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* $Var = \{P_1, P_2, \ldots\}$. Множество *пропозициональных формул*, обозначаемое Fm, строится из этих переменных, логических связок $\wedge$, $\vee$, $\to$, $\neg$ и скобок по индукции, как наименьше 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 $(A \to B) \in Fm$.
(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.[1]

Правила построения формул можно записать схематически так:

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

Эти правила задают множество Fm с помощью «формальной грамматики». бычно 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 $\to$. И конечно, $\neg$ сильнее всех, но это и так видно из записи.

Еще одно сокращение:

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

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 $C = (A \to B)$,
(V) Существует единственная формула A, такая что $C = \neg A$.

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

[1] Этот алфавит бесконечен за счет множества Var. Можно обойтись и конечным алфавитом, если каждую переменную P_n изображать в виде слова $P1 \ldots 1$ (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, расположеннная между какими-то двумя позициями, т.е. слово вида $a_i \dots a_j$, где $i < j$.[2] *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. [3]

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

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

- Если $B = \neg C$, то

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

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 $f : Var \longrightarrow \mathbb{B}$, где $\mathbb{B} = \{\text{и,л}\} = \{1, 0\}$.

Лемма 2.1. *(о продолжении оценок на формулы). Для любой оценки $f : Var \longrightarrow \mathbb{B}$ существует единственное отображение $\overline{f} : Fm \longrightarrow \mathbb{B}$, такое что для всех $A, B \in Fm$*

(1) $\overline{f}(A) = f(A)$, *если* $A \in Var$,
(2) $\overline{f}(A \wedge B) = 1 \Leftrightarrow \overline{f}(A) = \overline{f}(B) = 1$,
(3) $\overline{f}(A \vee B) = 1 \Leftrightarrow (\overline{f}(A) = 1$ *или* $\overline{f}(B) = 1)$,
(4) $\overline{f}(A \to B) = 1 \Leftrightarrow (\overline{f}(A) = 0$ *или* $\overline{f}(B) = 1)$,
(5) $\overline{f}(\neg A) = 1 \Leftrightarrow \overline{f}(A) = 0$.

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

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

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

Пусть $\overline{f}$ 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 $\overline{f}$ 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 $\overline{f}(A), \overline{f}(B)$ однозначно определены по предположению индукции. Тогда $\overline{f}(C) = \min(\overline{f}(A), \overline{f}(B))$ тоже задается однозначно.

Аналогично рассуждаем для других случаев. ∎

$\overline{f}(C)$ 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) $\overline{f}(A \wedge B) = \overline{f}(A) \mathbin{\textcircled{\wedge}} \overline{f}(B)$,
(3) $\overline{f}(A \vee B) = \overline{f}(A) \mathbin{\textcircled{\vee}} \overline{f}(B)$,
(4) $\overline{f}(A \to B) = \overline{f}(A) \mathbin{\textcircled{\to}} \overline{f}(B)$,
(5) $\overline{f}(\neg A) = \textcircled{\neg}\, \overline{f}(A)$,

[2] 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 $k = 1, \dots, j - i$.

[3] Знаки $\preceq$, $\Leftrightarrow$, которые встречаются в этом определении, относятся к метаязыку; они сокращают русский текст.

где $\textcircled{\vee}$, $\textcircled{\wedge}$, $\textcircled{\rightarrow}$, $\textcircled{-}$ 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:

$$f(A) = f(B) \textcircled{\vee} f(C) = g(B) \textcircled{\vee} g(C) = g(A)$$

(по определению значения формулы и предположению индукции). ■

Булевы функции

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

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

Каждой формуле $A(P_1, \ldots, P_n)$ отвечает *n-местная булева функция* φ_A^n (или короче, φ_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 φ_A^n.

Определение 6. Для каждого двоичного вектора $\overrightarrow{x} = (x_1, \ldots, x_n) \in \mathbb{B}^n$ построим оценку $f_{\overrightarrow{x}} : Var \longrightarrow \mathbb{B}$, такую что $f_{\overrightarrow{x}}(P_i) = x_i$ при $i \leq n$ и (например[4]) $f_{\overrightarrow{x}}(P_i) = 0$ при $i > n$.

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

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 $\sim$.[5]

Из леммы 2.2 сразу получаем, что формулы от одних и тех же переменных равносильны, если и только если (тождественно) совпадают их булевы функции:[6]

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

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

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

Лемма 2.3.

(1) $A \sim B \Leftrightarrow ((A \to B) \wedge (B \to A))$ *— тавтология.*

(2) A*— тавтология* $\Leftrightarrow A \sim \top$.

Доказательство (1) Заметим, что

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

Действительно,

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

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. ■

[4]На самом деле неважно, каковы значения при $i > n$ (лемма 2.2).

[5]Это тоже символ метязыка.

[6]$\equiv$ обозначает совпадение функций при всех значениях аргумента. Часто пишут ‘=’ вместо $\equiv$.

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) $A \wedge (B \vee C) \sim (A \wedge C) \vee (B \wedge C),\ A \vee (B \wedge C) \sim (A \vee C) \wedge (B \vee C)$ *(дистрибутивность).*
(5) $A \vee (A \wedge B) \sim A,\ A \wedge (A \vee B) \sim A$ *(поглощение).*
(6) $A \wedge \neg A \sim \bot,\ A \vee \bot \sim A,$
$A \vee \neg A \sim \top,\ A \wedge \top \sim A.$
(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) $A \to B \sim \neg A \vee B.$

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

$$\varphi^n_{A_{\overrightarrow{x}}}(\overrightarrow{y}) = 1 \Leftrightarrow \overrightarrow{x} = \overrightarrow{y}.$$

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

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 $\overrightarrow{x} = (x_1, \dots, x_n)$ можно взять

$$A_{\overrightarrow{x}} = P_1^{x_1} \wedge \ldots \wedge P_n^{x_n}.$$

В самом деле, для любой оценки f

$$f(A_{\overrightarrow{x}}) = 1 \Leftrightarrow (\text{так как } A_{\overrightarrow{x}} \text{ — конъюнкция})\ \forall i < n\ f(P_i^{x_i}) = 1$$

$$\Leftrightarrow (\text{по замечанию выше})\ \forall i < n\ f(P_i) = x_i.$$

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

Теорема 2.6. *[Теорема о функциональной полноте] Любая булева функция отвечает формуле логики высказываний, точнее:*
для любой функции $\alpha : \mathbb{B}^n \longrightarrow \mathbb{B}$ *существует формула* $A(P_1, \dots, P_n)$*, такая что* $\varphi_A \equiv \alpha$.

Доказательство Сначала рассмотрим случай, когда α не всюду равна 0. Тогда положим

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

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

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

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

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

По лемме 2.5,

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

Получаем:

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

Таким образом, функции φ_A и α 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 $\bot$. Она ложна при всех оценках, а потому $\varphi_\bot \equiv \alpha$. ■

Лекция 3

Нормальные формы

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

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

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

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

Определение 10. *Совершенная дизъюнктивная нормальная форма* (СДНФ) от переменных $P_1, \ldots, P_n$ — 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 $\bot$.

Теорема 3.1.

(1) Каждая формула, построенная из переменных $P_1, \ldots, P_n$, равносильна некоторой СДНФ от этих переменных.

(2) Каждая формула равносильна единственной СДНФ (с точностью до перестановок и расстановки скобок в дизъюнкциях):
если $\bigvee\limits_{\overrightarrow{x} \in I} A_{\overrightarrow{x}} \sim \bigvee\limits_{\overrightarrow{x} \in J} A_{\overrightarrow{x}}$, то $I = J$.

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

(2) Докажем единственность (это почти уже сделано). Заметим, что запись $\bigvee\limits_{\overrightarrow{x} \in I} A_{\overrightarrow{x}}$ 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 $\overrightarrow{x}$. Порядок на $\mathbb{B}^n$ можно задать, как в двоичной системе счисления: (0,...,0,0) — наименьший, (0,...,0,1) — следующий, и т.д.

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

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

Действительно,

$$\varphi_{A_I}(\overrightarrow{y}) = 1 \Leftrightarrow f_{\overrightarrow{y}}(A_I) = 1 \Leftrightarrow \exists \overrightarrow{x} \in I \ f_{\overrightarrow{y}}(A_{\overrightarrow{x}}) = 1 \text{ (т.к. } A_I \text{ — дизъюнкция)}$$

$$\Leftrightarrow \exists \overrightarrow{x} \in I \ \overrightarrow{y} = \overrightarrow{x} \text{ (по лемме 2.5)} \Leftrightarrow y \in I.$$

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 $P_1^{x_1} \vee \ldots \vee P_n^{x_n}$. И соответственно определяем *совершенную конъюнктивную нормальную форму* (СКНФ) (от $P_1, \ldots P_n$) как конъюнкцию элементарных дизъюнкций (причем пустая конъюнкция считается равной $\top$).

Справедлива следующая

Теорема (об СКНФ)**.**

(1) Каждая формула, построенная из переменных $P_1, \ldots, P_n$, 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:

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

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

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 $(\mathcal{B}, \sqcup, \sqcap, -, \mathbf{0}, \mathbf{1})$[7], где

- $\sqcup, \sqcap$ — 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:

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

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

[7] 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 $\mathcal{B}$.

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

$$2 = (\{0,1\},\ \circledvee,\ \circledwedge,\ \ominus,\ 0,\ 1),$$

где $x \circledvee y = \max(x,y)$, $x \circledwedge y = \min(x,y)$, $\ominus\, x = 1 - x$ (см. лекцию 1). То, что *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 $\varnothing, E$ в качестве $\mathbf{0}, \mathbf{1}$.

Предложение 3.2. *Пусть E — произвольное множество. Тогда $(\mathcal{P}(E), \cup, \cap, -, \varnothing, E)$ (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 $a \in E$

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

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

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

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 $\varphi : \mathcal{A} \longrightarrow \mathcal{B}$ 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 $x, y \in \mathcal{A}$

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

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

Как легко видеть, изоморфность — отношение эквивалентности между алгебрами[8].

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

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 $a = b$.

[8]В более общем контексте понятие изоморфизма будет обсуждаться позже.

- $\mathbf{1}$ — наибольший: $a = a \sqcap \mathbf{1}$ — по определению 12.
- $\mathbf{0}$ — наименьший, т.е. $\mathbf{0} = \mathbf{0} \sqcap a$. Это получается так:

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

■

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 $f : Var \longrightarrow \mathcal{B}$.

По аналогии с леммой 2.1, получаем:

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

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

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

Как и в случае оценок в *2*, пишем $f(A)$ вместо $\overline{f}(A)$; $f(A)$ 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 *2* — это обычные равносильность ($\sim$) и тавтологичность ($\vDash$); они определялись в лекции 2.

Аналогично лемме 2.3, получаем:

Лемма 3.6.

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

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

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

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

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

где $a \ominus b := -a \sqcup b$.

Утверждение ($\Rightarrow$) очевидно: $a \ominus a = -a \sqcup a = \mathbf{1}$, $\mathbf{1} \sqcap \mathbf{1} = \mathbf{1}$ 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

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

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 алгебреназываются *атомами*; их может быть несколько, а может не быть вообще.

Справедлива следующая теорема Стоуна (в курсе не доказывается):

Теорема 3.7. *

(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 $\varnothing$ 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 $\mathcal{L} = Fm/\sim$. Пусть $\tilde{A}$ обозначает класс формулы A. Тогда определим

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

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*

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

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

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

для каждого i. Из свойств булевых алгебр получаем:

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

и аналогично для $\sqcap$.

