МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in
ЛЕКЦИИ УЧЕНЫХ МГУ

ВВЕДЕНИЕ В МАТЕМАТИЧЕСКУЮ ЛОГИКУ И ТЕОРИЮ АЛГОРИТМОВ

ШЕХТМАН
ВАЛЕНТИН БОРИСОВИЧ

МЕХМАТ МГУ

КОНСПЕКТ ПОДГОТОВЛЕН СТУДЕНТАМИ, НЕ ПРОХОДИЛ ПРОФ. РЕДАКТУРУ И МОЖЕТ СОДЕРЖАТЬ ОШИБКИ. СЛЕДИТЕ ЗА ОБНОВЛЕНИЯМИ НА VK.COM/TEACHINMSU.

ЕСЛИ ВЫ ОБНАРУЖИЛИ ОШИБКИ ИЛИ ОПЕЧАТКИ, ТО СООБЩИТЕ ОБ ЭТОМ, НАПИСАВ СООБЩЕСТВУ VK.COM/TEACHINMSU.

Содержание

Лекция 1

Введение

Три вопроса, которыми занималась математическая логика:

1) Что и как можно доказать?

2) Как можно вычислить?

3) Что считать истинным?

Из этих вопросов выросли теория доказательств, теория алгоритмов и теория моделей.

Логика произошла из философии. Её родоначальником считается Аристотель. В старом смысле логику можно определить как науку о рассуждениях. Тогда она аналогична грамматике – науке о правильном употреблении языка. Аристотель придумал правила, по которым можно рассуждать так, чтобы не допускать ошибки, – силлогистику.

Приведём пример. Если любое A есть B, а любое B есть C, то любое A есть C.

Через много столетий логика стала приобретать очертания более точной науки. Вклад в это сделал Лейбниц (XVII век), у него была идея об универсальном формальном языке и формальном исчислении для решения математических задач. Он определил две основные задачи (сейчас это две основные проблемы теории алгоритмов):

1) нахождение всех истинных утверждений (проблема порождения);

2) ответ на вопрос об истинности данного утверждения (проблема разрешения).

Дальше развитие логике дал Джордж Буль (1815-1864). Он предложил рассматривать высказывания как формальные элементы некоторой алгебры – алгебры высказываний (1847).

В XIX веке логика стала постепенно превращаться в математическую дисциплину. Де Морган придумал алгебру отношений (1860). Фреге придумал кванторы и логику предикатов (1879).

Одновременно с этим происходил другой процесс, не имеющий непосредственного отношения к логике. В самой математике появились аксиоматические теории.

История построения аксиоматической теории геометрии:

1) Евклид, III век до н. э. (неформальная);

2) Гильберт, 1899 (почти формальная);

3) Тарский, 1957 (формальная).

Кроме этого, из анализа проблемы независимости 5-го постулата Евклида удалось построить неевклидовы геометрии.

Построение аксиоматической теории арифметики: Пеано, 1889 (почти формальная).

Построение аксиоматической теории анализа (с действительными числами): Дедекинд, 1876 (почти формальная).

С построением аксиоматической теории множеств возникла серьёзная проблема. В XIX веке была предложена неудачная формализация, которая приводила к парадоксам. Наиболее знаменитый из них – это парадокс Рассела, приведём его. Рассмотрим множество всех множеств, которые не являются элементами самих себя: $R = \{x \mid x \notin x\}$. Является ли это множество собственным элементом, то есть $R \in R$?

Несложно показать, что утверждение $R \in R$ и утверждение $R \notin R$ приводят к противоречиям. Значит, такое множество R нельзя строить. Тогда возникает вопрос: какие правильные принципы построения множеств? В итоге пришли к современным аксиоматикам теории множеств, одна из них – аксиоматика Цермело-Френкеля с аксиомой выбора (ZFC, 1925).

Тогда возник естественный вопрос: как надо действовать, чтобы формальные теории не приводили к противоречию? И вообще, как обосновывать математику, если выдвигаемые принципы неверны в смысле логики? Гильберт предложил следующую программу:

1) построение формальных теорий для различных разделов математики;

2) доказательство непротиворечивости формальных теорий «финитными» методами, то есть с использованием только конечных множеств и натуральных чисел;

3) по возможности построение полных теорий.

Определение 1.1. Теория T *непротиворечива*, если ни для какого утверждения A (записанного в её языке) в T нельзя доказать одновременно A и не-A.

Определение 1.2. Теория T *полна*, если для всякого утверждения A (в её языке) в T можно доказать A или доказать не-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).

Программа Гильберта не была реализована. Этому помешали появившиеся результаты Гёделя (приводим из ниже).

1) Теорема о неполноте утверждает, что арифметика Пеано (PA) неполна.

2) Вторая теорема Гёделя утверждает, что нельзя доказать непротиворечивость арифметики в самой арифметики: $PA \nvdash$ непротиворечивость PA.

