |Y|$ . Чтобы его доказать, нужна аксиома выбора.

Дополнительные замечания Из теоремы о повышении мощности следует такой факт:

**Признак полноты Лося — Вота** Пусть  $T$  — теория в конечной или счетной сигнатуре, не имеющая конечных моделей. Если  $k$  — бесконечная мощность и все модели  $T$  мощности  $k$  изоморфны, то  $T$  полна.

Доказательство — упражнение для читателя.

## О нестандартных моделях арифметики

Пусть  $\mathbb{N}$  — стандартная модель  $PA$  (см. лекцию 12).

**Теорема 14.6.** Существует счетная модель  $M$  такая, что  $M \equiv \mathbb{N}$ , но  $M \not\cong \mathbb{N}$ .

**Доказательство** Построим теорию в сигнатуре  $PA$  с дополнительной новой константой  $c$ .

$$T := Th(\mathbb{N}) \cup \{c \neq 0, c \neq 1, \dots, c \neq \underline{n}, \dots\},$$

где  $\underline{n}$  обозначает терм  $\underbrace{1 + (1 + (1 + \dots))}_{n \text{ раз}}$ .

В стандартной модели, очевидно, имеем  $|\underline{n}|_{\mathbb{N}} = n$ .

Как и в предыдущих теоремах, докажем выполнимость  $T$ , используя компактность. Для этого рассмотрим

$$T_n := Th(\mathbb{N}) \cup \{c \neq 0, c \neq 1, \dots, c \neq \underline{n}\}.$$

Пусть  $M_n$  — модель  $\mathbb{N}$  с интерпретацией  $c_{M_n} := n + 1$ . Тогда  $M_n \models T_n$ . Таким образом, любая  $T_n$  выполнима.

По компактности,  $T$  выполнима, а по теореме Лёвенгейма — Сколема, она имеет не более, чем счетную модель  $M^+$ .

Заметим, что  $M^+ \models Th(\mathbb{N})$  и  $\mathbb{N} \models \underline{m} \neq \underline{n}$  при  $m \neq n$ . Поэтому и  $M^+ \models \underline{m} \neq \underline{n}$  при  $m \neq n$ . Значит,  $M^+$  бесконечна, и следовательно, счетна.

Кроме того, для всех  $n$ ,  $M^+ \models c \neq \underline{n}$ , или<sup>32</sup>

$$M^+ \models c_{M^+} \neq \underline{n}.$$

Рассмотрим теперь  $M^+$  в исходной сигнатуре арифметики. Обозначим эту модель через  $M$ . Имеем:

$$(*) \quad M \models c_{M^+} \neq \underline{n}$$

для всех  $n$ , а также  $M \models Th(\mathbb{N})$ , т.е.  $M \equiv \mathbb{N}$ .

Наконец, докажем, что  $M \not\cong \mathbb{N}$ . Предположим противное, и пусть  $\alpha : M \cong \mathbb{N}$ . Из (\*) по теореме 7.4 получаем

$$\mathbb{N} \models \alpha(c_{M^+}) \neq \underline{n},$$

т.е.

$$\alpha(c_{M^+}) \neq |\underline{n}|_{\mathbb{N}}.$$

Но  $|\underline{n}|_{\mathbb{N}} = n$ , т.е.  $\alpha(c_{M^+})$  не равно никакому натуральному числу. Противоречие. ■

Замечание Можно показать, что в модели  $M$  новые элементы — бесконечно большие, т.е. больше всех натуральных чисел (упражнение).

<sup>32</sup>  $c_{M^+}$  — это элемент модели, а потому оцененный терм.

## Наивная теория множеств

Будем строить аксиоматику теории множеств в сигнатуре с двумя двуместными предикатными символами  $\in, =$ .

Рассмотрим сначала теорию  $\mathcal{N}$  (“наивную теорию множеств”) со следующими аксиомами.