Кроме того,
$-\mathbf{0} = \mathbf{1}$, т.к. $\mathbf{1} = \mathbf{0} \sqcup -\mathbf{0} = -\mathbf{0}$,
$-\mathbf{1} = \mathbf{0}$, 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 $\mathit{2}$. Обозначим этот изоморфизм через $\approx$, т.е. пусть

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

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

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

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

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

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).

<u>Схемы аксиом</u>

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

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

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

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

Эта запись означает, что если доказаны формулы A и $A \to B$, 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
$A_1, \ldots, A_n = A$, что для всех k $(1 \leq k \leq n)$ A_k — аксиома или существуют $i, j < k$, для которых $A_j = A_i \to A_k$.

Действительно, из A_i и $A_i \to A_k$ 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 $\vdash A \vee B \to B \vee A$.
Приведем доказательство (с комментариями). Для удобства обозначим формулу $B \vee A$ через C.

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

Формула 5 и есть нужная теорема.

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

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

Расширим теперь определение вывода 16.

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

Т.е. это последовательность формул $A_1, \ldots, A_n$, где для всех k
A_k — аксиома или $A_k \in \Gamma$ или существуют $i, j < k$, для которых $A_j = A_i \to A_k$.

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

Если рассматриваются выводы из Γ, то формулы из Γ 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 $\Gamma = \varnothing$, то вывод из Γ — 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 Δ 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 Γ на его конечное подмножество Γ_1, т.е. мы имеем

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

Пусть $\Gamma_1 = \{B_1, \dots, B_n\}$. Пусть Π_i —- вывод B_i из Δ. Возьмем вывод A из Γ_1; в нем встречаются какие-то гипотезы B_i:

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

Заменим в этом выводе каждую B_i на ее вывод Π_i:

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

Получится вывод A из из Δ. Действительно, все формулы из исходного вывода, кроме гипотез B_i, — аксиомы CL или получаются из предыдущих по MP. А в каждом вставном выводе Π_i все формулы — аксиомы CL или входят в Δ или получаются по MP 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 $\dfrac{A_1, \dots, A_n}{B}$ — *производное правило* CL.

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

Лемма 4.3. *Всякое производное правило CL допустимо.*[9]

Доказательство Пусть $\Gamma = \{A_1, \dots, A_n\} \vdash B$. Тогда, если $\varnothing \vdash \Gamma$, то $\varnothing \vdash B$ — 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

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

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

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

Теорема о дедукции для исчисления высказываний

Теорема 4.4. *(теорема*[10] *о дедукции)*

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

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

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

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

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

1. B (аксиома)
2. $B \to (A \to B)$ (аксиома 1)
3. $A \to B$ (1,2, MP)

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

[9] Обратное утверждение (при некотором уточнении понятия “правило вывода ”) тоже верно, но в этом курсе мы его не доказываем.
[10] Конечно, это — не теорема нашего формального исчисления, а утверждение о его свойствах (“метатеорема”).

1. B (гипотеза)
2. $B \to (A \to B)$ (аксиома 1)
3. $A \to B$ (1,2, MP)

(3) Если $B = A$, то $A \to B = A \to A$. Но $\vdash A \to A$ (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 Γ, A короче, чем вывод B, то $\Gamma \vdash A \to C$.

Докажем, что $\Gamma \vdash A \to B$.

Рассмотрим вывод из Γ, 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 $\Gamma \vdash A \to B$ по (1)–(3).

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

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

С другой стороны,

(**) $A \to C,\ A \to (C \to B) \vdash A \to B$:

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

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

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

$$A \vdash B \ \Leftrightarrow \vdash A \to B.$$

Пример 4 Допустимо *правило силлогизма*

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

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

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

По теореме дедукции это равносильно

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

Последнее утверждение очевидно: надо два раза применить MP.

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 MP из формул B, $B \to A$ с более короткими выводами.

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

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

$$\mathbf{1} = f(B \to A) = f(B) \ominus\!\!\!\to f(A) = \mathbf{1} \ominus\!\!\!\to a.$$

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:

Теорема 5.5. *Если $\vdash_{CL} A$, то $\mathcal{B} \vDash A$ для любой булевой алгебры $\mathcal{B}$.*

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) если $x \leq z$ *и* $y \leq z$, *то* $x \sqcup y \leq z$;

(3) если $x \leq x'$ *и* $y \leq y'$, *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

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

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

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

По лемме 3.4 это равносильно

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

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

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

По лемме 3.4 это равносильно

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

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

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

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

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

Заметим, что
$$a \ominus \mathbf{0} = -a \sqcup \mathbf{0} = -a.$$
Значит, надо проверить, что
$$(a \ominus (b \ominus \mathbf{0})) \ominus ((a \ominus b) \ominus (a \ominus \mathbf{0})) = \mathbf{1}.$$
Но это мы установили при проверке аксиомы 2: надо взять $c = \mathbf{0}$.

Аксиома 8 Надо доказать
$$(a \ominus c) \ominus ((b \ominus c) \ominus ((a \sqcup b) \ominus c)) = \mathbf{1},$$
или
$$a \ominus c \leq (b \ominus c) \ominus ((a \sqcup b) \ominus c),$$
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
$$(\sharp) \qquad -a \leq (b \sqcap -c) \sqcup (-a \sqcap -b) \sqcup c.$$
Для доказательства ($\sharp$) используем неравенства:
$$(**) \qquad -a \leq (-a \sqcap -b) \sqcup b,$$
$$(***) \qquad b \leq (b \sqcap -c) \sqcup c.$$
Каждое из них — это вариант неравенства (*) (см. выше). Теперь по лемме 5.1 получаем ($\sharp$):
$$-a \leq (-a \sqcap -b) \sqcup b \leq (-a \sqcap -b) \sqcup (b \sqcap -c) \sqcup c.$$
■

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:
$$2 \vDash A \ \Rightarrow \vdash_{CL} A.$$

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

Лемма 5.4.

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

(2) Если Γ *противоречиво, то* $\Gamma \vdash B$ *для всех формул* B.

Доказательство (леммы).
(1) ($\Leftarrow$) очевидно.
Докажем ($\Rightarrow$). Пусть $\Gamma, B \vdash A, \neg A$. Тогда по теореме дедукции
$$\Gamma \vdash B \to A,\ B \to \neg A.$$
С другой стороны,
$$B \to A,\ B \to \neg A \vdash \neg B.$$
Это получается из аксиомы 9, если заменить в ней A на B и наоборот и 2 раза применить MP. Тогда по транзитивности
$$\Gamma \vdash \neg B.$$

(2) Если Γ противоречиво, то и подавно $\Gamma \cup \{\neg B\}$ противоречиво. По (1) тогда $\Gamma \vdash \neg\neg B$. Добавив к этому выводу аксиому 10 $\neg\neg B \to B$ и применив MP, получаем $\Gamma \vdash B$. ■

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

Пусть Φ — 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 Φ (т.е. Γ', такое что $\Gamma \subset \Gamma' \subseteq \Phi$) противоречиво.

Очевидно, что Φ 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 MP.

Лемма 5.5. *Любое непротиворечивое подмножество Φ содержится в каком-то максимальном.*

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

Лемма 5.6. *Пусть Γ — 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) $(B \wedge C) \in \Gamma \Leftrightarrow (B \in \Gamma$ и $C \in \Gamma)$ (для $(B \wedge C) \in \Phi$);

(3) $(B \vee C) \in \Gamma \Leftrightarrow (B \in \Gamma$ или $C \in \Gamma)$ (для $(B \vee C) \in \Phi$);

(4) $(B \to C) \in \Gamma \Leftrightarrow (B \notin \Gamma$ или $C \in \Gamma)$ (для $(B \to C) \in \Phi$).

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. Γ максимально). Тогда по лемме 5.4(1) $\Gamma \vdash \neg B$, и следовательно, $\Gamma \nvdash B$ — иначе бы Γ было противоречиво.

(1) ($\Rightarrow$) очевидно, т.к. Γ 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 Φ, поэтому и B, C — подформулы и лежат в Φ.

($\Rightarrow$) Пусть $(B \wedge C) \in \Gamma$. Тогда $\Gamma \vdash B, C$ (по аксиомам 3,4 и MP). 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 MP), 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, $\bot$ ($= P_1 \wedge \neg P_1$ — см. лекцию 2). Поэтому $\neg B, B \vdash \bot$, откуда $\neg B \vdash B \to \bot$ — по теореме дедукции. Аналогично $\neg C \vdash C \to \bot$. В результате имеем:

$$\Gamma \vdash B \vee C, B \to \bot, C \to \bot.$$

Однако

$$B \vee C, B \to \bot, C \to \bot \vdash \bot$$

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

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

($\Rightarrow$) Если $(B \to C), B \in \Gamma$, то $\Gamma \vdash C$ по MP, 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 $\neg B \vdash B \to C$. Значит, $\Gamma \vdash B \to C$, и $(B \to C) \in \Gamma$ — по (0).

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

[11] 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 Φ, содержащих Γ, упорядоченное по включению.

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

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

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,

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

  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, $2 \not\models A$. ∎

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) $2 \models A$.

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,
- $Pred_\Omega \neq \varnothing$,
- $\nu : Pred_\Omega \cup Fun_\Omega \longrightarrow \mathbb{N}_+ = \{1, 2, \ldots\}$.

Множества $Pred_\Omega, Const_\Omega, Fun_\Omega$ называются соответственно множеством *предикатных символов*, множеством *(предметных) констант* и множеством *функциональных символов* сигнатуры Ω. ν 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 Ω состоит из

- всех предикатных символов, констант и функциональных символов Ω;
- счетного множества свободных (предметных) переменных $FVar = \{a_0, a_1, \ldots\}$;
- счетного множества связанных (предметных) переменных $BVar = \{v_0, v_1, \ldots\}$;
- 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 $a, b, c, \ldots$ вместо символов a_i, а для связанных — $x, y, z, \ldots$ вместо v_i.

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

Определение 20. *Термы сигнатуры* Ω строятся индуктивно:

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

Таким образом, мы индукцией по длине слова, определяем, какие слова считаются термами.

Это определение можно сформулировать иначе:

Множество термов сигнатуры Ω — это наименьшее множество слов X, такое что

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

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

Определение 22. *Формулы сигнатуры* Ω 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 Ω):

Tm_Ω — множество всех термов,

Fm_Ω — множество всех формул,

AFm_Ω — множество всех атомарных формул.

<u>Замечание</u> 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* Ω

(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 $C = (A \to B)$,*
- *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,

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

Языки первого порядка: семантика

Определение 23. *Модель сигнатуры* Ω, или Ω*-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 $\mathcal{I}(P) : \underline{M}^n \longrightarrow \{\text{и,л}\}$[12] (т.е. $\mathcal{I}(P)$ — *n-местный предикат на* $\underline{M}$),
- Если $f^n \in Fun_\Omega$, то $\mathcal{I}(f) : \underline{M}^n \longrightarrow \underline{M}$ (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 Ω множество всех замкнутых термов обозначается CTm_Ω,

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

- $|c|_M := c_M$ для $c \in Const_\Omega$,

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

- $|f(t_1,\dots,t_n)|_M := f_M(|t_1|_M,\dots,|t_n|_M)$ 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 Ω 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). А

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 $\mathbb{N}$.