Следующий результат Гёделя касался проблемы 1 Гильберта: доказать или опровергнуть континуум-гипотезу (CH). Эта гипотеза утверждает, что всякое бесконечное подмножество множества действительных чисел либо счётно, либо континуально. Кантор много лет посвятил решению этой проблемы, но у него ничего не вышло. Гёдель доказал (1940), что в теории Цермело-Френкеля с аксиомой выбора нельзя опровергнуть континуум гипотезу: $ZFC \nvdash \neg CH$. Позже Коэн доказал (1963), что в теории Цермело-Френкеля с аксиомой выбора нельзя и доказать континуум гипотезу: $ZFC \nvdash CH$.

В заключение скажем о нерешённой проблеме. Это проблема из списка 7 проблем тысячелетия, поставленных в начале XXI века. Она называется проблема перебора: совпадают ли два класса сложности $P = NP$?

Логика высказываний. Пропозициональные формулы

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

Определение 1.3. Фиксируем счётное множество символов – так называемых *пропозициональных переменных* $Var = \{P_1, P_2, \ldots\}$. Множество *пропозициональных формул*, обозначаемое Fm, строится из этих переменных, логических связок $\wedge$, $\vee$, $\to$, $\neg$ и скобок по индукции, как наименьшее множество, удовлетворяющее условиям:

1) если $A \in Var$, то $A \in Fm$;
2) если $A, B \in Fm$, то $(A \wedge B) \in Fm$;
3) если $A, B \in Fm$, то $(A \vee B) \in Fm$;
4) если $A, B \in Fm$, то $(A \to B) \in Fm$;
5) $A \in Fm \ \Rightarrow \ \neg A \in Fm$.

Таким образом, формулы представляют собой конечные последовательности знаков, то есть некоторые слова в алфавите, состоящем из переменных, связок и скобок.

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

1) $C \in Var$;
2) $\exists! A\colon\ C = \neg A$;
3) $\exists! A, B\colon\ C = (A \wedge B)$;
4) $\exists! A, B\colon\ C = (A \vee B)$;
5) $\exists! A, B\colon\ C = (A \to B)$.

Упражнение 1.1. Доказать однозначность анализа для бесскобочной записи формул, то есть когда вместо записей $(A \vee B)$, $(A \wedge B)$, $(A \to B)$ используются записи $\vee AB$, $\wedge AB$, $\to AB$.

Лекция 2

Логика высказываний. Пропозициональные формулы (продолжение)

Приведём упрощающие соглашения, позволяющие записывать формулы короче.

1) Можно опускать внешние скобки: вместо записи формулы $(A \vee B)$ пишем $A \vee B$.

2) Устанавливаем приоритет связок: самая сильная связка – отрицание $\neg$, затем идёт конъюнкция $\wedge$, потом – дизъюнкция $\vee$, а последняя связка – это импликация $\to$. То есть можно, например, вместо записи формулы $P_1 \to (P_2 \vee P_3)$ использовать запись $P_1 \to P_2 \vee P_3$.

Введём ещё полезную для сокращения связку: $\leftrightarrow$ – эквиваленция: $(A \leftrightarrow B) \coloneqq \coloneqq ((A \to B) \wedge (B \to A))$.

Подформулы

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

Определение 2.1. Определим отношение $A \preccurlyeq B$ (A – *подформула* B) индукцией по длине B.

1) Если $B \in Var$, то $A \preccurlyeq B \Leftrightarrow A = B$.

2) Если $B = (C \vee D)$ для формул C, D, то $A \preccurlyeq B \Leftrightarrow (A = B$, или $A \preccurlyeq C$, или $A \preccurlyeq D)$.

3) Если $B = (C \wedge D)$ для формул C, D, то $A \preccurlyeq B \Leftrightarrow (A = B$, или $A \preccurlyeq C$, или $A \preccurlyeq D)$.

4) Если $B = (C \to D)$ для формул C, D, то $A \preccurlyeq B \Leftrightarrow (A = B$, или $A \preccurlyeq C$, или $A \preccurlyeq D)$.

5) Если $B = \neg C$, то $A \preccurlyeq B \Leftrightarrow (A = B$ или $A \preccurlyeq C)$.

Замечание 2.1. Можно ещё определить отношение $A \prec B$ (A – *собственная подформула* B): A – подформула B и $A \neq B$.

Определение 2.2. *Подсловом* слова $a_1 \dots a_n$ (где $a_1, \dots, a_n$ – буквы) называется его часть, расположенная между какими-то двумя позициями, то есть слово вида $a_i \dots a_j$, где $i < j$. *Подформулой* формулы A называется любое её подслово, которое является формулой.

Упражнение 2.1. Доказать эквивалентность определений (2.1) и (2.2).

Оценки и значения формул

Определение 2.3. *Оценкой (пропозициональных переменных)* называется любое отображение $f : Var \to \mathbb{B}$, где $\mathbb{B} \coloneqq \{0, 1\}$.

Значение 0 соответствует понятию «ложь», а значение 1 – понятию «истина».

