Введение в математическую логику (осень 2017)

В.Б. Шехтман

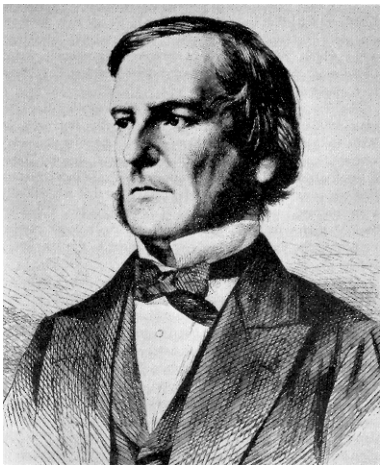
Лекция 1

ВВЕДЕНИЕ

Логика как раздел философии появилась более 2000 лет назад. Ее формализация и постепенное превращение в математическую дисциплину начались только в 19-м веке.

Отметим некоторые этапы.

1. "Алгебра логики"(Дж. Буль, 1847), "алгебра отношений"(А. Де Морган, 1860).



Джордж Буль

2. Появление новых аксиоматических теорий (неевклидова геометрия, арифметика Пеано).

3. Парадоксы теории множеств. Пример — парадокс Рассела:

с одной стороны, для любого свойства $\varphi(x)$ можно построить множество всех множеств с этим свойством, т.е. $\{x \mid \varphi(x)\}$;

с другой стороны, простое рассуждение показывает, что множество $\{x \mid x \notin x\}$ не существует.

Возможный выход — построить систему аксиом теории множеств, из которой не следует противоречие.

4. Программа Гильберта.

Давид Гильберт

(1) Построение формальных теорий для различных разделов математики.

(2) Доказательство непротиворечивости формальных теорий "финитными"методами, т.е. с использованием только конечных множеств и натуральных чисел.

(3) По возможности, построение полных теорий.

Теория *непротиворечива*, если ни для какого утверждения (записанного в ее языке) в T нельзя доказать одновременно A и $\neg A$.

Теория *полна*, если ни для всякого утверждения (в ее языке) в T можно доказать A или доказать $\neg A$.

Исследование формальных теорий финитными методами Гильберт назвал *метаматематикой*. В современной науке используется название *теория доказательств*; эти же задачи решаются (но не всегда финитными методами) в *теории моделей*.

В первом приближении, финитные рассуждения можно отождествить с доказательствами в формальной теории натуральных чисел - арифметики Пеано. Но возникает вопрос о непротиворечивости самой арифметики Пеано (2-я проблема Гильберта, 1900).

С мат. логикой связаны еще 3 проблемы Гильберта: 1 (проблема континуума), 6 (аксиоматизация физики) , 10 (решение диофантовых уравнений).

Континуум-гипотеза Кантора: всякое бесконечное подмножество $\mathbf{R}$ либо счетно, либо имеет мощность континуума.

4. Работы К. Гёделя 1930х гг. ("один из наиболее выдающихся мыслителей 20-го века" — Википедия).

Курт Гёдель

- Первая теорема о неполноте: арифметика Пеано (PA) неполна (в предположении, что она непротиворечива), и нельзя ее сделать непротиворечивой и полной, добавив конечное число новых аксиом.
- Вторая теорема о неполноте: непротиворечивость PA нельзя доказать в самой PA.
- Непротиворечивость континуум-гипотезы: исходя из общепринятых основных аксиом теории множеств, континуум-гипотезу нельзя опровергнуть (в предположении, что аксиоматика теории множеств непротиворечива).

В 1963 г. П. Коэн уставил, что доказать континуум-гипотезу в стандартной системе аксиом теории множеств также невозможно.

Таким образом, первые две проблемы Гильберта оказались неразрешимыми, а его программа обоснования математики требует корректировки.

5. Теория алгоритмов.

Логика изучает доказательства, а теория алгоритмов – вычисления. Эти процессы имеют много общего, а потому теория алгоритмов тесно связана с математической логикой. Она возникла в середине 1930х гг. почти одновременно в работах нескольких специалистов по мат. логике (А. Чёрча, А. Тьюринга, Э. Поста, К. Гёделя).

Теория алгоритмов непосредственно применяется в компьютерных науках. В различных областях математики также возникают алгоритмические проблемы. Вот некоторые примеры:

- Проблема Туэ: в полугруппе, заданной конечным числом образующих и базовых соотношений, определить, верно ли данное (не базовое) соотношение.

- Проблема гомеоморфии: по двум многообразиям, заданным как полиэдры, определить, гомеоморфны ли они.
- 10 проблема Гильберта: по данной системе алгебраических уравнений с целыми коэффициентами, определить, имеет ли она решение.

Все эти проблемы оказались алгоритмически неразрешимыми: невозможно составить программы на компьютере, которые бы отвечали на эти вопросы. Результаты о неразрешимости были получены специалистами по математической логике: для проблемы Туэ — в 1947 г. Э.Постом и А.А. Марковым (независимо), для проблемы гомеоморфии — в 1957 г. А.А. Марковым, для 10й проблемы Гильберта — в 1970 г. Ю.В. Матиясевичем.

Из более новых направлений в теории алгоритмов отметим теорию сложности вычислений. В этой области до сих пор остаются нерешенными многие проблемы. Самая известная из них - проблема перебора (P=NP?).

ЛОГИКА ВЫСКАЗЫВАНИЙ

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* пропозициональных переменных $Var = \{P_1, P_2, \ldots\}$ *Множество* пропозициональных формул Fm *строится из этих переменных, логических связок* $\wedge$, $\vee$, $\to$, $\neg$ *и скобок по индукции:*

(1) *Если* $P \in Var$, *то* $P \in Fm$.

(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. При записи формул обычно используются дополнительные сокращения: внешние скобки опускаются; для экономии внутренних скобок устанавливается приоритет связок : $\wedge$ сильнее $\vee$, $\vee$ сильнее $\to$,

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].

Определение 2 *Формула* B *называется* подформулой *формулы* A, *если* B *входит в* A *как подслово (т.е. состоит из всех знаков слова* A, *расположенных между какими-то двумя позициями).*

Подформулы можно также определить по индукции:

- *Подформулы переменной* P — *это* P.

- *Если* $C = (A \wedge B)$, $(A \vee B)$ *или* $(A \to B)$ *для формул* A, B, *то подформулы* C *— это* C, *а также все подформулы* A *и все подформулы* B.
- *Если* $C = \neg A$, *подформулы* C *— это* C *и все подформулы* A.

Определение 3 Оценкой (пропозициональных переменных) *называется любое отображение* $f : Var \longrightarrow \mathbb{B}$, *где* $\mathbb{B} = \{и,л\} = \{1, 0\}$.

Лемма 1.2 *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) $C = (A \wedge B)$, и полагаем $\overline{f}(C) = \min(\overline{f}(A), \overline{f}(B))$; и т. д. Единственность продолжения следует из единственности пары (A, B). ■

$\overline{f}(C)$ 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) $\overline{f}(A \wedge B) = \overline{f}(A) \circledwedge \overline{f}(B)$,

(3) $\overline{f}(A \vee B) = \overline{f}(A) \circledvee \overline{f}(B)$,

(4) $\overline{f}(A \to B) = \overline{f}(A) \circledrightarrow \overline{f}(B)$,

(5) $\overline{f}(\neg A) = \circledneg \overline{f}(A)$,

где $\circledvee$, $\circledwedge$, $\circleddash$, $\circledminus$ 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 1.2 является аналогом следующего утверждения: любое отображение базиса векторного пространства в другое пространство однозначно продолжается до линейного отображения.