Лемма 6.2. *Пусть M — модель сигнатуры Ω. Значения замкнутых термов в M определены корректно. Это означает, что существует единственное отображение $t \mapsto |t|_M$ из CTm_Ω 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 Ω множество всех замкнутых формул обозначается CFm_Ω.

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

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

Определение 29. Теорией первого порядка в сигнатуре Ω 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 $M \vDash T$, 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:

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

Всякая модель M сигнатуры равенства — это непустое множество с произвольным 2-местным предикатом $=_M$. Если же $M \vDash Eq$, 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: $T \vDash A$), если A истинна во всех моделях T.

Очевидны следующие свойства:

1. Если T не выполнима, то $T \vDash A$ для всех A.
2. $T \nvDash A \Leftrightarrow T \cup \{\neg A\}$ 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 $T \vDash A$, либо $T \vDash \neg A$, 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 $Th(M) \vDash \neg A$.

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

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

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

- $Eq \nvDash \neg A_{=1}$ — т.к. теория $Eq \cup \{A_{=1}\}$ выполнима: у нее есть 1-элементная нормальная модель.
- $Eq \nvDash A_{=1}$ — 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 $T' \not\sim T$. Тогда найдется формула $A \in ([T'] \setminus [T])$. Поскольку $T \nvDash A$ и T полна, получаем $T \vDash \neg A$. Но тогда и $T' \vDash \neg A$. С другой стороны, $T' \vDash A$. Значит, T' невыполнима.

(2) $\Rightarrow$ (3). Предположим (2). Если $M \vDash T$, 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 $M' \vDash T$ следует $M' \vDash Th(M)$. Значит, всякая замкнутая формула, истинная в M, будет истинной в M'. И наоборот, если $M \not\vDash A$, т.е. $M \vDash \neg A$, то $M' \vDash \neg A$, т.е. $M' \not\vDash A$. Итак, $M \equiv M'$.

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

Определение истинности в модели

Пусть M — модель сигнатуры Ω; предполагаем, что ее носитель $\underline{M}$ состоит из совершенно новых элементов, которые не являются словами, содержащими символы из Ω. Через $\Omega \cup M$ обозначим *расширенную сигнатуру модели* M, которая получается из Ω 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 Ω. [13]

Определение 35. Пусть M — модель сигнатуры Ω. *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 $m \in \underline{M}$,
- $|f(t_1, \ldots, t_n)|_M := f_M(|t_1|_M, \ldots, |t_n|_M)$ для $f^n \in Fun_{\Omega}$, $t_1, \ldots, t_n \in CTm_{\Omega \cup M}$.

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* $|C|_M$:

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

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

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

$$|\forall x[x/a]A|_M = \min_{m \in \underline{M}} |[m/a]A|_M.$$

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.

[13] 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.

[14] 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.

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 Ω 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 $A = \neg B$, $(B \vee C)$, $(B \to C)$.

6. Пусть $A = \exists x[x/a]B$. Тогда надо определить $|A|_M = \max\limits_{m \in M} |[m/a]B|_M$. 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

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

то также получаем и

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

Таким образом, $|A|_M$ и 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:

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

т.к.

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

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,

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

т.к.

$$\mathbb{Q} \nvDash r \cdot r = 1 + 1$$

для всех $r \in \mathbb{Q}$.

Изоморфизмы моделей

Определим теперь точно, какие модели будут считаться "одинаковыми".

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

- α — биекция,
- $\alpha(c_M) = c_{M'}$ для всех $c \in Const_\Omega$,
- $\alpha(f_M(m_1, \dots, m_k)) = f_{M'}(\alpha(m_1), \dots, \alpha(m_k))$ для всех $f^k \in Fun_\Omega$ 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 $P^k \in Pred_\Omega$ 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 α — 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 Ω, $\alpha : M \cong M'$. 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 Ω, $\alpha : M \cong M'$.*

(1) Если $t \in CTm_{\Omega\cup M}$, то $|\alpha{\cdot}t|_{M'} = \alpha(|t|_M)$.

(2) Если $A \in CFm_{\Omega\cup M}$, 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:

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

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

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

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

Утверждение (2) докажем на следующей лекции.

Лекция 8

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

(1) Если $t \in CTm_{\Omega\cup M}$, то $|\alpha\cdot t|_{M'} = \alpha(|t|_M)$.

(2) Если $A \in CFm_{\Omega\cup M}$, то $|\alpha\cdot A|_{M'} = |A|_M$.

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,

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

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

по (1) и определению изоморфизма. Отсюда получаем:

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

(2.2) $A = (B \wedge C)$.
(2.3) $A = (B \vee C)$,
(2.4) $A = (B \to C)$,
(2.5) $A = \neg B$.

Эти простые случаи оставляются читателю в качестве упражнения.

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

По определению истинности

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

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

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

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

Но

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

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

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

$$M \vDash A \Leftrightarrow M' \vDash A.$$

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 $\gamma : M^k \longrightarrow \{0,1\}$. 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 $\gamma : M^k \longrightarrow \{0,1\}$:

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

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

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

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 $A(b_1, \ldots, b_k)$, если хотим отметить, что $FV(A) \subseteq \{b_1, \ldots, b_k\}$. 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 $t(b_1, \ldots, b_k)$ означает, что $FV(t) \subseteq \{b_1, \ldots, b_k\}$.

Определение 42. Рассмотрим формулу $A(\overrightarrow{b})$, где $\overrightarrow{b} = (b_1, \ldots, b_k)$.
k-местный предикат, определимый формулой $A(\overrightarrow{b})$ в модели M — это
$A_M : \underline{M}^k \longrightarrow \{0,1\}$, такой что для всех $m_1, \ldots, m_k$

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

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

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

для всех $\overrightarrow{m} \in M^k$.[15]

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 $\exists x(b_1 + x = b_2)$:

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

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:

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

Докажем необходимое условие определимости предиката в модели.

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

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

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

В сокращенной записи:

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

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

[15] Для краткости мы пишем M^k вместо $\underline{M}^k$.

Доказательство По определению 42 и теореме 7.4

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

■

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

$$M \vDash A(\overrightarrow{m}) \Leftrightarrow \overrightarrow{m} \in R.$$

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

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

Теорема 8.2 означает, что определимые отношения инвариантны при автоморфизмах:

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

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.

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:

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

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 Ω, $x_1, \dots, x_n$ — (различные) связанные переменные, не входящие в A. Тогда для любой модели M сигнатуры Ω*

$$M \vDash \forall x_1 \dots \forall x_n A(x_1, \dots, x_n) \Leftrightarrow \textit{для всех } m_1, \dots, m_n \in M \ M \vDash A(m_1, \dots, m_n),$$

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

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) $M \vDash A \Leftrightarrow$ для всех $m_1 \in M$ $M \vDash B(m_1)$.

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) $\qquad M \vDash \forall x_2 \dots \forall x_n A(m_1, x_2, \dots, x_n) \Leftrightarrow$

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

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

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

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

(I) $\forall x_1 \dots \forall x_n \forall y_1 \dots \forall y_n (\bigwedge\limits_{i=1}^{n} x_i = y_i \to (P^n(x_1, \dots, x_n) \leftrightarrow P^n(y_1, \dots, y_n)))$
для всех $P^n \in Pred_\Omega$.

(II) $\forall x_1 \dots \forall x_n \forall y_1 \dots \forall y_n (\bigwedge\limits_{i=1}^{n} x_i = y_i \to f^n(x_1, \dots, x_n) = f^n(y_1, \dots, y_n))$
для всех $f^n \in Fun_\Omega$.

Запишем эти аксиомы в сокращенном виде:

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

(II) $\ \forall \overrightarrow{x} \forall \overrightarrow{y} (\overrightarrow{x} = \overrightarrow{y} \to f^n(\overrightarrow{x}) = f^n(\overrightarrow{y})).$

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

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

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

По лемме 8.3, формула (I) верна в M, если и только если для всех $\overrightarrow{m}, \overrightarrow{m'} \in M^n$
$$M \vDash \overrightarrow{m} = \overrightarrow{m'} \to (P(\overrightarrow{m}) \leftrightarrow P(\overrightarrow{m'}))$$
(где $\overrightarrow{m} = \overrightarrow{m'}$ — сокращение для $m_1 = m_1' \wedge \dots \wedge m_n = m_n'$).

Но последнее утверждение очевидно: в нормальной модели
$M \vDash \overrightarrow{m} = \overrightarrow{m'}$ означает, что $\overrightarrow{m}$ и $\overrightarrow{m'}$ совпадают; тогда и
$|P(\overrightarrow{m})|_M = |P(\overrightarrow{m'})|_M$, а потому $|P(\overrightarrow{m}) \leftrightarrow P(\overrightarrow{m'})|_M = 1$.

Следовательно, верна импликация
$$\overrightarrow{m} = \overrightarrow{m'} \to (P(\overrightarrow{m}) \leftrightarrow P(\overrightarrow{m'})).$$

Аналогично рассуждаем для формулы (II):
$$M \vDash \overrightarrow{m} = \overrightarrow{m'} \to f(\overrightarrow{m}) = f(\overrightarrow{m'}),$$
т.к. из совпадения $\overrightarrow{m}$ и $\overrightarrow{m'}$ следует совпадение $f_M(\overrightarrow{m})$ и $f_M(\overrightarrow{m'})$. ■

Покажем теперь, как из произвольной модели теории Eq_Ω построить элементарно эквивалентную нормальную модель.

Пусть $M \vDash Eq_\Omega$. Тогда предикат $=_M$ задает отношение эквивалентности на $\underline{M}$, которое мы обозначим $\approx$. Т.е.
$$m_1 \approx m_2 \ \Leftrightarrow =_M(m_1, m_2) = 1 \ \Leftrightarrow \ M \vDash m_1 = m_2.$$
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 Ω следующим образом:

$$\begin{aligned}
&c_{\widetilde{M}} := \widetilde{c_M},\\
&f^k_{\widetilde{M}}(\widetilde{m_1}, \dots, \widetilde{m_k}) := f^k_M(\widetilde{m_1, \dots, m_k}),\\
&P^k_{\widetilde{M}}(\widetilde{m_1}, \dots, \widetilde{m_k}) := P^k_M(m_1, \dots, m_k)
\end{aligned}$$

(где соответственно, $c \in Const_\Omega,\ f^k \in Fun_\Omega,\ P^k \in Pred_\Omega$).

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

Доказательство Надо проверить, что если заменить m_i на эквивалентные элементы, то правые части в определении $f^k_{\widetilde{M}}$ и $P^k_{\widetilde{M}}$ не изменятся.

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

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

Лекция 9

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

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

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

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

Для символа $=$ также имеем[16]

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

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 α — сюръекция.[17] ■

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

Теорема 9.2. *Пусть T — теория в сигнатуре с равенством Ω, содержащая Eq_Ω. 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 $M, M' \vDash T$. По лемме 8.5, $M \equiv \widetilde{M}$, $M' \equiv \widetilde{M'}$. Поэтому $\widetilde{M}, \widetilde{M'} \vDash T$. Т.к. эти модели нормальны, по условию они изоморфны. Следовательно, $\widetilde{M} \equiv \widetilde{M'}$ (теорема 8.1). В итоге имеем $M \equiv M'$. ■

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

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

(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.

[16] Здесь знак $=$ употребляется в двух смыслах.

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

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)

$\forall x \forall y \forall z\ (x < y \wedge y < z \to x < z)$ (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 Ω.

Мы построим формулу A_M, которая полностью описывает M.