Лемма 2.1 (Лемма о продолжении оценки на формулы)**.**
$\forall$ *оценки* $f : Var \to \mathbb{B}$ $\exists!$ *отображение* $\overline{f}$: $Fm \to \mathbb{B}$ *такое, что* $\forall A, B \in Fm$:
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) $\overline{f}(\neg A) = 1 \Leftrightarrow \overline{f}(A) = 0$;
5) $\overline{f}(A \to B) = 1 \Leftrightarrow (\overline{f}(A) = 0$ *или* $\overline{f}(B) = 1)$.

Замечание 2.2. 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) $\overline{f}(\neg A) = 1 - \overline{f}(A)$;
5) $\overline{f}(A \to B) = \overline{f}(\neg A \vee B) = \max(1 - \overline{f}(A), \overline{f}(B))$.

Доказательство:
Для формулы A длины 1 лемма верна, так как тогда $A \in Var$ и $\overline{f}(A) = f(A)$.
Надо доказать шаг индукции: если $\overline{f}$ однозначно определена на формулах длины $< n$, то $\overline{f}$ однозначно определяется на формулах длины n.
По лемме (1.1) об однозначном анализе формул каждая формула C записывается одним из следующих способов:
1) $C \in Var$, тогда $\overline{f}(C) = f(C)$);
2) $C = \neg A$, тогда $\overline{f}(C) = 1 - \overline{f}(A)$;
3) $C = (A \vee B)$, тогда $\overline{f}(C) = \max(\overline{f}(A), \overline{f}(B))$;
4) $C = (A \wedge B)$, тогда $\overline{f}(C) = \min(\overline{f}(A), \overline{f}(B))$;
5) $C = (A \to B)$, тогда $\overline{f}(C) = \max(1 - \overline{f}(A), \overline{f}(B))$.
Таким образом, по индукции лемма доказана. □

Договоримся далее для краткости вместо записи продолжения оценки $\overline{f}$ использовать запись f, подразумевая продолжение оценки на используемых формулах.

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

Доказательство этой леммы выполняется тривиально с помощью индукции по длине формулы.

Определение 2.4. $A \in Fm$ *– тавтология (тождественно истинная формула)*, если $f(A) = 1$ при всех оценках f.

Определение 2.5. $A \in Fm$ *выполнима*, если $\exists$ оценка f: $f(A) = 1$.

A – тавтология $\Leftrightarrow$ $\neg A$ не выполнима.
A выполнима $\Leftrightarrow$ $\neg A$ – не тавтология.
Тавтологии выражают законы логики.
Введём обозначения: $\top := (P_1 \to P_1)$ – тождественно истинная формула, $\bot := \neg\top$ – тождественно ложная формула.

Булевы функции

Определение 2.6. Мы говорим, что формула A *построена из переменных* $P_1, \dots, P_n$, если в ней нет других переменных (но не обязательно все $P_1, \dots, P_n$ в ней встречаются).

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

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

Дадим точное определение φ_A^n.

Определение 2.7. Для каждого двоичного вектора $\vec{x} = (x_1, \dots, x_n) \in \mathbb{B}^n$ построим оценку $f_{\vec{x}} : Var \to \mathbb{B}$ такую, что

$$f_{\vec{x}}(P_i) = \begin{cases} x_i, \text{ если } i \leq n \\ 0, \text{ если } i > n \end{cases}.$$

Тогда $\varphi_A^n : \mathbb{B}^n \to \mathbb{B}$ – *n-местная булева функция* для $A(P_1, \dots, P_n)$ определяется следующим образом:

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

Приведём пример. Чтобы полностью задать булеву функцию для формулы $P_1 \leftrightarrow P_2$, построим для неё таблицу истинности.

$P_1 \leftrightarrow P_2$	P_1	P_2
1	1	1
0	0	1
0	1	0
1	0	0

Можем переформулировать определение тавтологии с использованием булевой функции: $A(P_1, \dots, P_n)$ – тавтология $\Leftrightarrow\ \varphi_A^n \equiv 1$.

Равносильность формул

Определение 2.8. $A \sim B$ *(A и B равносильны)*, если $\forall f \quad f(A) = f(B)$.

Из леммы (2.2) сразу получаем, что формулы от одних и тех же переменных равносильны тогда и только тогда, когда их булевы функции тождественно равны: $A(P_1, \dots, P_n) \sim B(P_1, \dots, P_n) \ \Leftrightarrow\ \varphi_A^n \equiv \varphi_B^n$.

Лемма 2.3.
1) $(A \sim B) \ \Leftrightarrow\ (A \leftrightarrow B)$ *– тавтология.*
2) A *– тавтология* $\Leftrightarrow\ A \sim \top$.

Доказательство:
Докажем пункт (1) этой леммы.

$A \leftrightarrow B$	A	B
1	1	1
0	0	1
0	1	0
1	0	0

Из выписанной таблицы истинности видно, что $f(A) = f(B) \Leftrightarrow f(A \leftrightarrow B) = 1$, значит, $(A \sim B) \Leftrightarrow (A \leftrightarrow B)$ – тавтология.