Лемма 1.3 *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:

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

(по определению значения формулы и предположению индукции). ■

Определение 4 *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 5 *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[1]) $f_{\overrightarrow{x}}(P_i) = 0$ при $i > n$.*

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

Лекция 2

Определение 6 *Формула называется* тавтологией*, если при любой оценке она принимает значение 1.*

[1] На самом деле неважно, каковы значения при $i > n$.

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

Равносильность формул обозначается знаком $\sim$.
Из леммы 1.3 сразу получаем:

$$A(P_1, \ldots, P_n) \sim B(P_1, \ldots, P_n) \Leftrightarrow \varphi^n_A \equiv \varphi^n_B.$$

Также очевидно, что отношение равносильности рефлексивно, симметрично и транзитивно.
Обозначим через $\top$ формулу $P_1 \to P_1$, а через $\bot$ — формулу $P_1 \wedge \neg P_1$.

Лемма 2.1

(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. ■

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

Лемма 2.2

(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 2.3 *Для любого вектора* $\overrightarrow{x} \in \mathbb{B}^n$ *можно построить* сигнальную формулу $A_{\overrightarrow{x}}$*, 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 $\overrightarrow{x} = (x_1, \ldots, x_n)$ 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 2.4 *[Теорема о функциональной полноте] Любая булева функция отвечает формуле логики высказываний, точнее:*

для любой функции $\alpha : \mathbb{B}^n \longrightarrow \mathbb{B}$ *существует формула* $A(P_1, \ldots, P_n)$*, такая что* $\varphi_A \equiv \alpha$.[2]

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

[2] $\equiv$ обозначает совпадение функций при всех значениях аргумента. Часто пишут '=' вместо $\equiv$.

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

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,

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

Но, по определению 5, $\varphi_{A_{\overrightarrow{x}}}(\overrightarrow{y}) = f_{\overrightarrow{y}}(A_{\overrightarrow{x}})$, а по лемме 2.3,

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

Поэтому

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

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

Нормальные формы

Определение 8 *Литерал — это переменная или ее отрицание. Дизъюнктивная нормальная форма (ДНФ) — это дизъюнкция нескольких конъюнкций литералов.*

Сюда включаются частные случаи: когда конъюнкция литералов состоит из одного литерала; когда дизъюнкция берется по множеству, состоящему из одной формулы; а также случай пустой дизъюнкции — ее считаем равной $\bot$.

При доказательстве теоремы 2.4 мы установили, что любая формула равносильна некоторой ДНФ. В действительности, доказано более сильное утверждение: эта ДНФ имеет специальный вид.

Определение 9 Элементарная конъюнкция от переменных $P_1, \ldots, P_n$ *— это конъюнкция литералов, построенных из этих переменных, в которой каждая переменная встречается ровно 1 раз.* Совершенная дизъюнктивная нормальная форма *(СДНФ) от переменных* $P_1, \ldots, P_n$ *— это дизъюнкция элементарных конъюнкций от этих переменных, в которой каждая элементарная конъюнкция встречается не более 1 раза.*

Из определения ясно, что любая элементарная конъюнкция от $P_1, \ldots, P_n$ равносильна формуле вида $A_{\overrightarrow{x}}$, где $\overrightarrow{x}$ — двоичный вектор (см. лекцию 2).

Теорема 2.5

(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 конъюнкциях и 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 2.4.

(2) Докажем единственность (это почти уже сделано). Сначала отметим, что, строго говоря, даже формула $A_{\overrightarrow{x}}$ определена неоднозначно: в конъюнкции можно по-разному расставить скобки. Для единообразия можно считать, что скобки расставлены слева направо:

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

Запись $\bigvee\limits_{\overrightarrow{x}\in I} A_{\overrightarrow{x}}$ тоже не задает формулу однозначно, т.к. 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,

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

$$\Leftrightarrow \exists \overrightarrow{x} \in I \ \overrightarrow{y} = \overrightarrow{x} \text{ (по лемме 2.3)} \Leftrightarrow y \in I.$$

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 $P_1, \dots P_n$) как конъюнкцию элементарных дизъюнкций (причем пустая конъюнкция считается равной $\top$).

Справедлива следующая теорема

Теорема 2.6

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

(2) Каждая формула равносильна единственной СКНФ, с точностью до перестановок и расстановки скобок в конъюнкциях и дизъюнкциях.

Доказательство мы опускаем; оно аналогично теореме 2.5 или получается по двойственности — см. далее.

Двойственность

Определение 10 *Для формулы A, построенной из $\wedge, \vee, \neg$,* двойственная формула A^* *получается заменой всех $\wedge$ на $\vee$ и наоборот. Более формальное определение A^* — по индукции:*

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

Теорема 2.7 *Если $A \sim B$, то $A^* \sim B^*$. В частности, если $\vDash A$ (т.е. $A \sim \top$), то $\vDash \neg A^*$ (т.е. $A^* \sim \top^* \sim \bot$).*

Доказательство на лекции не приводилось и в программу не входит.

План его — такой. Сначала по индукции доказывается, что

$$A^*(P_1, \dots, P_n) \sim \neg A(\neg P_1, \dots, \neg P_n).$$

Затем можно проверить, что из $A(P_1, \dots, P_n) \sim B(P_1, \dots, P_n)$ следует $A(\neg P_1, \dots, \neg P_n) \sim B(\neg P_1, \dots, \neg P_n)$; это получается потому, что для любой оценки f, $f(A(\neg P_1, \dots, \neg P_n)) = f'(A(P_1, \dots, P_n))$, где $f'(P) = f(\neg P)$ для всех $P \in Var$.

И наконец, из $A(\neg P_1, \dots, \neg P_n) \sim B(\neg P_1, \dots, \neg P_n)$, очевидно, следует $\neg A(\neg P_1, \dots, \neg P_n) \sim \neg B(\neg P_1, \dots, \neg P_n)$.

Лекция 3

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 11 Булевой алгеброй *называется непустое множество с заданными на нем операциями и выделенными элементами* $(\mathcal{B}, \sqcup, \sqcap, -, \mathbf{0}, \mathbf{1})$[3], *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 2.2):

(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:

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

[3] 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 $\mathcal{B}$.

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 11 очевидны.

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

$$\mathit{2} = (\{0,1\}, \bigvee, \bigwedge, -, \ 0, \ 1),$$

где $x \bigvee y = \max(x, y)$, $x \bigwedge y = \min(x, y)$, $-x = 1 - x$ (см. лекцию 1). То, что *2* — булева алгебра, фактически доказано в лемме 2.2.

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 3.1 *Пусть E — произвольное множество. Тогда $(\mathcal{P}(E), \cup, \cap, -, \varnothing, E)$ (где $-A = E \backslash A$)— булева алгебра.*

Доказательство Доказательство проводится непосредственной проверкой булевых тождеств. При этом можно использовать равносильности из леммы 2.2.

Например, дистрибутивность

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

означает, что для любого $a \in E$

$$a \in (x \cup y) \cap z \text{ равносильно } a \in (x \cap z) \cup (y \cap z).$$

Чтобы это проверить, возьмем произвольное a и рассмотрим пропозициональные переменные P, Q, R, которые будут означать соответственно $a \in x$, $a \in y$, $a \in z$. Тогда $a \in (x \cup y) \cap z$ запишется как $(P \vee Q) \wedge R$, а $a \in (x \cap z) \cup (y \cap z)$ — как $(P \wedge R) \vee (Q \wedge R)$. Из леммы 2.2 мы знаем, что $(P \vee Q) \wedge R$ и $(P \wedge R) \vee (Q \wedge R)$ равносильны (т.е. одновременно истинны или одновременно ложны), что и требовалось.