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

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

где

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

$$\bigwedge \{c = a_i \mid c \in Const_\Omega,\ c_M \text{ равно } m_i\} \wedge$$

$$\bigwedge \{f^k(a_{i_1}, \ldots, a_{i_k}) = a_j \mid f^k \in Pred_\Omega,\ f^k_M(m_{i_1}, \ldots, m_{i_k}) \text{ равно } m_j\} \wedge$$

$$\bigwedge \{P^k(a_{i_1}, \ldots, a_{i_k}) \mid P^k \in Pred_\Omega,\ M \vDash P^k(m_{i_1}, \ldots, m_{i_k})\} \wedge$$

$$\bigwedge \{\neg P^k(a_{i_1}, \ldots, a_{i_k}) \mid P^k \in Pred_\Omega,\ M \nvDash P^k(m_{i_1}, \ldots, m_{i_k})\}.$$

Лемма 9.4. *Для нормальной модели M' сигнатуры Ω*

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

Доказательство

($\Leftarrow$) Заметим, что
$$M \vDash \psi_M(m_1, \ldots, m_n).$$
Действительно,
$$\psi_M(m_1, \ldots, m_n) = \bigwedge_{1\le i<j\le n} (m_i \ne m_j) \wedge \forall v_{n+1} \bigvee_{i=1}^{n} (v_{n+1} = m_i) \wedge$$
$$\bigwedge\{c = m_i \mid c \in Const_\Omega,\ c_M \text{ равно } m_i\} \wedge$$
$$\bigwedge\{f^k(m_{i_1}, \ldots, m_{i_k}) = m_j \mid f^k \in Pred_\Omega,\ f^k_M(m_{i_1}, \ldots, m_{i_k}) \text{ равно } m_j\} \wedge$$
$$\bigwedge\{P^k(m_{i_1}, \ldots, m_{i_k}) \mid P^k \in Pred_\Omega,\ M \vDash P^k(m_{i_1}, \ldots, m_{i_k})\} \wedge$$
$$\bigwedge\{\neg P^k(m_{i_1}, \ldots, m_{i_k}) \mid P^k \in Pred_\Omega,\ M \nvDash P^k(m_{i_1}, \ldots, m_{i_k})\}.$$
Проверим, что все 6 членов этой конъюнкции (все они — тоже конъюнкции, кроме второго) истинны в M.

(1) $M \vDash \bigwedge\limits_{1\le i<j\le n} (m_i \ne m_j)$, т.к. M нормальна и все m_i различны,

(2) $M \vDash \forall v_{n+1} \bigvee\limits_{i=1}^{n} (v_{n+1} = m_i)$, т.к. всякий элемент из M равен одному из m_i.

(3) $M \vDash \bigwedge\{c = m_i \mid c \in Const_\Omega,\ c_M \text{ равно } m_i\}$,
т.к. для всякой константы c, $M \vDash c = m_i$, если c_M равно m_i — это очевидно, по определению истинности (см. определения 36, 37 лекции 7).

(4) Аналогично, для четвертого члена имеем: $M \vDash f(m_{i_1}, \ldots, m_{i_k}) = m_j$, если $f_M(m_{i_1}, \ldots, m_{i_k})$ равно m_j.

(5) Истинность пятого члена означает, что $M \vDash P^k(m_{i_1}, \ldots, m_{i_k})$, если $M \vDash P^k(m_{i_1}, \ldots, m_{i_k})$. Это тривиальность.

(6) Также очевидно.

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

($\Rightarrow$) Предположим, что $M' \vDash A_M$ и построим изоморфизм M на M'. Снова по лемме 8.3, найдутся $m'_1, \ldots, m'_n \in M'$, для которых
$$M' \vDash \psi_M(m'_1, \ldots, m'_n).$$
Для удобства опять распишем $\psi_M(m'_1, \ldots, m'_n)$:
$$\bigwedge_{1\le i<j\le n} (m'_i \ne m'_j) \wedge \forall v_{n+1} \bigvee_{i=1}^{n} (v_{n+1} = m'_i) \wedge$$
$$\bigwedge\{c = m'_i \mid c \in Const_\Omega,\ c_M \text{ равно } m_i\} \wedge$$
$$\bigwedge\{f^k(m'_{i_1}, \ldots, m'_{i_k}) = m'_j \mid f^k \in Pred_\Omega,\ f^k_M(m_{i_1}, \ldots, m_{i_k}) \text{ равно } m_j\} \wedge$$
$$\bigwedge\{P^k(m'_{i_1}, \ldots, m'_{i_k}) \mid P^k \in Pred_\Omega,\ M \vDash P^k(m_{i_1}, \ldots, m_{i_k})\} \wedge$$
$$\bigwedge\{\neg P^k(m'_{i_1}, \ldots, m'_{i_k}) \mid P^k \in Pred_\Omega,\ M \nvDash P^k(m_{i_1}, \ldots, m_{i_k})\}.$$
Докажем, что отображение φ, переводящее каждый m_i в m'_i — искомый изоморфизм.

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

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

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

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

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

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

Если же $M \nvDash P^k(m_{i_1}, \ldots, m_{i_k})$, то из 6-го члена, $M' \nvDash P^k(m'_{i_1}, \ldots, m'_{i_k})$. ■

Продолжим доказательство теоремы 9.3.

Заметим, что $Th(M) \sim \{A_M\}$.[18] Действительно, по лемме 9.4 $A_M \in Th(M)$ и значит,

$$M' \vDash Th(M) \Rightarrow M' \vDash A_M.$$

Обратно, пусть $M' \vDash A_M$. По той же лемме, $M' \cong M$. И тогда $M' \vDash Th(M)$.

Итак, $Th(M)$ конечно аксиоматизируема.

Также $Th(M)$ 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 $M' \vDash Th(M)$. 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 $A(\overrightarrow{b})$ — формула сигнатуры Ω; $\overrightarrow{x}$, $\overrightarrow{y}$ — списки (той же длины, что $\overrightarrow{b}$) различных связанных переменных, не входящих в A.*

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

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

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

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

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

и

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

Поэтому

$$M \vDash \forall \overrightarrow{x} A(\overrightarrow{x}) \Leftrightarrow M \vDash \forall \overrightarrow{y} A(\overrightarrow{y}).$$

Значит, эти формулы равносильны (лемма 9.4).

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

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

$\forall x_1 \ldots \forall x_n [x_1, \ldots, x_n / b_1, \ldots, b_n] A$.

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 $b_1, \ldots, b_n$ в любом порядке, и переменные $x_1, \ldots, x_n$ 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 $\overline{\forall} A$.

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 $\overline{\forall}(A \leftrightarrow B)$.

[18] Эквивалентность здесь понимается относительно нормальных моделей. Если рассматривать произвольные модели, то надо добавить еще Eq_Ω.

[19] Этот порядок задается нумерацией множества $FVar$, см. лекцию 6.

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

Таким образом, по лемме 8.3

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

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

Лемма 9.8.

(1) $\sim$ задает отношение эквивалентности на Fm_Ω.

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

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

(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 Ω. Пусть S — подстановка, заменяющая каждое вхождение P_i на B_i. При этой замене из F получится формула сигнатуры Ω, 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.

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 пропозоциональных 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) $Яx[x/a](A \circ B) \sim (Яx[x/a]A \circ B)$, если a не входит в B (и x не входит ни в A, ни в B). Здесь $Я$ обозначает квантор $\forall$ или $\exists$, а $\circ$ — 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 $\to$).
(7) Если $A \sim B$, то $Яx[x/a]A \sim Яx[x/a]B$ (при условии, что x не входит ни в A, ни в B).
(8) $Яx[x/a]A \sim Яy[y/a]A \sim Яy[y/b][b/a]A$, 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 $\theta : Var \longrightarrow \{0, 1\}$ 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 θ, 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 $M \vDash SF(m_1, \dots, m_k)$ для любой M и при любом выборе $m_1, \dots, m_k$. Это дает общезначимость SF. ■

[20] Подразумевается, что M — в нужной сигнатуре, а $\overrightarrow{m}$ — список ее элементов нужной длины.

Лемма 9.10.

(1) Если $F_1 \sim F_2$, то $SF_1 \sim SF_2$ (для любых пропозоциональных 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) $Ꙗx[x/a](A \circ B) \sim (Ꙗx[x/a]A \circ B)$, если a не входит в B (и x не входит ни в A, ни в B).
Здесь Ꙗ обозначает квантор $\forall$ или $\exists$, а $\circ$ — 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 $\to$).

(7) Если $A \sim B$, то $Ꙗx[x/a]A \sim Ꙗx[x/a]B$ (при условии, что x не входит ни в A, ни в B).

(8) $Ꙗx[x/a]A \sim Ꙗy[y/a]A \sim Ꙗy[y/b][b/a]A$, 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 $A(a, \overrightarrow{b})$; надо проверить, что в любой модели M для всех $\overrightarrow{m}$

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

Но это сразу следует из определения истинности:

$$|\neg\forall x A(x, \overrightarrow{m})|_M = 1 \Leftrightarrow |\forall x A(x, \overrightarrow{m})|_M = 0 \Leftrightarrow$$
$$\text{не для всех } k \in M\ |A(k, \overrightarrow{m})|_M = 1 \Leftrightarrow$$
$$\text{найдется } k \in M,\ \text{для которого } |A(k, \overrightarrow{m})|_M = 0 \Leftrightarrow$$
$$\text{найдется } k \in M,\ \text{для которого } |\neg A(k, \overrightarrow{m})|_M = 1 \Leftrightarrow |\exists x \neg A(x, \overrightarrow{m})|_M = 1.$$

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

(4) Проверим это для $Ꙗ = \exists$ и $\circ = \wedge$; остальные случаи разбираются аналогично.

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

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

В самом деле,

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

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

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

Таким образом, $(*)$ выполняется.

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

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

По тому же определению,

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

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

$$Я_1 x_1 \dots Я_n x_n [x_1, \dots, x_n / a_1, \dots, a_n] A,$$

где $Я_1, \dots, Я_n$ — 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[21].

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) $A = (B \to C)$. 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) $A = Яx[x/a]B$, 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), $A \sim Яx[x/a]B_1$. Ясно, что $Яx[x/a]B_1$ — 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) $B = (C \to D)$. Из логики высказываний, $A = \neg(C \to D) \sim (C \wedge \neg D)$. 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, $A \sim C_1$. ■

[21] 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 $A = \text{Я}x[x/a]A_1$.

Случай 1. a, x не входят в B.

По лемме 9.10,

$$(A \circ B) = (\text{Я}x[x/a]A_1 \circ B) \sim \text{Я}x[x/a](A_1 \circ B).$$

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,

$$\text{Я}x[x/a](A_1 \circ B) \sim \text{Я}x[x/a]C.$$

Таким образом, $(A \circ B)$ равносильна ПНФ $\text{Я}x[x/a]C$.

(1.2) Если x входит в C, то возьмем новую связанную переменную y, которой нет в A_1, B, C. По лемме 9.10, $A = \text{Я}x[x/a]A_1 \sim \text{Я}y[y/a]A_1$, и далее $(A \circ B) \sim (\text{Я}y[y/a]A_1 \circ B)$. Теперь, как в (1.1):

$$(\text{Я}y[y/a]A_1 \circ B) \sim \text{Я}y[y/a]C.$$

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,

$$A = \text{Я}x[x/a]A_1 \sim \text{Я}y[y/b][b/a]A_1.$$

Формула $\text{Я}y[y/b][b/a]A_1$ 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) $A = \text{Я}x[x/a]B$.