Докажем пункт (2) этой леммы.

$\top$ – тавтология, значит, A – тавтология $\Leftrightarrow A \sim \top$. □

Выпишем основные равносильные формулы, из которых можно получить все остальные равносильные формулы.

Лемма 2.4.

1) $A \wedge B \sim B \wedge A$; $A \vee B \sim B \vee A$ *(коммутативность).*

2) $(A \wedge B) \wedge C \sim A \wedge (B \wedge C)$; $(A \vee B) \vee C \sim A \vee (B \vee C)$ *(ассоциативность).*

3) $A \wedge A \sim A$; $A \vee A \sim A$ *(идемпотентность).*

4) $(A \vee B) \wedge C \sim (A \wedge C) \vee (B \wedge C)$; $(A \wedge B) \vee C \sim (A \vee C) \wedge (B \vee C)$ *(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) $(A \to B) \sim (\neg A \vee B)$.

Упражнение 2.2. Доказать лемму (2.4).

Функциональная полнота

Пусть дана некоторая функция $\varphi : \mathbb{B}^n \to \mathbb{B}$. Всегда ли можно утверждать, что она отвечает некоторой формуле, то есть $\varphi^n_A \equiv \varphi$? Другими словами, всегда ли можно построить формулу по заданной таблице истинности? Покажем, что это действительно так.

Лемма 2.5 (Лемма о сигнальной формуле)**.** *Пусть* $\vec{x} \in \mathbb{B}^n$. *Тогда* $\exists$ *формула* $A_{\vec{x}}(P_1, \ldots, P_n)$ *такая, что*

$$\varphi^n_{A_{\vec{x}}}(\vec{y}) = \begin{cases} 1, \text{ если } \vec{y} = \vec{x} \\ 0, \text{ если } \vec{y} \neq \vec{x} \end{cases}.$$

Доказательство:

Введём обозначения: $P^1_i := P_i$, $P^0_i := \neg P_i$. Тогда пусть $A_{\vec{x}} := P^{x_1}_1 \wedge P^{x_2}_2 \wedge \ldots \wedge P^{x_n}_n$ (из-за ассоциативности неважно, как расставить скобки). Покажем, что эта формула является искомой.

По определению $\varphi^n_{A_{\vec{x}}}(\vec{y}) = f_{\vec{y}}(A_{\vec{x}})$.

$f_{\vec{y}}(A_{\vec{x}}) = 1 \Leftrightarrow f_{\vec{y}}(P_1^{x_1}) = f_{\vec{y}}(P_2^{x_2}) = \ldots = f_{\vec{y}}(P_n^{x_n}) = 1.$

$$f_{\vec{y}}(P_i^{x_i}) = \begin{cases} f_{\vec{y}}(P_i), \text{ если } x_i = 1 \\ 1 - f_{\vec{y}}(P_i), \text{ если } x_i = 0 \end{cases} = \begin{cases} y_i, \text{ если } x_i = 1 \\ 1 - y_i, \text{ если } x_i = 0 \end{cases}.$$

Таким образом, $f_{\vec{y}}(P_i^{x_i}) = 1 \Leftrightarrow y_i = x_i$, значит, $\varphi^n_{A_{\vec{x}}}(\vec{y}) = 1 \Leftrightarrow \vec{y} = \vec{x}$. □

Теорема 2.1 (Теорема о функциональной полноте)**.** $\forall$ *булевой функции* $\alpha : \mathbb{B}^n \to \mathbb{B}$ $\exists$ *формула* $A(P_1, \ldots, P_n)$ *такая, что* $\varphi^n_A \equiv \alpha$.

Доказательство:

Рассмотрим сначала тривиальный случай: пусть $\alpha \equiv 0$. Тогда $A \coloneqq \bot$.

Теперь рассмотрим случай $\alpha \not\equiv 0$, то есть формула должна быть выполнима. Тогда $A \coloneqq \bigvee\{A_{\vec{x}} \mid \alpha(\vec{x}) = 1\}$. Покажем, что $\varphi^n_A \equiv \alpha$.

$\varphi^n_A(\vec{y}) = 1 \Leftrightarrow \exists \vec{x}\colon\ (\alpha(\vec{x}) = 1$ и $\varphi^n_{A_{\vec{x}}}(\vec{y}) = 1) \Leftrightarrow \exists \vec{x}\colon\ (\alpha(\vec{x}) = 1$ и $\vec{x} = \vec{y}) \Leftrightarrow \alpha(\vec{y}) = 1$. □

Таким образом, количество неэквивалентных формул от n переменных равно количеству булевых функций от n переменных.

Лекция 3

Совершенная дизъюнктивная нормальная форма (СДНФ)

Определение 3.1. *Литерал* – это пропозициональная переменная P_i или её отрицание $\neg P_i$.