Так же поступаем и с другими булевыми тождествами для $\mathcal{P}(E)$; они превращаются в равносильности из леммы 2.2, если знаки $\cup, \cap, -$ заменить соответственно на $\vee, \wedge, \neg$. ■

Определение 12 *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 $x, y \in \mathcal{A}$*

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

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

Как легко видеть, изоморфность - отношение эквивалентности между алгебрами[4].

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

Лемма 3.2 *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 коммутативности и ассоциативности: если $a = b \sqcap a,\ b = c \sqcap b$, то

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

Антисимметричность следует из коммутативности: если $a = a \sqcap b$ и $b = b \sqcap a$, то $a = b$.

$\mathbf{1} \sqcap a = a$ — по определению 11.

$\mathbf{0} \sqcap a = \mathbf{0}$ 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. Минимальные ненулевые элементы для этого порядка называются *атомами*; их может быть несколько, а может не быть вообще.

Справедлива следующая теорема Стоуна (в курсе не доказывается):

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

Теорема 3.3 *(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. Заметим, что не все булевы алгебры имеют вид $\mathcal{P}(E)$.

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

$$\{V \subseteq \mathbf{N} \mid V \text{ конечно или } \mathbf{N}\backslash V \text{ конечно}\}.$$

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

Однако никакая алгебра $\mathcal{P}(E)$ не может быть счетной: она конечна при конечном E и несчетна 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 $\sim A'$ и $B \sim B'$, то $\vee B \sim A' \vee B'$ и т.д.

Лемма 2.2 показывает, что $\mathcal{L}$ — булева алгебра. Эта алгебра счетна, и в ней, как можно показать, атомов нет (в отличие от примера 4).

Определение 13 Оценка в булевой алгебре $\mathcal{B}$ *— это отображение* $f : Var \longrightarrow \mathcal{B}$.

По аналогии с леммой 1.2, получаем:

Лемма 3.4 *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 1.2 (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 14 *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 ($\vDash$), как они определялись в лекции 2.

Аналогично лемме 2.1, получаем:

Лемма 3.5

(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 2.1, 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

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

где $a \leftrightarrow b := -a \sqcup b$.

Утверждение ($\Rightarrow$) очевидно: $a \leftrightarrow a = -a \sqcup a = \mathbf{1}$, $\mathbf{1} \sqcap \mathbf{1} = \mathbf{1}$ по определению 11.

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

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

Теперь заметим, что $-a \sqcup b = \mathbf{1} \Rightarrow a \leq b$. Действительно, если $-a \sqcup b = \mathbf{1}$, то

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

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

Лемма 3.6 *Для любой нетривиальной булевой алгебры $\mathcal{B}$ и формулы A*

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

Доказательство Пусть $\mathcal{B} \vDash A$. Возьмем оценку $f : Var \longrightarrow \mathit{2}$, и рассмотрим "такую же" оценку в $\mathcal{B}$, т.е. $f_0 : Var \longrightarrow \mathcal{B}$, где

$$f_0(P_i) = \mathbf{1} \Leftrightarrow f(P_i) = 1$$

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 $\sqcap$. 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

$$f_0(P_i) \approx f(P_i),$$

откуда по индукции имеем для любой формулы B

$$f_0(B) \approx f(B).$$

Здесь надо разбирать все случаи построения B, но это — рутинная проверка. Например, пусть $B = C \vee D$. Тогда $f_0(B) = f_0(C) \sqcup f_0(D)$, $f(B) = \max(f(C), f(D))$, и если $f_0(C) \approx f(C)$, $f_0(D) \approx f(D)$, то $f_0(C) \sqcup f_0(D) \approx \max(f(C), f(D))$. 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 $f_0(A) = \mathbf{1}$.

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

Лекция 4

Исчисление высказываний

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

Приведем одну из формулировок исчисления высказываний (CL).

Схемы аксиом

(1) $A \to (B \to A)$
(2) $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
(3) $A \wedge B \to A$
(4) $A \wedge B \to A$
(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 15 Доказательство *(или* вывод*) в CL — это конечная последовательность формул, каждая из которых — аксиома или получается из предыдущих по правилу MP.*

Точнее: доказательство — это такая последовательность формул $A_1, \ldots, A_n$, что для всех k $(1 \le k \le n)$
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, которая встречается в каком-нибудь доказательстве 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.

Очевидно, что для всякой теоремы A существует доказательство с последней формулой A.

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 15.

Определение 16 *Пусть Γ — какое-то множество пропозициональных формул.* Вывод из Γ *в CL — это конечная последовательность формул, каждая из которых — аксиома или принадлежит Γ или получается из предыдущих по правилу MP.*

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 4.1

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

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

Заменим в этом выводе каждую B_i на ее вывод Π_i:

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

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 $\{A_1, \ldots, A_n\} \vdash_{CL} B$ обычно пишут $A_1, \ldots, A_n \vdash_{CL} B$. Говорят также, что $\dfrac{A_1, \ldots, A_n}{B}$ — *производное правило CL.*

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

Лемма 4.2 *Всякое производное правило* CL *допустимо.*[5]

Доказательство Пусть $\Gamma = \{A_1, \ldots, A_n\} \vdash B$. 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 4.3 *(теорема*[6] *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 $\varnothing$):

---

[5] Обратное утверждение тоже верно, но в этом курсе мы его не доказываем.

[6] Конечно, это — не теорема нашего формального исчисления, а утверждение о его свойствах (“метатеорема”).

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:

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

Доказательство Нам понадобится лемма о булевых алгебрах.

Лемма 4.5 *В любой булевой алгебре*

(1) $a \sqcap \mathbf{0} = \mathbf{0}$;

(2) $a \sqcup \mathbf{1} = \mathbf{1}$;

(3) $a \leq b \Leftrightarrow a \leftarrowtail b = \mathbf{1}$;

(4) $a \leq a \sqcup b$;

(5) если $a \leq c$ *и* $b \leq c$, *то* $a \sqcup b \leq c$.

Доказательство (1) доказано в лемме 3.2.

(4) $a \sqcap (a \sqcup b) = a$ — поглощение.

(2) По (4) (и коммутативности) $\mathbf{1} \leq a \sqcup \mathbf{1}$. Отсюда $\mathbf{1} = a \sqcup \mathbf{1}$, т.к. $\mathbf{1}$ — наибольший элемент (лемма 3.2).

(3) Утверждение ($\Leftarrow$) мы получили при доказательстве леммы 3.5. Докажем ($\Rightarrow$). Пусть $a \leq b$, т.е. $a = a \sqcap b$. Тогда $a \rightarrowtail b = -a \sqcup b = -(a \sqcap b) \sqcup b = -a \sqcup -b \sqcup b = -a \sqcup \mathbf{1} = \mathbf{1}$ (по (2)).

(5) Если $a \sqcap c = a,\ b \sqcap c = b$, то $(a \sqcup b) \sqcap c = (a \sqcap c) \sqcup (b \sqcap c) = a \sqcup b$. ■

Доказываем теперь 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

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

По лемме 4.5 (3) $\mathbf{1} \leq a$, и значит, $a = \mathbf{1}$, т.к. $\mathbf{1}$ — наибольший элемент.

В случае (I) надо доказывать общезначимость всех 10 аксиом.

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

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

По лемме 4.5 (3) это равносильно

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

Теперь можно применить лемму 4.5(4).

Общезначимость аксиом 3,4,6,7,10 проверяется легко (упражнение). Аксиомы 2,8,9 рассмотрим на следующей лекции. ■

Лекция 5

Доказательство (теоремы 4.4; окончание)

Аксиома 2 Надо доказать

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

По лемме 4.5(3) это равносильно

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

т.е.

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

или (применяя закон Де Моргана)

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

Чтобы доказать это неравенство, используем лемму 4.5(5). Достаточно проверить два неравенства

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

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

Первое из них очевидно. Для проверки второго покажем

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

В самом деле,

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

Теперь снова можно применить лемму 4.5(5):

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

очевидно, а

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

тоже легко получается.