(1) (аксиома объемности)

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y).$$

(2) (схема аксиом свертывания)

$$\bar{\forall} \exists y \forall x (x \in y \leftrightarrow A(x, \dots)).$$

Здесь  $A(x, \dots)$  — произвольная формула, в которой один параметр (например,  $a$ ) заменен на связанную переменную  $x$ . Отметим, что  $y$  не входит в  $A$ .

Смысл аксиомы объемности: если 2 множества состоят из одних и тех же элементов, то они равны.

Смысл аксиомы свертывания: существует множество  $y$ , состоящее из всех  $x$ , обладающих свойством  $A$ , т.е.  $y = \{x \mid A(x, \dots)\}$ .

**Предложение 14.7.** Теория  $\mathcal{N}$  противоречива.

### Доказательство

Выведем противоречие в  $\mathcal{N}$ ; это доказательство — формализация парадокса Рассела.

1.  $\forall x (x \in a \leftrightarrow x \notin x) \rightarrow (a \in a \leftrightarrow a \notin a)$  — аксиома П.1 исчисления предикатов.
2.  $(a \in a \leftrightarrow a \notin a) \rightarrow \exists y (y \in y \leftrightarrow y \notin y)$  — аксиома П.2 исчисления предикатов.
3.  $\forall x (x \in a \leftrightarrow x \notin x) \rightarrow \exists y (y \in y \leftrightarrow y \notin y)$  — по правилу силлогизма из 1, 2.
4.  $\exists y \forall x (x \in y \leftrightarrow x \notin x) \rightarrow \exists y (y \in y \leftrightarrow y \notin y)$  — 3, второе правило Бернайса.
5.  $\exists y \forall x (x \in y \leftrightarrow x \notin x)$  — аксиома свертывания для  $(a \notin a)$ .
6.  $\exists y (y \in y \leftrightarrow y \notin y)$  — 4, 5, МР.
7.  $(A \leftrightarrow \neg A) \rightarrow B \wedge \neg B$  — подстановочный пример тавтологии (с любыми  $A, B$ ). В частности,

$$(a \in a \leftrightarrow a \notin a) \rightarrow B \wedge \neg B,$$

где  $B$  — любая замкнутая формула.

8.  $\exists y (y \in y \leftrightarrow y \notin y) \rightarrow B \wedge \neg B$  — 7, второе правило Бернайса.
9.  $B \wedge \neg B$  — 6, 8, МР. ■

## Теория множеств Цермело

Самая известная аксиоматическая теория множеств — это теория Цермело – Френкеля с аксиомой выбора (ZFC). В этом курсе мы рассмотрим очень кратко более слабую теорию Цермело (Z).<sup>33</sup>

Сигнатура теории Z состоит из  $\in, =$ . Ее аксиомы — это аксиома объемности, некоторые варианты аксиомы свертывания и еще 2 особые аксиомы (бесконечности и выбора).

1. Аксиома объемности — такая же, как в  $\mathcal{N}$ :

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y).$$

Введем обозначение

$$a \subseteq b := \forall x (x \in a \leftrightarrow x \in b)$$

(“ $a$  — подмножество  $b$ ”). Вот равносильная формулировка аксиомы объемности:

$$\forall x \forall y (x \subseteq y \wedge y \subseteq x \rightarrow x = y).$$

<sup>33</sup>См. также лекции Л.Д. Беклемишева “Аксиомы теории множеств” на <http://www.mi-ras.ru/bekl/logic2013.html>

2. Аксиома пары.

$$\forall x \forall y \exists z \forall u (u \in z \leftrightarrow (u = x \vee u = y)).$$

Смысл этой аксиомы: для всех  $x, y$  можно построить множество  $z = \{x, y\}$  (неупорядоченную пару). Если  $x = y$ , то получается множество  $\{x, x\}$ , которое обозначается просто  $\{x\}$ ; это множество состоит из 1 элемента  $x$ .