Определение 3.2. *Элементарная конъюнкция от переменных* $P_1, \dots, P_n$ – это конъюнкция литералов от этих переменных, в которой каждая переменная встречается ровно 1 раз.

С точностью до эквивалентности всякую элементарную конъюнкцию можно записать в виде $\bigwedge\limits_{i=1}^{n} P_i^{x_i}$.

$A_{\vec{x}} = \bigwedge\limits_{i=1}^{n} P_i^{x_i}$ – сигнальная формула для двоичного вектора $\vec{x} = (x_1, \dots, x_n)$.

Определение 3.3. *Совершенная дизъюнктивная нормальная форма (СДНФ)* от $P_1, \dots, P_n$ – это дизъюнкция $\bigvee\limits_{\vec{x} \in I} A_{\vec{x}}$ элементарных конъюнкций $A_{\vec{x}}$ от $P_1, \dots, P_n$, в которой элементарные конъюнкции не повторяются.

Если I состоит из 1 элемента, то СДНФ – это одна элементарная конъюнкция.

Если $I = \varnothing$, то СДНФ $\coloneqq \bot$.

С точностью до перестановок и применения скобок СДНФ однозначна для заданного множества I.

Количество различных СДНФ для векторов x длины n равно количеству подмножеств множества двоичных векторов длины n, то есть 2^{2^n}.

Теорема 3.1.

1) Любая формула от $P_1, \dots, P_n$ равносильна некоторой СДНФ от $P_1, \dots, P_n$.

2) Такая СДНФ единственна с точностью до порядка членов дизъюнкции и скобок.

Доказательство:

Докажем пункт (1) этой теоремы. Из доказательства теоремы (2.1) о функциональной полноте понятно, что для любой формулы A можно построить СДНФ $\bigvee\limits_{\vec{x} \in I} A_{\vec{x}}$, причём $A \sim \bigvee\limits_{\vec{x} \in I} A_{\vec{x}}$.

Докажем пункт (2) этой теоремы. Введём обозначение $A_I \coloneqq \bigvee\limits_{\vec{x} \in I} A_{\vec{x}}$. Надо показать, что если $A_I \sim A_J$, то $I = J$.

$\varphi^n_{A_I}(\vec{y}) = 1 \;\Leftrightarrow\; f_{\vec{y}}(A_I) = 1 \;\Leftrightarrow\; \exists \vec{x} \in I\colon\; f_{\vec{y}}(A_{\vec{x}}) = 1 \;\Leftrightarrow\; \exists \vec{x} \in I\colon\; \vec{x} = \vec{y} \;\Leftrightarrow\; \vec{y} \in I.$

Таким образом, из $A_I \sim A_J$ следует, что $\vec{y} \in I \;\Leftrightarrow\; \vec{y} \in J$, значит, $I = J$. □

Совершенная конъюнктивная нормальная форма (СКНФ)

Можно вместо совершенной дизъюнктивной нормальной формы рассматривать совершенную конъюнктивную нормальную форму.

Определение 3.4. *Элементарная дизъюнкция* от переменных $P_1, \dots, P_n$ – это дизъюнкция литералов от этих переменных, в которой каждая переменная встречается ровно 1 раз.

С точностью до эквивалентности всякую элементарную дизъюнкцию можно записать в виде $\bigvee\limits_{i=1}^{n} P_i^{x_i}$. Введём обозначение: $B_{\vec{x}} = \bigvee\limits_{i=1}^{n} P_i^{x_i}$.

Определение 3.5. *Совершенная конъюнктивная нормальная форма (СКНФ)* от $P_1, \dots, P_n$ – это конъюнкция $\bigwedge\limits_{\vec{x} \in I} B_{\vec{x}}$ элементарных дизъюнкций $B_{\vec{x}}$ от $P_1, \dots, P_n$, в которой элементарные дизъюнкции не повторяются.

Если I состоит из 1 элемента, то СКНФ – это одна элементарная дизъюнкция.

Если $I = \varnothing$, то СКНФ $:= \top$.

Теорема 3.2.

1) Любая формула от $P_1, \dots, P_n$ равносильна некоторой СКНФ от $P_1, \dots, P_n$.

2) Такая СКНФ единственна с точностью до порядка членов конъюнкции и скобок.

Упражнение 3.1. Доказать теорему (3.2).

Принцип двойственности

Определение 3.6. Определим *операцию построения двойственной формулы* $A \mapsto A^*$ следующим образом:

1) избавиться от всех импликаций: $B \to C \sim \neg B \vee C$;

2) заменить в полученной записи дизъюнкции на конъюнкции, а конъюнкции – на дизъюнкции.

Утверждение 3.1 (Принцип двойственности)**.** $A \sim B \;\Rightarrow\; A^* \sim B^*$.

Упражнение 3.2. Доказать утверждение (3.1) о принципе двойственности.

Сформулируем следствие из утверждения (3.1) о принципе двойственности.