Аксиома 9 Надо доказать

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

Заметим, что

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

Значит, надо проверить, что

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

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

Аксиома 8 Надо доказать

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

или

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

или

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

или (если применить закон Де Моргана)

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

Теперь применим лемму 4.5(5).

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

очевидно; остается доказать

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

Обозначим правую часть этого неравенства через x. Запишем

$$-a = -a \sqcap (b \sqcup -b) = (-a \sqcap b) \sqcup (-a \sqcap -b).$$

Снова применим лемму 4.5(5).

$$-a \sqcap -b \leq x$$

очевидно; с другой стороны,

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

Заметим, что

$$b \sqcap -c \leq x,$$

и также

$$b \sqcap c \leq c \leq x.$$

Поэтому (опять по лемме 4.5(5))

$$b \leq x.$$

Это завершает доказательство неравенства $-a \leq x$. ■

Полнота исчисления высказываний

Теорема 5.1 *(Теорема о полноте CL)*
Все тавтологии выводимы в CL.

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

Лемма 5.2

(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 5.1 докажем от противного: предполагаем $\nvdash_{CL} A$ и доказываем *2* $\nvdash A$.

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 5.2(1)), и тогда $\vdash A$ — по аксиоме 10 и MP.

Лемма 5.3 *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.[7] ■

Лемма 5.4 *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 5.2(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 $B \in \Phi$: если $\neg B$ — подформула A, то и B — тоже подформула; а все подформулы A лежат

[7] 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, упорядоченное по включению.

в Φ. 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 5.2(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 5.2(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). ■

Закончим теперь доказательство теоремы. Исходное непротиворечивое множество $\neg A$ расширим до максимального Γ (лемма 5.3). 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 5.4.

- 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 5.4.

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

Применив доказанное утверждение к $F = \neg A$, получаем $f(\neg A) = 1$, и следовательно, $f(A) = 0$. Итак, $\mathit{2} \nvDash A$. ■

Теорема 5.5 *Для любой пропозициональной формулы A и нетривиальной булевой алгебры $\mathcal{B}$ следующие утверждения эквивалентны.*

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

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

(3) $\mathit{2} \vDash A$.

Доказательство (1)⇒(2) — это теорема корректности 4.4, (2)⇒(3) — лемма 3.6, а (3)⇒(1) — теорема полноты 5.1. ■

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 17 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,*
- $Pred_\Omega \neq \varnothing$,
- $\nu : Pred_\Omega \cup Fun_\Omega \longrightarrow \mathbf{N}_+ = \{1, 2, \ldots\}$.

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 18 *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:* $\vee, \wedge, \to, \neg$;
- *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 19 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 20 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 21 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* $(A \to B)$ *— 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*).*

Заметим, что 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.

Обозначения (для сигнатуры Ω):

Tm_Ω — множество всех термов,

Fm_Ω — множество всех формул,

AFm_Ω — множество всех атомарных формул.

Замечание 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.

С другой стороны, нельзя построить формулу, которая утверждает, что a нильпотентен: для этого потребуется возведение в натуральную степень и квантор по натуральным n:

$$\exists n \in \mathbf{N}\,(a^n = 0)$$

или же бесконечная дизъюнкция:

$$a = 0 \vee (a \cdot a) = 0 \vee ((a \cdot a) \cdot a) = 0 \vee \ldots$$

Но таких выражений в языке 1-го порядка нет. (Точное доказательство того, что нильпотентность не выразима в сигнатуре колец, будет обсуждаться позже.)

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 $f^n(t_1, \ldots, t_n)$ для единственного функционального символа f^n и термов $t_1, \ldots, t_n$.

(2) Каждая атомарная формула имеет вид $P^n(t_1, \ldots, t_n)$ для единственного предикатного символа P^n и термов $t_1, \ldots, t_n$.

(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 22 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*

- $c \in Const_\Omega \Rightarrow \mathcal{I}(c) \in \underline{M}$,
- $P^n \in Pred_\Omega \Rightarrow \mathcal{I}(P^n) : \underline{M}^n \longrightarrow \{0,1\}$
  (т.е. $\mathcal{I}(P^n)$ — n-местный предикат на $\underline{M}$*),*
- $f^n \in Fun_\Omega \Rightarrow \mathcal{I}(f^n) : \underline{M}^n \longrightarrow \underline{M}$
  (т.е. $\mathcal{I}(f^n)$ — 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 23 *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 *индукцией по длине определяется его* значение в модели M*; оно обозначается* $|t|_M$*.*

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

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

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

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

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 23:*

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

Доказательство Аналогично лемме 1.2. Индукцией по длине t доказываем, что $|t|_M$ определяется однозначно.

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

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

Определение 24 *Формула, не содержащая свободных переменных, называется* замкнутой*, или* предложением*.*

Таким образом, замкнутая атомарная формула имеет вид $P^n(t_1, \ldots, t_n)$, где $t_1, \ldots, t_n$ — замкнутые термы.

Для сигнатуры Ω множество всех замкнутых формул обозначается CFm_Ω.

Определение 25 *Для замкнутой атомарной формулы сигнатуры Ω ее* значение в модели M *той же сигнатуры определяется так:*

$$|P(t_1, \ldots, t_n)|_M = P_M(|t_1|_M, \ldots, |t_n|_M)$$

(где $P^n \in Pred_\Omega$, $t_1, \ldots, t_n \in CTm_\Omega$).

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

Доказательство Очевидное следствие леммы 6.2. ■

Значение произвольной замкнутой формулы в модели определяется по индукции; это определение отражает интуитивное понимание связок и кванторов. Точная формулировка его будет дана в лекции 8, 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 26 *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 $M \models A$.*

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

Лекция 7

Модели формул и теорий

Определение 27 *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:

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

Всякая модель 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*).

Модель M сигнатуры равенства называется *нормальной*, если для всех $m_1, m_2 \in M$

$$=_M (m_1, m_2) = \begin{cases} 1, & \text{если } m_1, m_2 \text{ совпадают,} \\ 0, & \text{иначе.} \end{cases}$$

Ясно, что в любой нормальной модели истинны все аксиомы Eq.

Определение 28 *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.

Для каждой теории T можно рассмотреть класс всех ее моделей[8]; он обозначается $Mod(T)$.

Определение 29 *Теории T_1, T_2 одной сигнатуры называются* эквивалентными (равносильными)*, если у них одни и те же модели, т.е. $Mod(T_1) = Mod(T_2)$; обозначение: $T_1 \sim T_2$.*

Двойственным образом, по модели строится теория:

Определение 30 *Элементарной теорией модели M называется множество всех замкнутых формул в ее сигнатуре, истинных в M; обозначение: $Th(M)$. Модели M_1, M_2 одной сигнатуры называются* элементарно эквивалентными*, если в них истинны одни и те же предложения, т.е. $Th(M_1) = Th(M_2)$; обозначение: $M_1 \equiv M_2$.*

Определение 31 *Теория 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 несовместная теория полна: из нее следуют все формулы той же сигнатуры. Если же теория совместна и полна, то либо $T \vDash A$, либо $T \vDash \neg A$, но не одновременно: в модели не могут быть истинны и A, и $\neg A$.

Пример 2 Чистая теория равенства Eq неполна. Чтобы в этом убедиться, рассмотрим формулу

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

Заметим, что в нормальной модели

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

(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 3 Теория $Eq \cup \{A_{=1}\}$ 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.

---

[8] Неформально говоря, классы — это "большие множества". Различие классов и множеств для нас сейчас не важно.