Имея неупорядоченные пары, можно определить упорядоченные пары (по Куратовскому):

$$(x, y) := \{\{x\}, \{x, y\}\}.$$

Лемма (в теории с аксиомами 1,2)

$$\vdash \bar{\forall}((x, y) = (x', y') \rightarrow x = x' \wedge y = y').$$

3. Аксиома объединения.

$$\forall x \exists y \forall z (z \in y \leftrightarrow \exists u (z \in u \wedge u \in x)).$$

Т.е.  $y = \{z \mid \exists u (z \in u \wedge u \in x)\}$ . Другими словами, множество  $y$  является объединением всех множеств, являющихся элементами множества  $x$ , то есть  $y = \bigcup_{u \subseteq x} u$ . Такое  $y$  называется *объединением множества  $x$*  и обозначается  $\bigcup x$ .

Теперь можем определить:

$$x \cup y := \bigcup \{x, y\},$$

$$\{x, y, z\} := \{x, y\} \cup \{z\}$$

и т.п.

4. Аксиома степени.

$$\forall x \exists y \forall z (z \in y \leftrightarrow z \subseteq x).$$

Т.е.  $y = \{z \mid z \subseteq x\}$  — множество всех подмножеств  $x$ . Оно обычно обозначается  $\mathcal{P}(x)$ .

5. Схема аксиом выделения — ослабленный вариант свертывания.

$$\bar{\forall} \forall x \exists y \forall z (z \in y \leftrightarrow (z \in x \wedge A(z, \dots))).$$

В этой теории мы не можем строить произвольные множества вида  $\{x \mid A(x, \dots)\}$ . Однако неформально можно рассматривать такие совокупности (*классы*). Некоторые классы заведомо не являются множествами (они называются *собственными*). Например  $R := \{x \mid x \notin x\}$  — собственный класс; в нашей теории это доказывается, см. предыдущий раздел.

Аксиома выделения утверждает, что пересечение любого класса  $\{z \mid A(z, \dots)\}$  с любым множеством  $x$  — множество. Или: подкласс любого множества — множество.

**Предложение 14.8.** (1) (*существование пустого множества*)  $Z \vdash \exists y \forall x x \notin y$ .

(2) Пусть  $V := \{x \mid x = x\}$  — класс всех множеств. Тогда

$$Z \vdash (V \text{ — собственный класс}).$$

**Доказательство** (1) Существует хотя бы одно множество, формально:  $\vdash_{PC} \exists x (x = x)$ . Это получается из аксиомы равенства  $\forall x (x = x)$  и теоремы  $\forall x A \rightarrow \exists x A$ , которую легко доказать (упражнение).

Взяв это  $x$ , по аксиоме выделения построим

$$y := \{z \mid z \in x \wedge z \neq z\}.$$

Очевидно, что  $y$  пусто.

(2) Очевидно, что  $R \subseteq V$ . По аксиоме выделения, если  $V$  — множество, то и  $R$  — множество. ■

Из аксиомы объемности следует, что все пустые множества равны. Поэтому можно ввести обозначение  $\emptyset$ .

Теперь мы можем последовательно (по индукции) определить натуральные числа:

$$0 := \emptyset, 1 := \{0\}, 2 := \{0, 1\}, \dots, n + 1 := n \cup \{n\}, \dots$$

(определение фон Неймана). Т.е. получается  $n = \{0, 1, \dots, n - 1\}$ . Однако для построения множества всех натуральных чисел нужна дополнительная аксиома.

6. Аксиома бесконечности.

$$\exists x (0 \in x \wedge \forall y (y \in x \rightarrow (y \cup \{y\}) \in x)).$$

Множество  $x$  назовем *индуктивным*, если оно имеет свойства, указанные в этой аксиоме, т.е. содержит 0 и вместе с каждым  $y$  содержит ' $y + 1$ '. Аксиома утверждает, что существует индуктивное множество. Теперь можно определить множество натуральных чисел  $\omega$  как наименьшее индуктивное множество:

$$\omega := \{y \mid \forall x (x \text{ индуктивно} \rightarrow y \in x)\}.$$

Этот класс — действительно множество по аксиоме выделения, т.к.  $\omega \subseteq x_0$  для индуктивного множества  $x_0$  (какого-то, которое существует по аксиоме бесконечности).