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:

$$A = \text{Я}x[x/a]B \sim \text{Я}y[y/a]B \sim \text{Я}y[y/a]B'.$$

Формула $\text{Я}y[y/a]B'$ — ПНФ. ∎

Пример Рассмотрим формулу $\forall x P(x) \vee \exists x Q(x)$. Она приводится к ПНФ следующим образом:

$$(\forall x P(x) \,\vee\, \exists x Q(x)) \sim (\forall x P(x) \,\vee\, \exists y Q(y)) \sim \forall x\,(P(x) \,\vee\, \exists y Q(y)) \sim \forall x \exists y\,(P(x) \,\vee\, Q(y)).$$

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

$$\models \text{Я}x_1 \ldots \text{Я}x_n[x_1, \ldots, x_n/a_1, \ldots, a_n]A \;\Rightarrow \models A.$$

Например, формула $\exists x \forall y\,(P(x) \to P(y))$ общезначима, т.к.

$$\exists x \forall y\,(P(x) \to P(y)) \sim \exists x \forall y\,(\neg P(x) \,\vee\, P(y)) \sim$$

$$\exists x\,(\neg P(x) \,\vee\, \forall y P(y)) \sim (\exists x \neg P(x) \,\vee\, \forall y P(y)) \sim (\neg \forall x P(x) \,\vee\, \forall y P(y))$$

$$\sim (\neg \forall x P(x) \,\vee\, \forall x P(x)).$$

При этом $P(x) \to P(y)$ — совсем не общезначима.

Лекция 11

Исчисление предикатов

Исчисление предикатов в сигнатуре Ω — это аксиоматическая система гильбертовского типа. Она обозначается через PC_Ω 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 Ω.

II. Предикатные аксиомы

(1) $\forall x[x/a]A \to [t/a]A$.

(2) $[t/a]A \to \exists x[x/a]A$.

(3) $\forall x[x/a](A \to B) \to (A \to \forall x[x/a]B)$.

(4) $\forall x[x/a](B \to A) \to (\exists x[x/a]B \to A)$.

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.[22]

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)

$$\frac{A,\ A \to B}{B},$$

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 Γ — некоторое множество формул сигнатуры Ω. *Вывод формулы A в PC_Ω из* Γ— это конечная последовательность формул, каждая из которых — аксиома или принадлежит Γ 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:

- A_k — аксиома,
- $A_k \in \Gamma$,
- существуют $i, j < k$, для которых $A_j = A_i \to A_k$,
- существует $i < k$ и переменные x, a такие, что $A_k = \forall x[x/a]A_i$.

Формула A *выводима из* Γ, если существует ее вывод из Γ; 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 Ω. 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.*

[22] Формально $[t/a]A$ надо определять индукцией по длине A и доказывать, что получается формула.

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:

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

то

$$SA = SB \to (SC \to SB),$$

и это аксиома I.1 (в исчислении предикатов). Аналогично для других аксиом.

2. Пусть A получается по правилу MP из B и $B \to A$. По предположению индукции, в PC_Ω выводимы SB и $S(B \to A)$. Но $S(B \to A) = SB \to SA$. Применив MP в исчислении предикатов, получим $\vdash_{PC_\Omega} SA$. ∎

Лемма 11.3. *Некоторые теоремы и допустимые правила в* PC_Ω.

(1) $\forall x[x/a]A \to A$ *(x не входит в A).*

(2) $A \to \exists x[x/a]A$ *(x не входит в A).*

(3) $\dfrac{A \to B}{A \to \forall x[x/a]B}$.

(4) $\dfrac{B \to A}{\exists x[x/a]B \to A}$.

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 Γ.

Пусть $\Gamma \vdash A \to B$. По правилу *Gen* тогда $\Gamma \vdash \forall x[x/a](A \to B)$. По аксиоме II.3, $\Gamma \vdash \forall x[x/a](A \to B) \to (A \to \forall x[x/a]B)$. Теперь $\Gamma \vdash A \to \forall x[x/a]B$ по MP.

(4) Аналогичное рассуждение с аксиомой II.4. (Упражнение.) ∎

Лемма 11.4. $\vdash_{PC_\Omega} \mathsf{Q} y[y/a]A \to \mathsf{Q} x[x/a]A$,
где Q — квантор, а переменные x, y не входят в A.

Доказательство Рассмотрим случай $\mathsf{Q} = \forall$.

$\vdash \forall y[y/a]A \to [x/a]A$ — аксиома II.1. Тогда $\vdash \forall y[y/a]A \to \forall x[x/a]A$ по правилу Бернайса.

Случай $\mathsf{Q} = \exists$ разбирается аналогично (упражнение). ∎

Лемма 11.5. *(Ослабленная теорема дедукции) Если $\Gamma, A \vdash_{PC_\Omega} B$ без применения правила Gen, то $\Gamma \vdash_{PC_\Omega} A \to B$.*

Доказательство Доказательство — такое же, как для теоремы дедукции в CL (см. лекцию 4). ∎

Лемма 11.6. *В исчислении предикатов допустимо правило силлогизма*

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

Доказательство Из теоремы дедукции следует, что это правило — производное. См. лекцию 4. ∎

Лемма 11.7. *В PC_Ω в выводах из гипотез допустимы правила Бернайса:*

(1) $\dfrac{A \to B}{A \to \forall x[x/a]B}$.

(2) $\dfrac{B \to A}{\exists x[x/a]B \to A}$.

где x не входит в B; переменная a не входит в A.

Доказательство Докажем допустимость 1го правила; второе рассматривается аналогично.

Пусть $\Gamma \vdash A \to B$. Выберем переменную y, не входящую ни в A, ни в B. Тогда по лемме 10.3

$$\Gamma \vdash A \to \forall y[y/a]B.$$

По лемме 11.4,

$$\vdash \forall y[y/a]B \to \forall x[x/a]B.$$

Отсюда по правилу силлогизма

$$\Gamma \vdash A \to \forall x[x/a]B.$$

■

Теорема 11.8. *(Теорема дедукции) Если A — замкнутая формула, то*

$$\Gamma, A \vdash_{PC_\Omega} B \Leftrightarrow \Gamma \vdash_{PC_\Omega} A \to B.$$

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 $\Gamma \vdash A \to C$. Тогда по правилу Бернайса (поскольку A замкнута) получаем

$\Gamma \vdash A \to \forall x[x/a]C$, т.е. $\Gamma \vdash A \to B$. ■

Следствие 11.9. *Для любой конечной теории T и формулы A сигнатуры Ω*

$$T \vdash_{PC_\Omega} A \Leftrightarrow\ \vdash_{PC_\Omega} (\bigwedge T) \to A.$$

Здесь $\bigwedge T$ обозначает конъюнкцию всех формул из T.[23]

Доказательство (Мы опять опускаем индекс при $\vdash$.) По теореме дедукции

(∗) $\bigwedge T \vdash A \Leftrightarrow\ \vdash (\bigwedge T) \to A.$

Заметим также, что

(∗∗) $T \vdash A \Leftrightarrow \bigwedge T \vdash A.$

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 1го порядка в сигнатуре Ω. Тогда для любой формулы A этой сигнатуры

$$T \vdash_{PC_\Omega} A \Rightarrow T \vDash \overline{\forall} A.$$

(2) Для любой формулы A сигнатуры Ω

$$\vdash_{PC_\Omega} A\ \Rightarrow\ \vDash A,$$

т.е. все теоремы исчисления предикатов общезначимы.

Доказательство Очевидно, что (2) следует из (1): надо взять $T = \varnothing$ и вспомнить, что по определению общезначимость A равносильна общезначимости $\overline{\forall} A$ (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 $\overline{\forall} A = A$, т.к. A замкнута.

(1.2) Все аксиомы группы I — подстановочные примеры аксиом CL. Например, предикатная формула $A \to (B \to A)$ — пример пропозициональной аксиомы $P_1 \to (P_2 \to P_1)$ и т.д. Аксиомы CL — тавтологии (теорема корректности 4.5). Поэтому аксиомы группы I общезначимы по лемме о тавтологиях (лемма 9.5).

[23] Не имеет значения, в каком порядке берутся формулы и расставляются скобки в конъюнкции: утверждение от этого не зависит.

(1.3) Пусть A получается по MP из B и $B \to A$. Выводы этих формул короче, и по предположению индукции

$$T \vDash \overline{\forall} B,\ T \vDash \overline{\forall}(B \to A).$$

Рассмотрим любую модель M теории T и докажем, что $M \vDash \overline{\forall} A$. По лемме 8.3 для этого надо заменить свободные переменные из A (обозначим их список $\overrightarrow{a}$) на произвольные элементы из M (обозначим этот список $\overrightarrow{m}$) и доказать, что полученная оцененная формула (обозначим ее A_1) истинна в M.

Заметим, что при замене $\overrightarrow{a}$ на $\overrightarrow{m}$ 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 $T \vDash \overline{\forall} B$ и $M \vDash T$, имеем $M \vDash \overline{\forall} B$, и по лемме 8.3, $M \vDash B_1$.

Аналогично $M \vDash \overline{\forall}(B \to A)$, откуда $M \vDash B_1 \to A_1$ по лемме 8.3. Теперь из истинности $B_1 \to A_1$ 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 $T \vDash \overline{\forall} B$.

Случай 1 Если a входит в B, то $\overline{\forall} B$ и $\overline{\forall}\forall x[x/a]B$ могут отличаться только порядком кванторов. Из леммы 8.3 следует, что эти формулы равносильны. Поэтому $T \vDash \overline{\forall} A$.

Случай 2 a не входит в B. В этом случае тоже из $M \vDash \overline{\forall} B$ следует $M \vDash \overline{\forall} A$.

В самом деле, пусть $B = B(\overrightarrow{b})$, a не входит в $\overrightarrow{b}$. Допустим, что $M \vDash \overline{\forall} B$. Тогда для всех наборов $\overrightarrow{m}$ элементов из M (той же длины, что $\overrightarrow{b}$) $M \vDash B(\overrightarrow{m})$.

В формуле $A = \forall x[x/a]B(\overrightarrow{b})$ остаются все те же свободные переменные $\overrightarrow{b}$. Поэтому $M \vDash \overline{\forall}\forall x[x/a]B(\overrightarrow{b})$ означает, что для для всех $\overrightarrow{m}$ из M

$$M \vDash \forall x[x/a]B(\overrightarrow{m}).$$

Но это — то же, что $M \vDash B(\overrightarrow{m})$: т.к. переменная a в $B(\overrightarrow{m})$ не входит, любая ее замена оказывается фиктивной. Итак, $M \vDash \overline{\forall} A$.

(1.5) A — аксиома II.3:

$$A = \forall x[x/a](C \to B) \to (C \to \forall x[x/a]B),$$

где x не входит в A 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

$$A_1 = \forall x[x/a](C_1 \to B_1) \to (C_1 \to \forall x[x/a]B_1).$$

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

$$A_1 = \forall x(C_1 \to B_1(x)) \to (C_1 \to \forall x B_1(x)).$$

Докажем, что $M \vDash A_1$. Предположим

$$M \vDash \forall x(C_1 \to B_1(x))$$

и проверим, что $M \vDash C_1 \to \forall x B_1(x)$. В свою очередь, для этого предположим

$$M \vDash C_1$$

и докажем $M \vDash \forall x B_1(x)$. Возьмем любое $m \in M$. Из $M \vDash \forall x(C_1 \to B_1(x))$ следует

$$M \vDash C_1 \to B_1(m).$$

Тогда из $M \vDash C_1$ следует $M \vDash B_1(m)$. Поскольку m произвольно, получаем $M \vDash \forall x B_1(x)$, 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

$$A(a, \overrightarrow{b}) := \forall x[x/a]B \to [t/a]B,$$

где $\overrightarrow{b}$ — список дополнительных параметров (кроме a).[24] Тогда запишем B как $B(a, \overrightarrow{b})$, t — как $t(a, \overrightarrow{b})$.