Точно так же теория $Eq \cup \{A_{=2}\}$ полна, где формула $A_{=2}$ утверждает, что в нормальной модели ровно 2 элемента. Ее можно построить как конъюнкцию $A_{\geq 2} \wedge A_{\leq 2}$, где

$$A_{\geq 2} =_{def} \exists x \exists y \neg(x = y),$$

$$A_{\leq 2} =_{def} \forall x \forall y \forall z (x = y \vee y = z \vee x = z).$$

Тогда для нормальной M

$$M \vDash A_{\geq 2} \Leftrightarrow |M| \geq 2,$$

$$M \vDash A_{\leq 2} \Leftrightarrow |M| \leq 2,$$

и следовательно,

$$M \vDash A_{=2} \Leftrightarrow |M| = 2.$$

Аналогичным образом строятся формулы $A_{\geq n},\ A_{\leq n}, A_{=n}$ и полные теории $Eq \cup \{A_{=n}\}$ для всех натуральных $n > 0$.

Лемма 7.1 *Для теории 1-гп порядка T следующие утверждения эквивалентны:*

(1) T полна;

(2) все модели T элементарно эквивалентны.

(3) для любой выполнимой теории $T' \supseteq T$ (той же сигнатуры) $T' \sim T$.

Утверждение (3) означает, что к теории нельзя добавить существенно новые аксиомы: получится либо эквивалентная, либо невыполнимая теория.

Доказательство
Будем доказывать импликации (1) $\Rightarrow$ (2), (2) $\Rightarrow$ (3), (3) $\Rightarrow$ (1). Во всех случаях рассуждаем от противного.

(1) $\Rightarrow$ (2). Пусть $M, M' \vDash T$, но $M \not\equiv M'$. Тогда для некоторой замкнутой формулы A, $M \vDash A$, $M' \nvDash A$ (т.е. $M' \vDash \neg A$).

Но это означает, что обе теории $T \cup \{A\},\ T \cup \{\neg A\}$ выполнимы. А тогда $T \nvdash \neg A,\ T \nvdash A$, а потому T неполна.

(2) $\Rightarrow$ (3). Пусть $T' \supseteq T$, T' выполнима, но $T' \not\sim T$. Из $T' \supseteq T$ следует, что все модели T' являются моделями T. Тогда из $T' \not\sim T$ получаем, что найдется модель $M_1 \vDash T$, такая что $M_1 \nvDash T'$.

С другой стороны, T' выполнима, поэтому найдется модель $M_2 \vDash T'$, и при этом $M_2 \vDash T$.

Итак, получаем модели $M_1, M_2 \vDash T$ такие, что $M_1 \nvDash T'$, $M_2 \vDash T'$. Тогда $M_1 \not\equiv M_2$.

(3) $\Rightarrow$ (1). Пусть T неполна, тогда $T \nvdash \neg A$, $T \nvdash A$ для некоторой замкнутой формулы A. Отсюда получаем выполнимые теории $T \cup \{A\}$, $T \cup \{\neg A\}$ и модели $M_1 \vDash T \cup \{A\}$, $M_2 \vDash T \cup \{\neg A\}$.

Тогда теория $T' = T \cup \{A\}$ содержит T и выполнима. Но T имеет модель M_2, которая не является моделью T' (т.к. $M_2 \vDash \neg A$). Поэтому $T' \not\sim T$. ■

Изоморфизмы

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

Определение 32 *Пусть M, M' — модели сигнатуры Ω. Отображение $\varphi : \underline{M} \longrightarrow \underline{M'}$ называется* изоморфизмом M на M', *если*

- φ — *биекция,*
- $\varphi(c_M) = c_{M'}$ *для всех* $c \in Const_\Omega$,
- $\varphi(f_M(m_1, \ldots, m_k)) = f_{M'}(\varphi(m_1), \ldots, \varphi(m_k))$ *для всех* $f^k \in Fun_\Omega$ *и* $m_1, \ldots, m_k \in \underline{M}$,
- $P_M(m_1, \ldots, m_k) = P_{M'}(\varphi(m_1), \ldots, \varphi(m_k))$ *для всех* $P^k \in Pred_\Omega$ *и* $m_1, \ldots, m_k \in \underline{M}$.

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

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

Лемма 7.2

(1) Если $\varphi : M \cong M'$ и $\psi : M' \cong M''$, то $\psi\varphi : M \cong M''$ ($\psi\varphi$ обозначает композицию).

(2) Если $\varphi : M \cong M'$, то $\varphi^{-1} : M' \cong M$.

Доказательство проводится непосредственной проверкой (упражнение).

Определение 33 *Модели M, M' называются* изоморфными *(обозначение: $M \cong M'$), если существует изоморфизм $\varphi : M \cong M'$.*

Очевидно, что $M \cong M$, а из леммы 7.2 получаем, что изоморфность моделей также обладает свойствами симметричности и транзитивности, т.е. $\cong$ задает отношение эквивалентности на классе всех моделей данной сигнатуры.

Понятно, что изоморфные модели должны быть элементарно эквивалентны; аккуратное доказательство будет дано на следующей лекции. Для него потребуется точное определение истинности.

Определение истинности в модели

Пусть M — модель сигнатуры Ω; предполагаем, что ее носитель $\underline{M}$ состоит из совершенно новых элементов, которые не являются словами в языке 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. [9]

Определение 34 *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 35 *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 $f^n \in Fun_\Omega$, $t_1, \ldots, t_n \in CTm_{\Omega\cup M}$.

Определение 36 *Для формулы C, оцененной в модели M, индукцией по длине 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* $|[m/a]A|_M = 1$,

[9] 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.

- $|\forall x[x/a]A|_M = 1 \Leftrightarrow$ *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.[10]

Заметим, что последние 2 пункта определения можно записать и так:

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

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

Как и в логике высказываний (леммы 1.2, 1.3), прежде, чем пользоваться этим определением, необходимо доказать его *корректность*. Мы отложим это доказательство до начала следующей лекции.

Пример 4 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 $\mathbf{R}$ и $\mathbf{Q}$ (с обычным пониманием нуля, единицы, сложения и умножения). Имеем:

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

т.к.

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

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

С другой стороны,

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

т.к.

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

для всех $r \in \mathbf{Q}$.

---

[10] Строго говоря, надо доказывать, что это — действительно формула; доказательство рутинное, по индукции. В определении 36 предполагается, что формула $\forall x[x/a]A$ замкнута, поэтому A не может содержать никаких свободных переменных, кроме a. И тогда $[m/a]A$ снова оказывается замкнутой.

Определимые предикаты

Определение 37 *k-местный предикат на множестве M — это отображение $M^k \longrightarrow \{0,1\}$. k-местное отношение на множестве M — это подмножество множества 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 38 Параметрами *формулы (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.

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 39 k-местный предикат, определимый формулой $A(b_1,\ldots,b_k)$ 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:

$$[m_1,\ldots,m_k/b_1,\ldots,b_k]A =_{def} [m_1/b_1]\ldots[m_k/b_k]A.$$

Примеры Рассмотрим опять сигнатуру колец и ее модель $\mathbf{N}$ — 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 $\exists x(b_1 + x = b_2)$:

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

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

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

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

Лекция 8

Определение истинности в модели: корректность

Докажем, что определение истинности в модели, данное на прошлой лекции (определение 26), корректно.

Лемма 8.1 *Для любой модели M существует единственное отображение $A \mapsto |A|_M$ оцененных в M формул в $\{0,1\}$, удовлетворяющее условиям из определения 26.*

Доказательство Аналогично лемме 1.2. "Длиной"формулы (в этом доказательстве) назовем число вхождений в нее логических связок и кванторов; значение $|A|_M$ определяем индукцией по длине A. Применим лемму 6.1 об однозначном анализе формул.