Дальше можно развивать арифметику в  $\omega$  и в частности, превратить его в модель *PA*.

Также можно определить декартово произведение (и доказать в  $Z$ , что оно всегда существует):

$$a \times b := \{(x, y) \mid x \in a \wedge y \in b\}.$$

Затем определяем

$$f \text{ — функция} := \forall z (z \in f \rightarrow \exists x \exists y z = (x, y)).$$

После этого можно определить формулы (упражнение)

[ $f$  — биекция  $a$  на  $b$ ]

и

[ $f$  — инъекция  $a$  в  $b$ ]

и сравнение множеств по мощности:

$$a \sim b := \exists f [f \text{ — биекция } a \text{ на } b],$$

$$a \preceq b := \exists f [f \text{ — инъекция } a \text{ в } b].$$

**Предложение 14.9.** (1)  $\sim$  задает отношение эквивалентности (на классе всех множеств  $V$ ).

(2)  $\preceq$  задает рефлексивное и транзитивное отношение на  $V$ .

Доказательство — нетрудное рассуждение, которое формализуется в  $Z$ .

**Теорема 14.10** (Теорема Кантора — Бернштейна).

$$Z \vdash \forall x \forall y (x \preceq y \wedge y \preceq x \rightarrow x \sim y).$$

Доказательство опускаем.<sup>34</sup>

Теперь можем записывать  $a \sim b$  как  $|a| = |b|$  (мощность  $a$  равна мощности  $b$ ), а  $a \preceq b$  как  $|a| \leq |b|$  (мощность  $a$  меньше или равна мощности  $b$ ), не уточняя при этом само понятие “мощность”.

**Теорема 14.11** (Теорема Кантора).

$$Z \vdash \forall x |x| < |\mathcal{P}(x)|.$$

<sup>34</sup>Содержательное доказательство можно найти, например, в книге Н.К. Верещагина и А.Х. Шеня “Начала теории множеств”.



**Доказательство** Имеется инъекция  $x$  в  $\mathcal{P}(x)$ : она отображает каждый  $a \in x$  в  $\{a\}$ .  
 $x \not\approx \mathcal{P}(x)$  доказывается от противного.<sup>35</sup>

Предположим, что  $f : x \rightarrow \mathcal{P}(x)$  — биекция. Тогда для некоторого  $y \in x$

$$\{z \in x \mid z \notin f(z)\} = f(y).$$

Поэтому для всех  $z \in x$

$$z \in f(y) \leftrightarrow z \notin f(z).$$

Тогда

$$y \in f(y) \leftrightarrow y \notin f(y).$$

Противоречие. ■

7. Аксиома выбора. Запишем ее (не совсем формально) в двух вариантах.

(I) Если  $x$  — непустое множество попарно не пересекающихся непустых множеств (разбиение), то

$$\exists y \forall z (z \in x \rightarrow |z \cap y| = 1).$$

(II) Если существует отображение  $x$  на  $y$  (сюръекция), то  $|y| \leq |x|$ .

Из аксиомы выбора следует теорема о сравнении мощностей:

$$\forall x \forall y (|x| \leq |y| \vee |y| \leq |x|).$$

Кроме того, явно определяются “мощности” — это множества специального вида (кардиналы).

Другое известное следствие аксиомы выбора — лемма Цорна. Она утверждает, что если в частично упорядоченном множестве  $X$  каждая цепь (линейно упорядоченное подмножество) ограничена сверху, то  $X$  имеет максимальный элемент.