Рассмотрим модель M и заменим набор параметров $a, \overrightarrow{b}$ на набор произвольных элементов $q, \overrightarrow{m}$ из M. Получим оцененную формулу

$$A(q, \overrightarrow{m}) = \forall x[x/a]B(a, \overrightarrow{m}) \to [t(q, \overrightarrow{m})/a]B(a, \overrightarrow{m}).$$

Обозначим

$$B_1(a) := B(a, \overrightarrow{m}),\ t_1 := t(q, \overrightarrow{m})$$

и перепишем формулу $A(q, \overrightarrow{m})$:

$$A(q, \overrightarrow{m}) = \forall x[x/a]B_1(a) \to B_1(t_1).$$

Здесь $B_1(t_1)$ обозначает $[t_1/a]B_1(a)$.

Нам надо доказать, что $M \vDash A(q, \overrightarrow{m})$. Для этого предположим

$$M \vDash \forall x[x/a]B_1(a)$$

и докажем

$$M \vDash B_1(t_1).$$

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 $M \vDash B_1(t_1)$ (в предположении $M \vDash \forall x[x/a]B_1(a)$), поскольку из $M \vDash \forall x[x/a]B_1(a)$ следует $M \vDash B_1(|t_1|_M)$.

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

$$r(t_1) = t_1,\ r(|t_1|) = |t_1|,$$

и также

$$|t_1| = ||t_1||,$$

по определению значения оцененного терма (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

$$r(t_1) = f(r_1(t_1), \dots, r_n(t_n)),\ r(|t_1|) = f(r_1(|t_1|), \dots, r_n(|t_n|)),$$

и

$$(*) \qquad |r(t_1)| = f_M(|r_1(t_1)|, \dots, |r_n(t_1)|),\ |r(|t_1|)| = f_M(|r_1(|t_1|)|, \dots, |r_n(|t_n|)|).$$

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 связок 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 $\wedge, \vee, \to$ или $\neg$. Эти случаи почти очевидны — упражнение.

(2.3) (шаг индукции) $B_1(a) = \exists x[x/b]C(a, b)$.

[24]Переменная a в формулу A может попасть из терма t. Если она не входит в t (и в A), рассуждение не меняется.

Тогда

$$(**)\qquad |B_1(t_1)| = |\exists x[x/b]C(t_1,b)| = \max_{l\in M}|C(t_1,l)|,\ \ |B_1(|t_1|)| = |\exists x[x/b]C(|t_1|,b)| = \max_{l\in M}|C(|t_1|,l)|.$$

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) (шаг индукции) $B_1(a) = \forall x[x/b]C(a,b)$.

Доказательство аналогично (2.3): $\exists$ заменяется на $\forall$, а max — на min. ■

Исчисление предикатов с равенством

Определение 51. Пусть Ω — сигнатура, содержащая предикатный символ равенства $=$. *Исчисление предикатов с равенством* в сигнатуре Ω получается из обычного исчисления предикатов PC_Ω добавлением аксиом стандартной теории равенства Eq_Ω (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 $\overline{\forall}A$ истинно во всех нормальных моделях данной сигнатуры.

Теорема 12.2. *(Теорема о корректности исчисления предикатов с равенством)*

(1) Пусть T — теория 1го порядка с равенством в сигнатуре Ω. 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 Ω

$$\vdash_{PC_\Omega} A \ \Rightarrow \vDash_{\text{норм}} A,$$

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 $T = \varnothing$ и применим (1) для $\overline{\forall}A$. ■

Непротиворечивость

Определение 52. Теория T в сигнатуре Ω 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 Ω с равенством *противоречива*, если $T \vdash_{PC_\Omega^=} A$ и $T \vdash_{PC_\Omega^=} \neg A$ для некоторой формулы A сигнатуры Ω.

Лемма 12.3. *Если теория T в сигнатуре Ω 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 1го порядка выполнима, то она непротиворечива.*

(2) Если теория 1го порядка с равенством нормально выполнима (т.е. имеет нормальную модель), то она непротиворечива.

Доказательство (1) Предположим, что теория T в сигнатуре Ω противоречива. Предположим, что $M \vDash T$. Возьмем какую-нибудь замкнутую формулу B, истинную в M (например, формулу вида $A \to A$). По лемме 12.3, $T \vdash_{PC_\Omega} \neg B$. Тогда по теореме корректности 11.10, $T \vDash \neg B$. Следовательно, $M \vDash \neg B$, что противоречит выбору B.

(2) Аналогично, с использованием $PC_\Omega^=$. ■

Пример: арифметика Пеано

Арифметика Пеано (PA) — это теория 1го порядка в сигнатуре $\{0, 1, +, \cdot, =\}$ (см. лекцию 6) со следующими аксиомами:

(1) $\forall x\,(x + 1 \neq 0)$.

(2) $\forall x \forall y\,(x + 1 = y + 1 \to x = y)$.

(3) $\forall x\,(x \neq 0 \to \exists y\,(y + 1 = x))$.

(4) $\forall x\,(x + 0 = 0)$.

(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) $\overline{\forall}\,(A(0) \wedge \forall x\,(A(x) \to A(x + 1)) \to \forall x\,A(x))$.

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. $A = A(a, \ldots)$. $A(0)$, $A(x)$ обозначают соответственно $[0/a]A$, $[x/a]A$; $\forall x\,(A(x) \to A(x + 1))$ — это формула $\forall x\,[x/a](A \to [a + 1/a]A)$.

(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 нуль, 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 $(A \to B) \in MFm$.
- 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)

$$\begin{array}{ll} (AK) & \Box(A \to B) \to (\Box A \to \Box B), \\ (AT) & \Box A \to A, \\ (A4) & \Box A \to \Box\Box A, \\ (A5) & \Diamond\Box A \to \Box A. \end{array}$$

Правила вывода S5

Modus Ponens (MP),

Правило добавления $\Box$ (Nec): $\dfrac{A}{\Box A}$

Понятия вывода и выводимости в $S5$ определяются аналогично CL (с учетом дополнительного правила), точное определение оставляется читателю.

Семантика Крипке для S5

Определение 54. Пусть $W \neq \varnothing$ — множество. *Оценка* (пропозициональных переменных) на W — это отображение $Var \longrightarrow \mathcal{P}(W)$. *Модель Крипке*[25] на W — это пара (W, θ), где θ — 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,
- $|A \wedge B|_u^M = \min(|A|_u^M, |B|_u^M)$,
- $|A \vee B|_u^M = \max(|A|_u^M, |B|_u^M)$,
- $|\neg A|_u^M = 1 - |A|_u^M$,
- $|A \to B|_u^M = \max(1 - |A|_u^M, |B|_u^M)$,
- $|\Box A|_u^M = \min\limits_{v \in W} |A|_v^M$.

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 $M, u \vDash A$ и говорят, что формула A *истинна в модели M в мире u*.

В этих обозначениях определение 55 записывается так:

- $M, u \vDash P_i \Leftrightarrow u \in \theta(P_i)$,
- $M, u \vDash A \wedge B \Leftrightarrow M, u \vDash A$ и $M, u \vDash B$,
- $M, u \vDash A \vee B \Leftrightarrow M, u \vDash A$ или $M, u \vDash B$,
- $M, u \vDash \neg A \Leftrightarrow M, u \nvDash A$,
- $M, u \vDash A \to B \Leftrightarrow M, u \nvDash A$ или $M, u \vDash B$,
- $M, u \vDash \Box A \Leftrightarrow \forall v \in W\ M, v \vDash A$.

Из определения сразу получаем:

$$M, u \vDash \Diamond A \Leftrightarrow \exists v \in W\ M, v \vDash A.$$

Таким образом, в семантике Крипке "необходимо" ($\Box$) понимается как истинность во всех мирах ("всегда"), а "возможно" ($\Diamond$) — как истинность в некоторых мирах ("иногда").

[25] Иногда говорят: модель Крипке – Лейбница

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 $W \vDash A$.

Теорема 12.5. *(теорема корректности для $S5$)*
Если $\vdash_{S5} A$, то $W \vDash A$ для любого $W \neq \varnothing$.

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: $P_1^1, P_2^1, \ldots$ *Стандартный перевод* (или перевод Вайсберга) $A \mapsto A^*$ модальных формул в формулы 1го порядка в этой сигнатуре определяется по индукции:

- $P_i^* := P_i^1(a)$,
- $(A \circ B)^* := (A^* \circ B^*)$ для $\circ = \vee, \to, \wedge$,
- $(\neg A)^* := \neg A^*$,
- $(\Box A)^* := \forall x\, [x/a] A^*$, где x — первая связанная переменная (в общем списке $BVar$ — см. лекцию 6), не входящая в A.[26]

Таким образом, A^* — формула с одной свободной переменной a или замкнутая.

Определение 58. Каждой модели Крипке $M = (W, \theta)$ поставим в соответствие модель M^* сигнатуры $\{P_1^1, P_2^1, \ldots\}$ с носителем W. А именно, полагаем для каждого $u \in W$

$$M^* \vDash P_i^1(u) \Leftrightarrow M, u \vDash P_i.$$

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 1го 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. [27] *Для любой модальной формулы A и непустого W*

$$W \vDash \forall x\, [x/a] A^* \textit{ в классической логике } \Leftrightarrow W \vDash A \textit{ в модальной логике }.$$

Доказательство ($\Rightarrow$) Доказываем от противного. Пусть $W \nvDash A$, тогда для некоторой модели Крипке M на W и какого-то мира $u \in W$

$$M, u \nvDash A.$$

Отсюда по лемме 12.6

$$M^* \nvDash A^*(u),$$

следовательно,

$$M^* \nvDash \forall x\, [x/a] A^*,$$

[26] Можно взять и любую другую переменную, не попавшую в A, но мы выбираем первую для единообразия.

[27] На лекции в формулировке этой леммы была допущена неточность: запись $\forall u A^*(u)$ неправомерна.

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 μ нашей сигнатуры (с одноместными предикатами) с носителем W такая, что
$$\mu \not\models \forall x\, [x/a] A^*.$$
т.е. для некоторого $u \in W$

$$(\sharp) \qquad \mu \not\models A^*(u).$$

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 ($\sharp$) по лемме 12.6 получаем
$$M, u \not\models A.$$
Таким образом, $W \not\models A$. ■

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) $\models A^*$,

(4) $W \models A^*$ *на всех конечных* W,

(5) $W \models A$ *на всех* W,

(6) $W \models A$ *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:

$$\begin{array}{ccccccc} 1 & \Rightarrow & 2 & \Rightarrow & 3 & \Rightarrow & 4 \\ \Uparrow & & & & \Downarrow & & \Downarrow \\ 6 & & & & 5 & \Rightarrow & 6 \end{array}$$

($1 \Rightarrow 2$). Индукция по длине вывода A в $S5$.