Утверждение 3.2. *A – тавтология $\Rightarrow$ $\neg A^*$ – тавтология.*

Доказательство:

A – тавтология, значит, $A \sim \top$, то есть $A \sim P_1 \vee \neg P_1$.

Тогда $A^* \sim P_1 \wedge \neg P_1$, то есть $A^* \sim \bot$, значит $\neg A^*$ – тавтология. □

Булевы алгебры

Определение булевой 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 3.7. *Булева алгебра* – это непустое множество с заданными на нём операциями и выделенными элементами: $(\mathcal{B}, \sqcup, \sqcap, -, \mathbb{0}, \mathbb{1})$, где

$\mathcal{B} \neq \varnothing$;
$\sqcup : \mathcal{B}^2 \to \mathcal{B}$ – сумма (объединение);
$\sqcap : \mathcal{B}^2 \to \mathcal{B}$ – произведение (пересечение);
$- : \mathcal{B} \to \mathcal{B}$ – дополнение;
$\mathbb{0}, \mathbb{1} \in \mathcal{B}$.

Причём $\forall x, y, z \in \mathcal{B}$ должны выполняться следующие аксиомы:
1) $x \sqcap y = y \sqcap x$, $x \sqcup y = y \sqcup x$ (коммутативность);
2) $(x \sqcap y) \sqcap z = x \sqcap (y \sqcap z)$; $(x \sqcup y) \sqcup z = x \sqcup (y \sqcup z)$ (ассоциативность);
3) $x \sqcap x = x$; $x \sqcup x = x$ (идемпотентность);
4) $(x \sqcup y) \sqcap z = (x \sqcap z) \sqcup (y \sqcap z)$; $(x \sqcap y) \sqcup z = (x \sqcup z) \sqcap (y \sqcup z)$ (дистрибутивность);
5) $(x \sqcup y) \sqcap x = x$, $(x \sqcap y) \sqcup x = x$ (поглощение);
6) $x \sqcap -x = \mathbb{0}$, $x \sqcup \mathbb{0} = x$,
$x \sqcup -x = \mathbb{1}$, $x \sqcap \mathbb{1} = x$ (свойства $\mathbb{0}$ и $\mathbb{1}$);
7) $-(x \sqcup y) = (-x \sqcap -y)$; $-(x \sqcap y) = (-x \sqcup -y)$ (законы де Моргана);
8) $- - x = x$ (закон двойного дополнения)

Определение 3.8. *Носитель булевой алгебры* – множество её элементов.

Упражнение 3.3. Доказать, что в определении булевой алгебры можно постулировать только равенства (1), (2), (4), (5), (6), а остальные равенства (3), (7), (8) выводятся из них.

В качестве примера покажем, как выводится равенство $x = x \sqcap x$ из пункта (3), используя равенства (5) и (6):
$x = (x \sqcap \mathbb{0}) \sqcap x = x \sqcap x$.

Приведём примеры булевых алгебр.

1) Тривиальный пример булевой алгебры – одноэлементная алгебра (она обозначается *1*). В ней $\mathbb{0} = \mathbb{1}$ и все операции дают $\mathbb{1}$, тогда выполнение аксиом из определения (3.7) очевидно.

2) Двухэлементная булева алгебра *2*. Её носителем является множество $\mathbb{B} = \{0, 1\}$. Операции в ней устроены следующим образом: $x \sqcap y \coloneqq \min(x, y)$, $x \sqcup y \coloneqq \max(x, y)$, $-x \coloneqq 1 - x$. Выделенные элементы: $\mathbb{0} \coloneqq 0$, $\mathbb{1} \coloneqq 1$. По лемме (2.4) аксиомы из определения (3.7) выполняются.

3) Алгебра множеств. Пусть $E \neq \varnothing$, рассмотрим $\mathcal{P}(E) = \{X \mid X \subseteq E\}$ – множество всех подмножеств множества E. Определим операции следующим образом: $X \sqcup Y \coloneqq X \cup Y$, $X \sqcap Y \coloneqq X \cap Y$, $-X \coloneqq E \backslash X$. Выделенные элементы: $\mathbb{0} \coloneqq \varnothing$, $\mathbb{1} \coloneqq E$.

Утверждение 3.3. *$\mathcal{P}(E)$ – булева алгебра.*

Доказательство:

Нужно проверить 8 свойств булевой алгебры. Но на самом деле можно использовать аналогию с формулами логики высказываний. Приведём пример для дистрибутивности.

$(X \sqcup Y) \sqcap Z = (X \sqcap Z) \sqcup (Y \sqcap Z)$ – хотим проверить.

$a \in (X \cup Y) \cap Z \Leftrightarrow a \in (X \cap Z) \cup (Y \cap Z)$ – хотим проверить.

Пусть P обозначает, что $a \in X$, Q обозначает, что $a \in Y$, R обозначает, что $a \in Z$. Тогда $a \in X \Leftrightarrow f(P) = 1$, $a \in Y \Leftrightarrow f(Q) = 1$, $a \in Z \Leftrightarrow f(R) = 1$. Значит, $a \in (X \cup Y) \cap Z \Leftrightarrow f((P \vee Q) \wedge R) = 1$, $a \in (X \cap Z) \cup (Y \cap Z) \Leftrightarrow f((P \wedge R) \vee (Q \wedge R)) = 1$.