---

<sup>35</sup>Рассуждение похоже на парадокс Рассела. В истории было наоборот: теорема Кантора появилась раньше.

# Лекция 15

## Алгоритмы

Свойства алгоритмов (вычислительных устройств), неформально.

1. Алгоритмы работают со словами. *Слово* — это конечная последовательность символов (букв), взятых из некоторого конечного алфавита. Слово может быть пустым.

2. Алгоритм основан на программе. Программа — конечный набор команд, которые записываются словами.

3. Алгоритм содержит “процессор”, который обращается к программе и изменяет текущее состояние (слово).

4. Имеется начальное слово (вход) и заключительное слово (выход). Если заключительное слово не появляется, алгоритм работает бесконечно долго (заикливание).

5. Вычисление разбивается на дискретные шаги.

6. Вычисление детерминированно (т.е. каждый следующий шаг однозначно определен) и не обращается к случайным данным.

Имеется несколько точных определений алгоритма (рекурсивные функции, машины Тьюринга, абстрактные РАМ и др.). Все они оказываются эквивалентными. Философский тезис Чёрча — Тьюринга утверждает, что они полностью соответствуют интуитивному пониманию вычислимости.

## Вычислимые функции

Будем записывать положительные натуральные числа как последовательности единиц, нуль — как 0. Конечный кортеж натуральных чисел  $(n_1, \dots, n_k)$  записывается как  $n_1\#\dots\#n_k$ , где  $\#$  — специальный символ (разделитель).

Рассматриваем частичные функции  $f$  из  $\mathbb{N}^k$  в  $\mathbb{N}$ . Это записывается так:  $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ . Если функция всюду определена (тотальна), пишем  $f : \mathbb{N}^k \rightarrow \mathbb{N}$ .

Также рассматриваем функции на словах. Если  $\Delta$  — конечный алфавит,  $\Delta^*$  — множество всех слов в нем, то рассматриваем частичные функции  $f$  из  $\Delta^*$  в  $\Delta^*$ . Обозначения аналогичны:  $f : \Delta^* \dashrightarrow \Delta^*$ ,  $f : \Delta^* \rightarrow \Delta^*$ .

Область определения  $f$  обозначается  $dom f$ , область значений —  $im f$ . В частности, возможно, что  $dom f = \emptyset$  (пустая функция).

**Определение 64.** Функция  $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$  или  $f : \Delta^* \dashrightarrow \Delta^*$  называется *вычислимой*, если существует алгоритм  $M$  со следующими свойствами.

- Если  $x \in dom f$ , то  $M$  на входе  $x$  заканчивает работу и выдает  $f(x)$ . Это записывается так:  $M : x \mapsto f(x)$
- Если  $x \notin dom f$ , то  $M$  на входе  $x$  заикливается. Это записывается так:  $M : x \mapsto$

## Разрешимость и перечислимость

**Определение 65.** Множество слов  $A \subseteq \Delta^*$  называется *разрешимым*, если его характеристическая функция  $\chi_A$  вычислима.

(Функция  $\chi_A : \Delta^* \rightarrow \{0, 1\}$  принимает значение 1 на  $A$  и 0 на его дополнении.)

Аналогично определяются разрешимые подмножества  $\mathbb{N}^k$ .

**Предложение 15.1.** (1) Если  $A$  разрешимо, то его дополнение  $(-A)$  (до  $\Delta^*$  или  $\mathbb{N}^k$ ) разрешимо.

(2) Если  $A$  и  $B$  разрешимы, то  $A \cap B$ ,  $A \cup B$  разрешимы.

**Следствие 15.2.** Конечные множества разрешимы.

**Определение 66.** Множество слов  $A \subseteq \Delta^*$  (или  $A \subseteq \mathbb{N}^k$ ) называется *полуразрешимым*, если его полухарактеристическая функция  $\chi_A^-$  вычислима.