1. Если $A = P(t_1, \ldots, t_n)$ — 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. ■

Преобразование значений термов и формул при изоморфизме

Лемма 8.2 *Пусть M, M' — модели сигнатуры Ω, $\varphi : M \cong M'$.*

(1) Если $t(b_1, \ldots, b_k) \in Tm_\Omega$, то

$$\varphi(|[m_1, \ldots, m_k/b_1, \ldots, b_k]t|_M) = |[\varphi(m_1), \ldots, \varphi(m_k)/b_1, \ldots, b_k]t|_{M'},$$

или, в упрощенной записи:

$$\varphi(|t(m_1, \ldots, m_k)|_M) = |t(\varphi(m_1), \ldots, \varphi(m_k))|_{M'}.$$

(2) Если $A(b_1, \ldots, b_k) \in Fm_\Omega$, то

$$|[m_1, \ldots, m_k/b_1, \ldots, b_k]A|_M = |[\varphi(m_1), \ldots, \varphi(m_k)/b_1, \ldots, b_k]A|_{M'},$$

или, в упрощенной записи:

$$|A(m_1, \ldots, m_k)|_M = |A(\varphi(m_1), \ldots, \varphi(m_k))|_{M'}.$$

Доказательство Еще упростим обозначения: пишем $\overrightarrow{b}$ вместо $b_1, \ldots, b_k$, $\overrightarrow{m}$ — вместо $m_1, \ldots, m_k$ и $\varphi\overrightarrow{m}$ — вместо $\varphi(m_1), \ldots, \varphi(m_k)$.

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

(1.1) (базис индукции). $t(\overrightarrow{b}) = b_i$.

Тогда

$$t(\overrightarrow{m}) = [m_i/b_i]b_i = m_i,\ |t(\overrightarrow{m})|_M = [m_i|_M = m_i$$

(определение значений термов, опр. 35); аналогично,

$$t(\varphi\overrightarrow{m}) = \varphi(m_i),\ |t(\varphi\overrightarrow{m})|_{M'} = [\varphi(m_i)|_{M'} = \varphi(m_i).$$

Теперь утверждение (1) очевидно.

(1.2) (базис индукции). $t(\overrightarrow{b}) = c$, $c \in Const_\Omega$.

Тогда t не содержит переменных, и $t(\overrightarrow{m}) = t(\varphi\overrightarrow{m}) = c$. По определению 35,

$$|t(\overrightarrow{m})|_M = c_M,\ |t(\varphi\overrightarrow{m})|_{M'} = c_{M'}.$$

Равенство (1) превращается в

$$\varphi(c_M) = c_{M'},$$

а это верно по определению изоморфизма (опр. 32)

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

$$t(\overrightarrow{m}) = f(t_1(\overrightarrow{m}), \ldots, t_n(\overrightarrow{m})),$$

$$(*) \qquad |t(\overrightarrow{m})|_M = f_M(|t_1(\overrightarrow{m})|_M, \ldots, |t_n(\overrightarrow{m})|_M)$$

(опр. 35). Аналогично,

$$t(\varphi\overrightarrow{m}) = f(t_1(\varphi\overrightarrow{m}), \ldots, t_n(\varphi\overrightarrow{m})),$$

откуда, по опр. 35 и предположению индукции,

$$(**)\ |t(\varphi\overrightarrow{m})|_{M'} = f_{M'}(|t_1(\varphi\overrightarrow{m})|_{M'}, \ldots, |t_n(\varphi\overrightarrow{m})|_{M'}) = f_{M'}(\varphi(|t_1(\overrightarrow{m})|_M), \ldots, \varphi(|t_n(\overrightarrow{m})|_M)).$$

Но, по определению изоморфизма,

$$(***)\ f_{M'}(\varphi(|t_1(\overrightarrow{m})|_M), \ldots, \varphi(|t_n(\overrightarrow{m})|_M)) = \varphi(f_M(|t_1(\overrightarrow{m})|_M, \ldots, |t_n(\overrightarrow{m})|_M)).$$

Теперь из (**),(***), и (*) получаем:

$$|t(\varphi\overrightarrow{m})|_{M'} = \varphi(|t(\overrightarrow{m})|_M).$$

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

(2.1) (базис индукции) $A = P(t_1, \ldots, t_n)$ — атомарная ($P^n \in Pred_\Omega$, $t_1, \ldots, t_n \in Tm_\Omega$).

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

$$A(\overrightarrow{m}) = P(t_1(\overrightarrow{m}), \ldots, t_n(\overrightarrow{m})),$$

$$(*) \qquad |A(\overrightarrow{m})|_M = P_M(|t_1(\overrightarrow{m})|_M, \ldots, |t_n(\overrightarrow{m})|_M)$$

(опр. 35). Аналогично,

$$|A(\varphi\overrightarrow{m})|_{M'} = P_{M'}(|t_1(\varphi\overrightarrow{m})|_{M'}, \ldots, |t_n(\varphi\overrightarrow{m})|_{M'})$$

откуда

$$(**) \qquad |A(\varphi\overrightarrow{m})|_{M'} = P_{M'}(\varphi(|t_1(\overrightarrow{m})|_M), \ldots, \varphi(|t_n(\overrightarrow{m})|_M)),$$

ввиду (1). Но, по определению изоморфизма,

$$(***) \; P_{M'}(\varphi(|t_1(\overrightarrow{m})|_M), \ldots, \varphi(|t_n(\overrightarrow{m})|_M)) = P_M(|t_1(\overrightarrow{m})|_M, \ldots, |t_n(\overrightarrow{m})|_M)).$$

Теперь из (**),(***), и (*) получаем:

$$|A(\varphi\overrightarrow{m})|_{M'} = |A(\overrightarrow{m})|_M.$$

(2.2) $A = (B \wedge C)$. В этом случае, по определению истинности

$$|A(\overrightarrow{m})|_M = min(|B(\overrightarrow{m})|_M, |C(\overrightarrow{m})|_M),$$

$$|A(\varphi\overrightarrow{m})|_{M'} = min(|B(\varphi\overrightarrow{m})|_{M'}, |C(\varphi\overrightarrow{m})|_{M'}).$$

Но, по предположению индукции,

$$|B(\overrightarrow{m})|_M = |B(\varphi\overrightarrow{m})|_{M'}, \; |C(\overrightarrow{m})|_M = |C(\varphi\overrightarrow{m})|_{M'},$$

а потому и

$$|A(\overrightarrow{m})|_M = |A(\varphi\overrightarrow{m})|_{M'}.$$

(2.3) $A = (B \vee C)$,
(2.4) $A = (B \to C)$,
(2.5) $A = \neg B$.
Эти случаи аналогичны (2.2), и мы их пропускаем.
(2.6) $A = \exists x[x/a]B$.

Вспомним, что в формулировке (2) имеется $\overrightarrow{b}$ — список, *содержащий* все параметры A. Переменная a, конечно же, не входит в A, но случайно может оказаться в этом списке $\overrightarrow{b}$. Поэтому разбираем два случая.

(2.6.1) a не входит в $\overrightarrow{b}$.