$(P \vee Q) \wedge R \sim (P \wedge R) \vee (Q \wedge R)$, значит, $f((P \vee Q) \wedge R) = 1 \Leftrightarrow f((P \wedge R) \vee (Q \wedge R)) = 1$, значит, $(X \sqcup Y) \sqcap Z = (X \sqcap Z) \sqcup (Y \sqcap Z)$.

Аналогичным образом, любое равенство множеств, требующее проверки, сводится к равносильности некоторых формул логики высказываний. □

Изоморфизм булевых алгебр

Определение 3.9. Изоморфизм булевых алгебр – это биекция, сохраняющая все операции.

Точнее, пусть $\mathcal{A}$, $\mathcal{B}$ – булевы алгебры. Биекция $\varphi : \mathcal{A} \to \mathcal{B}$ называется *изоморфизмом $\mathcal{A}$ на $\mathcal{B}$*, если:

$$\begin{aligned} \varphi(\mathbb{0}_{\mathcal{A}}) &= \mathbb{0}_{\mathcal{B}}; \\ \varphi(\mathbb{1}_{\mathcal{A}}) &= \mathbb{1}_{\mathcal{B}}; \\ \varphi(-_{\mathcal{A}} x) &= -_{\mathcal{B}} \varphi(x); \\ \varphi(x \sqcup_{\mathcal{A}} y) &= \varphi(x) \sqcup_{\mathcal{B}} \varphi(y); \\ \varphi(x \sqcap_{\mathcal{A}} y) &= \varphi(x) \sqcap_{\mathcal{B}} \varphi(y). \end{aligned}$$

Определение 3.10. Алгебры $\mathcal{A}$ и $\mathcal{B}$ *изоморфны ($\mathcal{A} \cong \mathcal{B}$)*, если существует изоморфизм $\mathcal{A}$ на $\mathcal{B}$.

Изоморфность $\mathcal{A} \cong \mathcal{B}$ является отношением эквивалентности между алгебрами.

Приведём примеры изоморфных булевых алгебр.

1) $\mathcal{P}(\varnothing) \cong \mathit{1}$.

2) $\mathcal{P}(\{a\}) \cong \mathit{2}$.

Отношение частичного порядка в булевой алгебре

Лемма 3.1. *В булевой алгебре можно определить частичный порядок, положив*

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

Относительно этого порядка $\mathbb{0}$ является наименьшим элементом, $\mathbb{1}$ – наибольшим элементом.

Доказательство:

Проверим свойства частичного порядка.

1) Рефлексивность: $a \leq a$ – верно в силу идемпотентности.

2) Транзитивность: $a \leq b$, $b \leq c \ \Rightarrow \ a \leq c$. Действительно, если $a \leq b$, $b \leq c$, то $a = a \sqcap b = a \sqcap (b \sqcap c) = (a \sqcap b) \sqcap c = a \sqcap c$, то есть $a \leq c$.

3) Антисимметричность: $a \leq b$, $b \leq a \ \Rightarrow \ a = b$. Действительно, если $a \leq b$, $b \leq a$, то $a = a \sqcap b$ и $b = b \sqcap a$, тогда в силу коммутативности $a = b$.

Таким образом, $\leq$ – частичный порядок на $\mathcal{B}$.

$a = a \sqcap \mathbb{1} \ \ \forall a$, то есть $a \leq \mathbb{1} \ \ \forall a$, поэтому $\mathbb{1}$ – наибольший элемент.

$\mathbb{0} \sqcap a = (a \sqcap -a) \sqcap a = a \sqcap (-a \sqcap a) = a \sqcap (a \sqcap -a) = (a \sqcap a) \sqcap -a = a \sqcap -a = \mathbb{0} \ \ \forall a$, то есть $\mathbb{0} \leq a \ \ \forall a$, поэтому $\mathbb{0}$ – наименьший элемент. □

Отношение частичного порядка $\leq$ в булевой алгебре, содержащей более 2 элементов, не является отношением линейного порядка.

Лемма 3.2. $a \leq b \ \Leftrightarrow \ -a \sqcup b = \mathbb{1}$.

Замечание 3.1. Выражение $-a \sqcup b$ является аналогом импликации.

Доказательство:

Докажем $\Rightarrow$. Пусть $a \leq b$, то есть $a = a \sqcap b$. Тогда $-a \sqcup b = -(a \sqcap b) \sqcup b = -(-a \sqcup -b) \sqcup b = -a \sqcup (-b \sqcup b) = -a \sqcup \mathbb{1} = -a \sqcup (-a \sqcup a) = (-a \sqcup -a) \sqcup a = -a \sqcup a = \mathbb{1}$.