(Частичная функция  $\chi_A^- : \Delta^* \dashrightarrow \{1\}$  принимает значение 1 на  $A$  и не определена на его дополнении.)

**Предложение 15.3.** Если  $A$  и  $B$  полуразрешимы, то  $A \cap B$ ,  $A \cup B$  полуразрешимы.

**Теорема 15.4** (Теорема Поста). Множество слов  $A \subseteq \Delta^*$  разрешимо  $\Leftrightarrow A$  и  $-A$  полуразрешимы.

**Определение 67.** Множество  $A \subseteq \Delta^*$  (или  $A \subseteq \mathbb{N}^k$ ) называется *перечислимым*, если оно пусто или является множеством значений некоторой вычислимой последовательности, т.е. тотальной функции  $\mathbb{N} \rightarrow \Delta^*$ .

**Теорема 15.5.** Существуют вычислимые биекции  $\mathbb{N} \rightarrow \mathbb{N}^k$  и  $\mathbb{N} \rightarrow \Delta^*$  (для конечного  $\Delta$ ), причем обратные биекции тоже вычислимы.

**Теорема 15.6.** Множество  $A \subseteq \Delta^*$  (или  $A \subseteq \mathbb{N}^k$ ) перечислимо, если только если оно полуразрешимо.

**Доказательство** Рассмотрим сначала случай  $A \subseteq \mathbb{N}$ .

(Только если).  $\emptyset$  разрешимо.

Пусть  $A = \text{im } f$  для вычислимой  $f : \mathbb{N} \rightarrow \mathbb{N}$ . Тогда  $\chi_A^-$  вычислима по следующему алгоритму.

0. Пусть на входе дано  $n$ .

1. Полагаем  $i := 0$ .

2. В цикле по  $i$  проверяем, верно ли  $f(i) = n$ . Если да, выдаем 1 и заканчиваем работу. Если нет, полагаем  $i := i + 1$  и продолжаем цикл.

(Если).  $\emptyset$  перечислимо.

Пусть  $A \neq \emptyset$ . Выберем  $a_0 \in A$ .

Пусть  $\gamma : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$  — вычислимая биекция (теорема 15.5). Пусть  $\gamma(n) = (\alpha(n), \beta(n))$ . Тогда  $\alpha$  и  $\beta$  тоже вычислимы.

Построим последовательность  $f$ , перечисляющую  $A$  следующим образом. Для нахождения  $f(n)$  делаем  $\beta(n)$  шагов в вычислении  $\chi_A^-(\alpha(n))$  (или меньше, если вычисление заканчивается раньше). Если за это время вычисление закончилось, полагаем  $f(n) := \alpha(n)$ . Иначе полагаем  $f(n) := a_0$ .

Тогда  $\text{im } f = A$ . Действительно, включение  $\subseteq$  очевидно (почему?).

Обратно, пусть  $a \in A$ . Тогда  $\chi_A^-(a)$  вычислится через сколько-то ( $k$ ) шагов. Т.к.  $\gamma$  — биекция, имеем  $\gamma(n) = (a, k)$  для некоторого  $n$ . Т.е.  $\alpha(n) = a$ ,  $\beta(n) = k$ . По построению тогда  $f(n) = a$ .

Общий случай сводится к случаю  $A \subseteq \mathbb{N}$  с помощью теоремы 15.5. ■

**Теорема 15.7.** Пусть  $h : \Delta^* \rightarrow \Delta^*$  — вычислимая тотальная функция.

(1) Если  $A \subseteq \Delta^*$  разрешимо, то  $h^{-1}(A)$  разрешимо.

(2) Если  $A \subseteq \Delta^*$  перечислимо, то  $h[A]$  (образ  $A$ ) и  $h^{-1}(A)$  перечислимы.

**Доказательство**

(1)  $\chi_{h^{-1}(A)} = \chi_A \cdot h$ , а композиция вычислимых функций вычислима.