Заметим, что B содержит те же параметры, что и A, и еще, возможно, a. Поэтому мы можем записать B как $B(\overrightarrow{b}, a)$. Заменив $\overrightarrow{b}$ на $\overrightarrow{m}$ в формуле A, получаем:

$$A(\overrightarrow{m}) = \exists x[x/a]B(\overrightarrow{m}, a)$$

Теперь, по определению истинности,

$$|A(\overrightarrow{m})|_M = \max_{q\in M} |B(\overrightarrow{m}, q)|_M,$$

и аналогично,

$$(*) \qquad |A(\varphi\overrightarrow{m})|_{M'} = \max_{q'\in M'} |B(\varphi\overrightarrow{m}, q')|_{M'},$$

По предположению индукции, для формулы $B(\overrightarrow{b}, a)$ имеем:

$$|B(\overrightarrow{m}, q)|_M = |B(\varphi\overrightarrow{m}, \varphi(q))|_{M'}.$$

Поэтому

$$|A(\overrightarrow{m})|_M = \max_{q\in M} |B(\varphi\overrightarrow{m}, \varphi(q))|_{M'}.$$

Но φ — биекция, поэтому все элементы из M' записываются как $\varphi(q)$, где $q \in M$. Тогда

$$|A(\overrightarrow{m})|_M = \max_{q'\in M'} |B(\varphi\overrightarrow{m}, q')|_{M'} = |A(\varphi\overrightarrow{m})|_{M'}$$

— по (*).

(2.6.2) a входит в $\overrightarrow{b}$.

Удалим a из $\overrightarrow{b}$; полученный список переменных обозначим $\overrightarrow{b}^-$. Соответственно уменьшим список элементов $\overrightarrow{m}$ до $\overrightarrow{m}^-$: а именно, если $a = b_i$, то $\overrightarrow{m}^-$ получается из $\overrightarrow{m}$ удалением i-го элемента.

Как мы уже заметили, a не входит в A, поэтому для оцененной формулы $A(\overrightarrow{m})$ имеем:

$$A(\overrightarrow{m}) = [\overrightarrow{m}/\overrightarrow{b}]A = [\overrightarrow{m}^-/\overrightarrow{b}^-]A.$$

Теперь для $\overrightarrow{m}^-$ и $\overrightarrow{b}^-$ можно использовать случай (2.6.1):

$$|[\overrightarrow{m}^-/\overrightarrow{b}^-]A|_M = |[\varphi\overrightarrow{m}^-/\overrightarrow{b}^-]A|_{M'}.$$

И опять же, поскольку a не входит в A,

$$[\varphi\overrightarrow{m}^-/\overrightarrow{b}^-]A = [\varphi\overrightarrow{m}/\overrightarrow{b}]A.$$

В итоге снова получаем

$$|[\overrightarrow{m}/\overrightarrow{b}]A|_M = |[\varphi\overrightarrow{m}/\overrightarrow{b}]A|_{M'},$$

что и требовалось.

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

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

Теорема 8.3 *Если $M \cong M'$, то $M \equiv M'$.*

Доказательство Пусть M, M' — изоморфные модели сигнатуры Ω. Если A — замкнутая формула данной сигнатуры, можно применить лемму 8.2(2) с любым списком параметров (в том числе, с пустым; тогда $k = 0$):

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

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

В этом разделе мы докажем необходимое условие определимости предиката в модели. Согласно определению 39, определимый k-местный предикат имеет вид A_M для некоторой формулы $A(b_1, \ldots, b_k)$; это означает, что

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

или, в сокращенной записи,

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

Как и в алгебре, *автоморфизм* модели — это ее изоморфизм на себя. Из леммы 8.2 сразу же получаем:

Теорема 8.4 *Если φ - автоморфизм модели сигнатуры Ω, $A(b_1, \ldots, b_k)$ — формула той же сигнатуры, то для всех $m_1, \ldots, m_k \in M$*

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

Таким образом, определимый в M предикат инвариантен при всех автоморфизмах 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 8.4 означает, что определимые отношения инвариантны при автоморфизмах:

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

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

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

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

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

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

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

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.

Лекция 9

Стандартные теории равенства и нормальные модели

Напомним (см. лекцию 7), что через $A(b_1, \ldots, b_n)$ мы обозначаем формулу, у которой все параметры содержатся среди $b_1, \ldots, b_n$. При этом, если $m_1, \ldots, m_n$ — элементы некоторой модели, то $A(m_1, \ldots, m_n)$ обозначает результат подстановки $[m_1, \ldots, m_n/b_1, \ldots, b_n]A$. Если же $x_1, \ldots, x_n$ — какие-то (различные) связанные переменные, не входящие в A, то результат подстановки $[x_1, \ldots, x_n/b_1, \ldots, b_n]A$ будем обозначать через $A(x_1, \ldots, x_n)$. (Заметим, что выражение $A(x_1, \ldots, x_n)$ — не формула, но может быть частью формулы: в частности, $\forall x_1 \ldots \forall x_n A(x_1, \ldots, x_n)$ — формула, согласно определению 21.)

Лемма 9.0 *Пусть $A(b_1, \ldots, b_n)$ — формула сигнатуры Ω, $x_1, \ldots, x_n$ — (различные) связанные переменные, не входящие в A. Тогда для любой*

модели M сигнатуры Ω

$M \vDash \forall x_1 \ldots \forall x_n A(x_1, \ldots, x_n) \Leftrightarrow$ *для всех* $m_1, \ldots, m_n \in M$ $M \vDash A(m_1, \ldots, m_n)$,

$M \vDash \exists x_1 \ldots \exists x_n A(x_1, \ldots, x_n) \Leftrightarrow$ *найдутся* $m_1, \ldots, m_n \in M$ *такие, что* $M \vDash A(m_1, \ldots, m_n)$,

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

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

И тогда

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

Но

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

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

(2) $M \vDash \forall x_2 \ldots \forall x_n A(m_1, x_2, \ldots, x_n) \Leftrightarrow$

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

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

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

Запишем эти аксиомы в сокращенном виде:

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

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

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

Лемма 9.1 *Если M — нормальная модель сигнатуры с равенством Ω, то $M \vDash Eq_\Omega$.*

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

По лемме 9.0, 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 $m_1 = m'_1 \wedge \ldots \wedge m_n = m'_n$).

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:

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

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

Лемма 9.2 *(о нормализации)*

(1) $\widetilde{M}$ корректно определена.

(2) Для любого терма $t(b_1,\dots,b_k)\in Tm_\Omega$ *и для всех* $m_1,\dots,m_k\in M$

$$|t(\widetilde{m_1},\dots,\widetilde{m_k})|_{\widetilde{M}}=|t(\widetilde{m_1,\dots,m_k})|_M.$$

(3) Для любой формулы $A(b_1,\dots,b_k)\in Fm_\Omega$ *и для всех* $m_1,\dots,m_k\in M$

$$|A(\widetilde{m_1},\dots,\widetilde{m_k})|_{\widetilde{M}}=|A(m_1,\dots,m_k)|_M.$$

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

Доказательство (1) 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 9.1, $M\vDash\overrightarrow{m}=\overrightarrow{m'}$, где $\overrightarrow{m}=(m_1,\dots,m_k)$, $\overrightarrow{m'}=(m_1',\dots,m_k')$. Как уже мы видели в лемме 9.1, из аксиомы (II) 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 (III) получаем: $M\vDash P(\overrightarrow{m})\leftrightarrow P(\overrightarrow{m'})$, т.е. $P_M(\overrightarrow{m})=P_M(\overrightarrow{m'})$.

(2) Доказательство аналогично лемме 8.2, с тем отличием, что теперь $\varphi: m\mapsto\overrightarrow{m}$ —- не биекция. Однако φ — "сильный гомоморфизм", т.е. удовлетворает остальным условиям определения изоморфизма (сравните определение 32 и определение $\widetilde{M}$).

(3) Доказательство тоже аналогично лемме 8.2. Оно ведется индукцией по длине A.

Если A — атомарная, то особый случай — когда A имеет вид $b_1=b_2$. Имеем:

$$M\vDash m_1=m_2\Leftrightarrow m_1\approx m_2\Leftrightarrow\widetilde{m_1}=\widetilde{m_2}\Leftrightarrow\widetilde{M}\vDash\widetilde{m_1}=\widetilde{m_2}$$

по определению $\approx$ и т.к. $\widetilde{M}$ нормальна.