- Если A — аксиома группы (I), то A^* — аксиома PC того же вида (из группы I). Например, если $A = (B \wedge C) \to B$, то $A^* = (B^* \wedge C^*) \to B^*$ и т.д.
- Пусть
$$A = (\Box(C \to B) \to (\Box C \to \Box B)).$$
Тогда
$$A^* = (\forall x (C^*(x) \to B^*(x)) \to (\forall x C^*(x) \to \forall x B^*(x))).$$

Тогда $\vdash_{PC} A^*$ получим по теореме дедукции (она применима, т.к. все гипотезы — замкнутые) из следуюшей выводимости:

$$\forall x(C^*(x) \to B^*(x)), \forall x C^*(x) \vdash \forall x B^*(x).$$

А это доказывается непосредственно:

1. $\forall x(C^*(x) \to B^*(x))$ — гипотеза.
2. $\forall x(C^*(x) \to B^*(x)) \to (C^*(a) \to B^*(a))$ — аксиома II.1 из PC.
3. $C^*(a) \to B^*(a)$ — 1, 2, MP.
4. $\forall x C^*(x)$ — гипотеза.
5. $\forall x C^*(x) \to C^*(a)$ — аксиома II.1 из PC.
6. $C^*(a)$ — 4, 5, MP.
7. $B^*(a)$ — 3, 6, MP.
8. $\forall x B^*(x)$ — 7, Gen.

- Пусть $A = (\Box B \to B)$. Тогда $A^* = \forall x B^*(x) \to B^*(a)$ — аксиома.
- $A = (\Box B \to \Box\Box B)$. Тогда $A^* = (\forall x B^*(x) \to \forall y \forall x B^*(x))$ получается с помощью правила Бернайса из $\forall x B^*(x) \to \forall x B^*(x)$ (примера тавтологии — см. лемму 11.2).
- $A = (\Diamond\Box B \to \Box B)$. Тогда $A^* = (\exists y \forall x B^*(x) \to \forall x B^*(x))$ получается из $\forall x B^*(x) \to \forall x B^*(x)$ с помощью второго правила Бернайса.
- A получается по MP из B, $B \to A$. По предположению индукции,

$$\vdash_{PC} B^*,\ B^* \to A^*.$$

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.[28]

$(3 \Rightarrow 5)$. 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

$$\frac{A \to B}{\Box A \to \Box B}, \quad \frac{A \to B}{\Diamond A \to \Diamond B}.$$

(2) $\equiv$ задает отношение эквивалентности на MFm.

(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 $\circ = \vee, \wedge, \to$.

(4) Если A — подформула формулы B и $A \equiv A'$, то замена вхождения A на A' в B даст эквивалентную формулу: $B(...A...) \equiv B(...A'...)$.

(5) $\Diamond(A \vee B) \equiv \Diamond A \vee \Diamond B$.

(6) $\Diamond(A \wedge \Diamond B) \equiv \Diamond A \wedge \Diamond B$.

[28] $W \vDash A^*$ означает то же, что $W \vDash \forall x[x/a]A^*(a)$.

(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,
- 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 $A \equiv \bigvee\limits_i A_i$, где A_i — вида $\bigwedge\limits_j Q_{ij}$, 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: $B \sim \bigvee\limits_i B_i$, 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 $\Box$ (это можно сделать, т.к. $\Box A \equiv \neg\Diamond\neg A$). 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 $\Diamond A \equiv \bigvee\limits_i \Diamond A_i$ (лемма 13.2 (5),(3)).

Рассмотрим $\Diamond A_i = \Diamond \bigwedge\limits_j Q_{ij}$. Используя лемму 13.2 (6),(7) (и эквивалентность $\neg\Diamond D \equiv \Box\neg D$), преобразуем эту формулу в конъюнкцию формул вида $\Diamond P_k$, $\Diamond D$, $\Box D$ (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 $S5$.

<u>Упражнение</u> Оцените количество этих формул в зависимости от n.

Определение 61. Для множества модальных формул Γ *выводимость* формулы A, (обозначение: $\Gamma \vdash_{S5} A$) означает, что существует вывод A с использованием формул из Γ, аксиом $S5$ и правила MP (но не Gen).

Γ *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 Φ — множество всех модальных формул от $P_1, \dots, P_n$. Рассматриваем непротиворечивые (в $S5$) подмножества Φ.

Определение 62. Множество $\Gamma \subseteq \Phi$ называется *максимальным*), если оно непротиворечиво, а всякое его собственное расширение внутри Φ противоречиво.

Лемма 13.7. *Всякое непротиворечивое множество содержится в максимальном.*

Доказательство Если Γ 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 $\vdash_{S5} A \to A'_i$, а тогда $\Gamma \cup \{A\} \vdash A'_i$ (по MP).

Если же мы будем расширять Γ, добавляя вместе с каждой формулой все эквивалентные ей, то за конечное число шагов мы получим все Φ — 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 Γ 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) $(B \wedge C) \in \Gamma \Leftrightarrow (B \in \Gamma$ *и* $C \in \Gamma)$*;*

(3) $(B \vee C) \in \Gamma \Leftrightarrow (B \in \Gamma$ *или* $C \in \Gamma)$*;*

(4) $(B \to C) \in \Gamma \Leftrightarrow (B \notin \Gamma$ *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 экавивалентности.*

Доказательство

- Рефлексивность.

  Пусть $\Box A \in \Gamma$. Т.к. $\Box A \to A$ — аксиома S5, она лежит в Γ (лемма 13.8 (0)). Тогда $\Gamma \vdash A$ по MP, 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. $\Box A \to \Box\Box A$ — аксиома S5, она лежит в Γ. Тогда $\Gamma \vdash \Box\Box A$ по MP, 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 Δ.

  Таким образом, $\Diamond\Box A \in \Gamma$. Кроме того, $(\Diamond\Box A \to A) \in \Gamma$ — это аксиома $S5$. Отсюда по MP 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. $\nvdash_{S5} A$, множество $\{\neg A\}$ непротиворечиво. По лемме 13.7 построим максимальное множество Γ, 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)*
$$M,\Delta \models B \Leftrightarrow B \in \Delta$$
для всех $B(P_1,\dots,P_n)$ *и* $\Delta \in W$.

Доказательство Индукция по длине B.

- B — переменная. Тогда утверждение верно по определению θ.
- $B = (C \vee D)$. Тогда по определению 5 лекции 12, предположению индукции и лемме 13.8 (3)
$$M,\Delta \models B \Leftrightarrow (M,\Delta \models C \text{ или } M,\Delta \models D) \Leftrightarrow (C \in \Delta \text{ или } D \in \Delta)$$
$$\Leftrightarrow (C \vee D) \in \Delta,$$
что и требовалось.
- Случаи связок $\wedge, \to, \neg$ разбираются аналогично (упражнение).
- $B = \Box C$. Проверим эквивалентность
$$M,\Delta \models \Box C \Leftrightarrow \Box C \in \Delta.$$
($\Leftarrow$) Пусть $\Box C \in \Delta$. Чтобы доказать $M,\Delta \models \Box C$, 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 $M,\Psi \models C$, по предположению индукции.

($\Rightarrow$) Предположим $\Box C \notin \Delta$ и докажем $M,\Delta \not\models \Box C$. Для этого надо построить $\Psi \in W$ такое, что $M,\Psi \not\models C$.

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
$$\vdash_{S5} \bigwedge_i D_i \to C,$$
откуда по правилу монотонности
$$(*) \qquad \vdash_{S5} \Box(\bigwedge_i D_i) \to \Box C.$$
Но по лемме 13.2 (8) (многократно)
$$\Box(\bigwedge_i D_i) \equiv \bigwedge_i \Box D_i.$$
Вспоминая, 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 MP следует $\Box C \in \Delta$. Это противоречит исходному предположению.

Итак, V непротиворечиво. Выберем максимальное Ψ, 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. $\Psi \in W$),

$M,\Psi \not\models C$ по предположению индукции, т.к. $C \notin \Psi$.

■

Наконец, из леммы 13.10 следует $W \not\models A$, что и требовалось. ■

Лекция 14

Полнота исчисления предикатов и ее следствия

Мощностью сигнатуры Ω (обозначение: $|\Omega|$) назовем мощность[29] 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 Ω. Тогда T имеет модель мощности $|\Omega|$ или счетную, если Ω конечна.

(2) Пусть T — непротиворечивая теория с равенством в сигнатуре Ω. Тогда T имеет нормальную модель мощности $\leq |\Omega|$ или не более, чем счетную, если Ω 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_Ω. 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 $|\widetilde{M}| \leq |M|$.[30] Таким образом, $\widetilde{M}$ — модель T нужной мощности. ■

Теорема 14.2. *(Гёделя о полноте)*

(1) Для теории T и замкнутой формулы A сигнатуры Ω

$$T \models A \Rightarrow T \vdash_{PC_\Omega} A.$$

(2) Для любой формулы A сигнатуры Ω

$$\models A \ \Rightarrow \vdash_{PC_\Omega} A.$$

($1^=$) Для теории с равенством T и замкнутой формулы A сигнатуры Ω

$$T \models_{\text{норм}} A \Rightarrow T \vdash_{PC_\Omega^=} A.$$

($2^=$) Для любой формулы A сигнатуры с равенством Ω

$$\models_{\text{норм}} A \ \Rightarrow \vdash_{PC_\Omega^=} A.$$

Доказательство (Не пишем индексы при $\vdash$.) (1) Если $T \nvdash A$, то $T \cup \{\neg A\}$ непротиворечива (по лемме 5.4; она переносится на предикатный случай). По теореме 14.1 эта теория выполнима, и значит, $T \not\models A$.

(2) По определению $\models A$ означает $\models \overline{\forall} A$. А в силу (1) для $T = \varnothing$ из $\models \overline{\forall} A$ следует $\vdash \overline{\forall} A$. Наконец, $\vdash \overline{\forall} A \to A$ (по аксиоме II.1 и правилу силлогизма). Тогда по MP получаем $\vdash A$.

($1^=$) Аналогично (1). Если $T \nvdash A$, то $T \cup \{\neg A\}$ непротиворечива в $PC_\Omega^=$, а потому нормально выполнима по теореме 14.1. Следовательно, $T \not\models_{\text{норм}} A$.

($2^=$) получается из ($1^=$) 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 Ω 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)*

[29] Пока что мы опираемся на интуитивное представление о мощности; некоторое уточнение будет дано в конце лекции.

[30] Это один из вариантов аксиомы выбора, о чем упомянем в конце лекции.

(1) *Если теория имеет конечные модели неограниченной мощности, то она имеет и бесконечную модель.*

(2) *Если теория в сигнатуре Ω 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 Ω^+, которая получается из Ω добавлением счетного множества новых констант $\{c_1, c_2, \ldots\}$. 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 Ω^+, добавив интерпретацию констант $c_1, \ldots, c_n$ 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 Ω, получаем бесконечную модель теории T.

(2) Аналогично (1), рассмотрим сигнатуру Ω^+ 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 $|\Omega^+| = k$.[31] 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 Ω, получим модель T мощности k. ■

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.

$$T := Th(\mathbb{N}) \cup \{c \neq 0,\ c \neq 1, \ldots,\ c \neq \underline{n}, \ldots\},$$

где $\underline{n}$ обозначает терм $\underbrace{1 + (1 + (1 + ..))}_{\text{n раз}}$.

В стандартной модели, очевидно, имеем $|\underline{n}|_{\mathbb{N}} = n$.