(2) Для прообраза:  $\chi_{h^{-1}(A)}^- = \chi_A^- \cdot h$ . И используем предыдущую теорему.

Для образа. Если  $A = \emptyset$ , все очевидно. Если  $A = \text{im } f$  для вычислимой  $f$ , то  $h[A] = \text{im } (h \cdot f)$ . ■

## Универсальная вычислимая функция. Неразрешимость

Ключевой результат теории алгоритмов следующий:

**Теорема 15.8** (Об универсальной вычислимой функции). Существует вычислимая функция  $F : \mathbb{N}^2 \rightarrow \mathbb{N}$  такая, что для любой вычислимой

$f : \mathbb{N} \rightarrow \mathbb{N}$  существует  $t$  такое, что

$$\text{для всех } n \quad F(t, n) \simeq f(n).$$

Здесь  $\simeq$  означает условное равенство, т.е. обе части определены одновременно и равны, когда определены.

Идея доказательства: нумеруем программы, работающие с натуральными числами.  $F$  вычисляется компьютером, который по номеру программы восстанавливает саму программу и запускает ее на различных входах. Т.е.  $F(m, n)$  — результат работы программы с номером  $m$  на входе  $n$  (если этот результат существует).

Обозначим через  $\varphi_m$  вычислимую функцию с номером  $m$ , т.е.

$$\varphi_m(n) \simeq F(m, n).$$

Тогда всякая вычислимая  $f : \mathbb{N} \rightarrow \mathbb{N}$  совпадает с  $\varphi_m$ , где  $m$  — номер программы, вычисляющей  $f$ .

**Теорема 15.9.** *Существует перечислимое неразрешимое подмножество в  $\mathbb{N}$ .*

**Доказательство** Пусть

$$d(x) \simeq F(x, x) \simeq \varphi_x(x).$$

Рассмотрим

$$K := \text{dom } d.$$

Ясно, что  $K$  полуразрешимо, т.е. перечислимо. Докажем, что  $(-K)$  не перечислимо.

Допустим противное. Тогда  $-K = \text{dom } \varphi_n$ , где  $\varphi_n = \chi_{-K}$ . Тогда для любого  $x$

$$x \notin K \Leftrightarrow x \in \text{dom } \varphi_n.$$

В частности,

$$n \notin K \Leftrightarrow n \in \text{dom } \varphi_n.$$

Но по определению  $K$

$$n \in K \Leftrightarrow n \in \text{dom } \varphi_n.$$

Таким образом,

$$n \in K \Leftrightarrow n \notin K.$$

Противоречие, аналогичное парадоксу Рассела и доказательству теоремы Кантора. ■

## О разрешимости теорий первого порядка

Рассмотрим теории в конечной сигнатуре  $\Omega$ .

**Лемма 15.10.** *Множества  $Fm_\Omega$ ,  $CFm_\Omega$  разрешимы.*

Для теории  $T \subseteq CFm_\Omega$  обозначим через  $[T]$  множество всех ее замкнутых теорем, т.е.  $[T] = \{A \in CFm_\Omega \mid T \vdash A\}$ .

**Теорема 15.11.** *Если  $T$  — разрешимое множество, то множество  $[T]$  перечислимо.*

**Доказательство** Будем записывать доказательства в  $T$  в виде  $A_1 \# \dots \# A_n$ . Пусть  $\text{Док}(T)$  — множество всех этих доказательств.

Заметим, что  $\text{Док}(T)$  разрешимо: по любой последовательности формул можно узнать, является ли она правильно построенным доказательством, т.к. элементы  $T$  и аксиомы исчисления предикатов распознаются алгоритмически, а применения правил вывода — также.