Случаи логических связок — легкие. Рассмотрим случай $A=\exists x[x/a]B$; запишем A как $A(\overrightarrow{b})$, где $a\notin\overrightarrow{b}$. Это соответствует случаю (2.6.1) в доказательстве леммы 8.2. Проследив это доказательство, мы видим, что все рассуждения можно сохранить и в нашей ситуации (теперь M' заменяется на $\widetilde{M}$). Действительно, биективность φ использовалась там для того, чтобы представить все элементы M' как φ-образы элементов из M, т.е. в этом месте достаточно сюръективности. Но и теперешнее φ сюръективно.

Случай $A(\overrightarrow{b})=\exists x[x/a]B$, где $a\in\overrightarrow{b}$, разбирается аналогично (2.6.2) из доказательства леммы 8.2.

(4) Очевидное следствие (3): для замкнутой A

$$M \vDash A \Leftrightarrow \widetilde{M} \vDash A.$$

■

Теорема 9.3 *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 9.2, $M \equiv \widetilde{M}$, $M' \equiv \widetilde{M'}$. Поэтому $\widetilde{M}, \widetilde{M'} \vDash T$. Т.к. эти модели нормальны, по условию они изоморфны. Следовательно, $\widetilde{M} \equiv \widetilde{M'}$ (теорема 8.3). В итоге имеем $M \equiv M'$.

■

Примеры 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 $\mathbf{Z}_6$.

3. 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.

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

Теория конечной модели

Теорема 9.4 *Элементарная теория конечной модели сильно категорична.*

Доказательство Пусть M — конечная модель сигнатуры Ω. Доказательство сильной категоричности $Th(M)$ проведем для случая, когда Ω также конечна.

Мы построим формулу A_M, которая полностью описывает M, следующим образом.

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

$$A =_{def} \exists v_1 \ldots \exists v_n [v_1 \ldots v_n / a_1 \ldots a_n] \psi_M,$$

где

$$\psi_M =_{def} \bigwedge_{1 \le i < j \le n} (a_i \neq a_j) \wedge \forall v_{n+1} \bigvee_{i=1}^{n} (v_{n+1} = a_i) \wedge$$

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

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

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

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

Здесь мы используем обычное сокращение: $a \neq b =_{def} \neg(a = b)$.

Для доказательства теоремы 9.4 потребуется лемма, которую мы докажем на следующей лекции:

Лемма 9.5 *Для нормальной модели M' сигнатуры Ω*

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

■

Лекция 10

Доказательство (леммы 10.2).

($\Leftarrow$) Заметим, что

$$M \vDash \psi_M(m_1, \ldots, m_n).$$

Действительно,

$$\psi_M(m_1, \ldots, m_n) = \bigwedge_{1 \le i < j \le n} (m_i \neq m_j) \wedge \forall v_{n+1} \bigvee_{i=1}^{n} (v_{n+1} = m_i) \wedge$$

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

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

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

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

Проверим, что все 6 членов этой конъюнкции (все они — тоже конъюнкции, кроме второго) истинны в M. Действительно, первый член утверждает, что все m_i различны (напомним, что M нормальна), второй — что всякий элемент из M равен одному из m_i. Истинность третьего члена означает, что для всякой константы c, $M \vDash c = m_i$, если c_M равно m_i — но это очевидно, по определению истинности (см. определения 35, 36). Аналогично, для четвертого члена имеем: $M \vDash f^k(m_{i_1}, \ldots, m_{i_k}) = m_j$, если $f^k_M(m_{i_1}, \ldots, m_{i_k})$ равно m_j.

Пятый и шестой члены также очевидны.

Теперь по лемме 9.0, 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 8.3.

($\Rightarrow$) Предположим, что $M' \vDash A_M$ и построим изоморфизм M на M'. Снова по лемме 9.0, найдутся $m'_1, \ldots, m'_n \in M'$, для которых

$$M' \vDash \psi_M(m'_1, \ldots, m'_n).$$

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

$$\bigwedge_{1 \le i < j \le n} (m'_i \neq m'_j) \wedge \forall v_{n+1} \bigvee_{i=1}^{n} (v_{n+1} = m'_i) \wedge$$

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

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

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

$$\bigwedge\{\neg P^k(m'_{i_1},\dots,m'_{i_k}) \mid P^k \in Pred_\Omega,\ M \not\models P^k(m_{i_1},\dots,m_{i_k})\}.$$

Докажем, что отображение φ, переводящее каждый m_i в m'_i — искомый изоморфизм.

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

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

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

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

5. $M' \models P^k(m'_{i_1},\dots,m'_{i_k}) \Leftrightarrow M \models P^k(m_{i_1},\dots,m_{i_k})$. Это получается из 5-го и 6-го членов.

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

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

Доказательство (теоремы 9.4)

Докажем сильную категоричность $Th(M)$.

Пусть $M' \models Th(M)$. По доказанной лемме, $A_M \in Th(M)$, поэтому $M' \models A_M$. Тогда $M' \cong M$ — по той же лемме. ■

Следствие 10.1 *Если M — конечная модель и $M' \equiv M$, то $M' \cong M$.*

Доказательство Если $M' \equiv M$, то $M' \models Th(M)$. Тогда, по теореме 9.4, $M' \cong M$. ■

Общезначимость и равносильность

Определение 40 *Замкнутые формулы A, B (в некоторой сигнатуре) называются* равносильными, *если формула $A \leftrightarrow B$ общезначима (см. определение 26).*

Как и в логике высказываний, равносильность обозначается знаком $\sim$. И мы имеем аналог леммы 2.1:

Лемма 10.2 *$A \sim B$ тогда и только тогда, когда для любой модели M (данной сигнатуры) $|A|_M = |B|_M$.*

Лемма 10.3 *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 $A \sim \forall xA$.

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

Доказательство (1) следует из леммы 9.0: 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 10.2).

(2) — очевидное следствие определения истинности. Действительно, в этом случае $M \vDash \forall xA$ (где $\forall xA$ 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 41 *Пусть $b_1, \ldots, b_n$ — список параметров формулы A в алфавитном порядке*[11]*, 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 9.0, 10.3 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.

---

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

Определение 42 *Формула A называется* общезначимой*, если общезначимо ее универсальное замыкание.*

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

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

Таким образом, по лемме 9.0

$$\vDash A(\overrightarrow{a}) \Leftrightarrow \text{ для любой модели } M \text{ и } \overrightarrow{m} \text{ из } M,\ M \vDash A(\overrightarrow{m}),^{12}$$

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

Лемма 10.4

(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 10.3 и транзитивность $\sim$. ■

Пусть теперь $F(P_1, \ldots, P_n)$ — пропозициональная формула, построенная из пропозициональных переменных $P_1, \ldots, P_n$, а $B_1, \ldots, B_n$ — формулы сигнатуры Ω. При замене в F каждой P_i на B_i получится формула сигнатуры Ω, которую мы обозначим $F(B_1, \ldots, B_n)$. Такая формула называется *подстановочным примером* формулы F.

Лемма 10.5 *(Лемма о тавтологиях) Подстановочные примеры тавтологий общезначимы.*

Доказательство Если даны $B_1, \ldots, B_n$, то для каждой $F(P_1, \ldots, P_n)$ будем обозначать $F(B_1, \ldots, B_n)$ через SF.

Формулы B_i запишем как $B_i(a_1, \ldots, a_k)$, считая, что список свободных переменных $a_1, \ldots, a_k$ содержит все параметры этих формул.

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

---

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

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

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

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

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: $SF = SF_1 \wedge SF_2$,

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

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

и можно применить предположение индукции.

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

Список литературы

1. Н.К.Верещагин, А.Х. Шень. Языки и исчисления. М., МЦНМО, 2012.