Как и в предыдущих теоремах, докажем выполнимость T, используя компактность. Для этого рассмотрим

$$T_n := Th(\mathbb{N}) \cup \{c \neq 0,\ c \neq 1, \ldots,\ c \neq \underline{n}\}.$$

Пусть M_n — модель $\mathbb{N}$ с интерпретацией $c_{M'} := n + 1$. Тогда $M_n \vDash T_n$. Таким образом, любая T_n выполнима.

По компактности, T выполнима, а по теореме Лёвенгейма — Сколема, она имеет не более, чем счетную модель M^+.

[31] Здесь мы используем следующий факт: если $|X| \leq |Y|$, то $|X \cup Y| = |Y|$. Чтобы его доказать, нужна аксиома выбора.

Заметим, что $M^+ \vDash Th(\mathbb{N})$ и $\mathbb{N} \vDash \underline{m} \neq \underline{n}$ при $m \neq n$. Поэтому и $M^+ \vDash \underline{m} \neq \underline{n}$ при $m \neq n$. Значит, M^+ бесконечна, и следовательно, счетна.

Кроме того, для всех n, $M^+ \vDash c \neq \underline{n}$, или[32]

$$M^+ \vDash c_{M^+} \neq \underline{n}.$$

Рассмотрим теперь M^+ в исходной сигнатуре арифметики. Обозначим эту модель через M. Имеем:

$$(*) \qquad M \vDash c_{M^+} \neq \underline{n}$$

для всех n, а также $M \vDash Th(\mathbb{N})$, т.е. $M \equiv \mathbb{N}$.

Наконец, докажем, что $M \ncong \mathbb{N}$. Предположим противное, и пусть $\alpha : M \cong \mathbb{N}$. Из $(*)$ по теореме 7.4 получаем

$$\mathbb{N} \vDash \alpha(c_{M^+}) \neq \underline{n},$$

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).

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)

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

(2) (схема аксиом свертывания)

$$\overline{\forall}\, \exists y \forall x\, (x \in y \leftrightarrow A(x, \ldots)).$$

Здесь $A(x, \ldots)$ — 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. $y = \{x \mid A(x, \ldots)\}$.

Предложение 14.7. *Теория $\mathcal{N}$ противоречива.*

Доказательство

Выведем противоречие в $\mathcal{N}$; это доказательство — формализация парадокса Рассела.

1. $\forall x\, (x \in a \leftrightarrow x \notin x) \to (a \in a \leftrightarrow a \notin a)$ — аксиома II.1 исчисления предикатов.
2. $(a \in a \leftrightarrow a \notin a) \to \exists y\, (y \in y \leftrightarrow y \notin y)$ — аксиома II.2 исчисления предикатов.
3. $\forall x\, (x \in a \leftrightarrow x \notin x) \to \exists y\, (y \in y \leftrightarrow y \notin y)$ — по правилу силлогизма из 1, 2.
4. $\exists y\, \forall x (x \in y \leftrightarrow x \notin x) \to \exists y\, (y \in y \leftrightarrow y \notin y)$ — 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, MP.
7. $(A \leftrightarrow \neg A) \to B \wedge \neg B$ — подстановочный пример тавтологии (с любыми A, B). В частности,

$$(a \in a \leftrightarrow a \notin a) \to B \wedge \neg B,$$

где B — любая замкнутая формула.

8. $\exists y\, (y \in y \leftrightarrow y \notin y) \to B \wedge \neg B$ — 7, второе правило Бернайса.
9. $B \wedge \neg B$ — 6, 8, MP. ■

[32] c_{M^+} — это элемент модели, а потому оцененный терм.

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). [33]

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 $\mathcal{N}$:

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

Введем обозначение

$$a \subseteq b := \forall x\, (x \in a \leftrightarrow x \in b)$$

("a — подмножество b"). Вот равносильная формулировка аксиомы объемности:

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

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):

$$(x, y) := \{\{x\}, \{x, y\}\}.$$

<u>Лемма</u> (в теории с аксиомами 1,2)

$$\vdash \overline{\forall}((x, y) = (x', y') \to x = x' \wedge y = y')).$$

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.

$$\overline{\forall}\, \forall x \exists y \forall z\, (z \in y \leftrightarrow (z \in x \wedge A(z, \ldots))).$$

В этой теории мы не можем строить произвольные множества вида
$\{x \mid A(x, \ldots)\}$. 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
$\{z \mid A(z, \ldots)\}$ 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*

$$Z \vdash (V \text{ — собственный класс}).$$

[33] См. также лекции Л.Д. Беклемишева "Аксиомы теории множеств" на http://www.mi-ras.ru/ bekl/logic2013.html

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 $\forall x A \to \exists x A$, 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 $\varnothing$.

Теперь мы можем последовательно (по индукции) определить натуральные числа:

$$0 := \varnothing,\ 1 := \{0\},\ 2 := \{0,1\}, \ldots,\ n+1 := n \cup \{n\}, \ldots$$

(определение фон Неймана). Т.е. получается $n = \{0, 1, \ldots, n-1\}$. Однако для построения множества всех натуральных чисел нужна дополнительная аксиома.

6. Аксиома бесконечности.

$$\exists x\, (0 \in x \wedge \forall y\, (y \in x \to (y \cup \{y\}) \in x)).$$

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 ω как наименьшее индуктивное множество:

$$\omega := \{y \mid \forall x\, (x \text{ индуктивно } \to y \in x)\}.$$

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 ω 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

$$f \text{ — функция} := \forall z (z \in f \to \exists x \exists y\, z = (x, y)).$$

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)*

$$Z \vdash \forall x \forall y\, (x \preceq y \wedge y \preceq x \to x \sim y).$$

Доказательство опускаем.[34]

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)*

$$Z \vdash \forall x\, |x| < |\mathcal{P}(x)|.$$

[34]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 $\{a\}$.

$x \not\sim \mathcal{P}(x)$ доказывается от противного.[35]

Предположим, что $f : x \longrightarrow \mathcal{P}(x)$ — 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

$$\exists y \forall z\, (z \in x \to |z \cap y| = 1)).$$

(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.

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 (зацикливание).
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 RAM 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 $(n_1, \ldots, n_k)$ записывается как $n_1 \sharp \ldots \sharp n_k$, где $\sharp$ — специальный символ (разделитель).

Рассматриваем частичные функции f из $\mathbb{N}^k$ в $\mathbb{N}$. Это записывается так: $f : \mathbb{N}^k \tilde{\longrightarrow} \mathbb{N}$. Если функция всюду определена (тотальна), пишем
$f : \mathbb{N}^k \longrightarrow \mathbb{N}$.

Также рассматриваем функции на словах. Если Δ — конечный алфавит, Δ^* — множество всех слов в нем, то рассматриваем частичные функции f из Δ^* в Δ^*. Обозначения аналогичны: $f : \Delta^* \tilde{\longrightarrow} \Delta^*$, $f : \Delta^* \longrightarrow \Delta^*$.

Область определения f обозначается $dom\, f$, область значений — $im\, f$. В частности, возможно, что $dom\, f = \varnothing$ (пустая функция).

Определение 64. Функция $f : \mathbb{N}^k \tilde{\longrightarrow} \mathbb{N}$ или $f : \Delta^* \tilde{\longrightarrow} \Delta^*$ 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: $M : x \models\Rightarrow f(x)$
- Если $x \notin dom\, f$, то M на входе x зацикливается. Это записывается так: $M : x \models\Rightarrow$

[35] Рассуждение похоже на парадокс Рассела. В истории было наоборот: теорема Кантора появилась раньше.

Разрешимость и перечислимость

Определение 65. Множество слов $A \subseteq \Delta^*$ называется *разрешимым*, если его характеристическая функция χ_A вычислима.

(Функция $\chi_A : \Delta^* \longrightarrow \{0,1\}$ 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 Δ^* 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 χ_A^- вычислима.

(Частичная функция $\chi_A^- : \Delta^* \tilde{\longrightarrow} \{1\}$ 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 $\mathbb{N} \longrightarrow \Delta^*$.

Теорема 15.5. *Существуют вычислимые биекции $\mathbb{N} \longrightarrow \mathbb{N}^k$ и $\mathbb{N} \longrightarrow \Delta^*$ (для конечного Δ), 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). $\varnothing$ разрешимо.

Пусть $A = im\, f$ для вычислимой $f : \mathbb{N} \longrightarrow \mathbb{N}$. Тогда χ_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). $\varnothing$ перечислимо.

Пусть $A \neq \varnothing$. Выберем $a_0 \in A$.

Пусть $\gamma : \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$ — вычислимая биекция (теорема 15.5). Пусть $\gamma(n) = (\alpha(n), \beta(n))$. Тогда α и β 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 $im\, f = A$. Действительно, включение $\subseteq$ очевидно (почему?).

Обратно, пусть $a \in A$. Тогда $\chi_A^-(a)$ вычислится через сколько-то (k) шагов. Т.к. γ — 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 $h : \Delta^* \longrightarrow \Delta^*$ — 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 $A = \varnothing$, все очевидно. Если $A = im\, f$ для вычислимой f, то $h[A] = im\,(h \cdot f)$. ∎

Универсальная вычислимая функция. Неразрешимость

Ключевой результат теории алгоритмов следующий:

Теорема 15.8. *(об универсальной вычислимой функции) Существует вычислимая функция $F : \mathbb{N}^2 \tilde{\longrightarrow} \mathbb{N}$ такая, что для любой вычислимой*
$f : \mathbb{N} \tilde{\longrightarrow} \mathbb{N}$ существует m такое, что

$$\text{для всех } n \ F(m,n) \simeq f(n).$$

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 φ_m вычислимую функцию с номером m, т.е.

$$\varphi_m(n) \simeq F(m,n).$$

Тогда всякая вычислимая $f : \mathbb{N} \tilde{\longrightarrow} \mathbb{N}$ совпадает с φ_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

$$K := dom\, d.$$

Ясно, что K полуразрешимо, т.е. перечислимо. Докажем, что $(-K)$ не перечислимо.

Допустим противное. Тогда $-K = dom\, \varphi_n$, где $\varphi_n = \chi^-_{-K}$. Тогда для любого x

$$x \notin K \Leftrightarrow x \in dom\, \varphi_n.$$

В частности,

$$n \notin K \Leftrightarrow n \in dom\, \varphi_n.$$

Но по определению K

$$n \in K \Leftrightarrow n \in dom\, \varphi_n.$$

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 Ω.

Лемма 15.10. *Множества Fm_Ω, CFm_Ω 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 $A_1 \sharp \ldots \sharp A_n$. Пусть Док$(T)$ — множество всех этих доказательств.

Заметим, что 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_Ω 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:

$$-[T] = -CFm_\Omega \cup (CFm_\Omega \backslash [T]).$$

Первое множество перечислимо, ввиду разрешимости CFm_Ω. Поскольку T полна,

$$CFm_\Omega \backslash [T] = \{A \in CFm_\Omega \mid T \vdash \neg A\}.$$

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, причем $\mathbb{N} \vDash T$. Тогда T неполна. В частности, PA неполна.*

Доказательство Допустим, что T полна. По теореме 15.12 $[T]$ разрешимо. Поскольку $\mathbb{N} \vDash T$, 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

$$n \in K \Leftrightarrow \mathbb{N} \vDash A(n).$$

Здесь $A(n)$ — формула, оцененная в $\mathbb{N}$. Заметим, что

$$\mathbb{N} \vDash A(n) \Leftrightarrow \mathbb{N} \vDash A(\underline{n}),$$

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), 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.