Имеем:  $[T] = h[\text{Док}(T)] \cap CFm_\Omega$ , где  $h$  — вычислимая функция, выбирающая последний член кортежа. По теореме 15.7 множество  $h[\text{Док}(T)]$  перечислимо. По лемме 15.10  $CFm_\Omega$  разрешимо и следовательно, перечислимо. Пересечение сохраняет перечислимость по предложению 15.3. ■

**Теорема 15.12.** *Если  $T$  — разрешимое множество и  $T$  полна, то множество  $[T]$  разрешимо.*

**Доказательство** По теореме 15.11 это множество перечислимо. Поэтому достаточно доказать перечислимость его дополнения и применить теорему Поста.

Имеем:

$$-[T] = -CFm_\Omega \cup (CFm_\Omega \setminus [T]).$$

Первое множество перечислимо, ввиду разрешимости  $CFm_\Omega$ . Поскольку  $T$  полна,

$$CFm_\Omega \setminus [T] = \{A \in CFm_\Omega \mid T \vdash \neg A\}.$$

Тогда это множество равно  $f^{-1}([T])$ , где  $f$  — вычислимая функция, которая добавляет в начале слова знак  $\neg$ . По теореме 15.7 оно перечислимо. Объединение сохраняет перечислимость. ■

## Теорема Гёделя о неполноте

Напомним, что определимые (в арифметической сигнатуре  $\{+, \times, 0, 1, =\}$ ) подмножества стандартной модели  $\mathbb{N}$  называются *арифметическими*.

**Теорема 15.13** (Гёделя об определимости). *Всякое перечислимое подмножество  $\mathbb{N}$  является арифметическим.*

**Теорема 15.14** (Первая теорема Гёделя о неполноте). *Пусть  $T$  — теория в сигнатуре  $PA$  с разрешимым множеством аксиом, причём  $\mathbb{N} \models T$ . Тогда  $T$  неполна. В частности,  $PA$  неполна.*

**Доказательство** Допустим, что  $T$  полна. По теореме 15.12  $[T]$  разрешимо. Поскольку  $\mathbb{N} \models T$ , получаем  $[T] = Th(\mathbb{N})$  и значит,  $Th(\mathbb{N})$  разрешима.

Рассмотрим теперь множество  $K$ , построенное в теореме 15.9. По теореме 15.13 существует формула  $A$  (с одной свободной переменной) такая, что для всех  $n$

$$n \in K \Leftrightarrow \mathbb{N} \models A(n).$$

Здесь  $A(n)$  — формула, оцененная в  $\mathbb{N}$ . Заметим, что

$$\mathbb{N} \models A(n) \Leftrightarrow \mathbb{N} \models A(\underline{n}),$$

где  $\underline{n}$  — терм (сумма единиц); это следует из леммы 12.1. Таким образом,

$$n \in K \Leftrightarrow A(\underline{n}) \in Th(\mathbb{N}).$$

Поэтому

$$K = h^{-1}(Th(\mathbb{N})),$$

где  $h$  — вычислимая функция, переводящая число  $n$  в формулу  $A(\underline{n})$ . По теореме 15.7  $K$  разрешимо. Противоречие.

Итак,  $T$  неполна. ■

## Список литературы

- [1] Н.К. Верещагин, А.Х. Шень. *Лекции по математической логике и теории алгоритмов. Часть 2: Языки и исчисления*, 2012, Изд. МЦНМО, <http://www.mccme.ru/>
- [2] В.А. Успенский, Н.К. Верещагин, В.Е. Плиско. *Вводный курс математической логики*. Издательство МГУ. М., 1991 и 1997. Физматлит, 2002.
- [3] Э. Мендельсон. *Введение в математическую логику*. М., 1984.
- [4] А.Н. Колмогоров, А.Г. Драгалин. *Математическая логика*. Серия «Классический университетский учебник», 2005.
- [5] В. Н. Крупский, В. Е. Плиско. *Математическая логика и теория алгоритмов*, Академия, 2013.
- [6] С.К. Клини. *Математическая логика*. М., Мир, 1973.
- [7] W. Rautenberg. *A concise introduction to mathematical logic*. Springer, 2006.