Докажем $\Leftarrow$. Пусть $-a \sqcup b = \mathbb{1}$. Тогда $a = a \sqcap \mathbb{1} = a \sqcap (-a \sqcup b) = (a \sqcap -a) \sqcup (a \sqcap b) = \mathbb{0} \sqcup (a \sqcap b) = a \sqcap b$, значит, $a \leq b$. □

Бесконечные булевы алгебры

Приведём примеры бесконечных булевых алгебр.

1) Рассмотрим такое множество подмножеств натурального ряда: $\mathcal{B} = \{V \subset \mathbb{N} \mid V$ конечно или $\mathbb{N} \backslash V$ конечно$\}$. На нём можно построить булеву алгебру $(\mathcal{B}, \cup, \cap, \backslash, \varnothing, \mathbb{N})$. Конечных подмножеств натурального ряда и дополнений к ним счётное количество, поэтому алгебра $\mathcal{B}$ является счётной подалгеброй алгебры $\mathcal{P}(\mathbb{N})$. Однако никакая алгебра $\mathcal{P}(E)$ не может быть счётной: такие алгебры конечны при конечном E и несчётны при бесконечном E. Таким образом, алгебра $\mathcal{B}$ отличается от любой из алгебр $\mathcal{P}(E)$.

2) Алгебра Линденбаума-Тарского. Рассмотрим множество классов всех пропозициональных формул по отношению равносильности $\mathcal{L} = Fm/\sim$. Пусть $[A]$ обозначает класс формулы A. Тогда определим $\mathbb{0} \coloneqq [\bot]$, $\mathbb{1} \coloneqq [\top]$, $[A] \sqcup [B] \coloneqq [A \vee B]$, $[A] \sqcap [B] \coloneqq [A \wedge B]$, $-[A] = [\neg A]$. В силу леммы (2.4) $\mathcal{L}$ – булева алгебра. Это алгебра тоже счётная. Она по сути и есть алгебра высказываний.

Определение 3.11. Атом – минимальный ненулевой элемент.

Упражнение 3.4. Доказать, что в алгебре Линденбаума-Тарского нет атомов.

Теорема 3.3 (Теорема Стоуна)**.**

1) Всякая булева алгебра изоморфна подалгебре алгебры вида $\mathcal{P}(E)$.

2) Всякая конечная булева алгебра $\mathcal{A}$ изоморфна алгебре $\mathcal{P}(E)$, где E – множество всех атомов $\mathcal{A}$.

Следовательно, всякая конечная булева алгебра состоит из 2^n элементов для некоторого n.

Оценки в булевой алгебре

Определение 3.12. *Оценка в булевой алгебре* $\mathcal{B}$ – это отображение $f : Var \to \mathcal{B}$.

Лемма 3.3. $\forall$ *оценки* $f : Var \to \mathcal{B}$ $\exists!$ *отображение* $\overline{f} : Fm \to \mathcal{B}$ *такое, что* $\forall A, B \in Fm$:
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 аналогично доказательству леммы (2.1) о продолжении оценки на формулы.

Дальше для краткости будем писать $f(A)$ вместо $\overline{f}(A)$.

Определение 3.13. $A \sim_{\mathcal{B}} B$ (формулы A и B *равносильны в булевой алгебре* $\mathcal{B}$), если $\forall f \quad f(A) = f(B)$.

Определение 3.14. $\mathcal{B} \vDash A$ (формула A *общезначима в булевой алгебре* $\mathcal{B}$), если $\forall f \quad f(A) = \mathbb{1}$.

Лемма 3.4.
1) $A \sim_{\mathcal{B}} B \;\Leftrightarrow\; \mathcal{B} \vDash A \leftrightarrow B$.
2) $\mathcal{B} \vDash A \;\Leftrightarrow\; A \sim_{\mathcal{B}} \top$.

Доказательство:

1) Надо показать, что $\forall$ оценки f выполняется: $f(A) = f(B) \;\Leftrightarrow\; f(A \leftrightarrow B) = \mathbb{1}$. Введём обозначения $a \coloneqq f(A)$ и $b \coloneqq f(B)$.

Так как $(A \leftrightarrow B)$ означает $(A \to B) \wedge (B \to A)$, то $f(A \leftrightarrow B) = (-a \sqcup b) \sqcap (-b \sqcup a)$.

Таким образом, надо показать, что $a = b \;\Leftrightarrow\; (-a \sqcup b) \sqcap (-b \sqcup a) = \mathbb{1}$.

Докажем $\Rightarrow$. Если $a = b$, то $(-a \sqcup b) \sqcap (-b \sqcup a) = (-a \sqcup a) \sqcap (-a \sqcup a) = \mathbb{1} \sqcap \mathbb{1} = \mathbb{1}$.

Докажем $\Leftarrow$. Заметим, что $x \sqcap y = \mathbb{1} \;\Rightarrow\; x = y = \mathbb{1}$. Действительно, $x \sqcap y \leq x$, $x \sqcap y \leq y$, а $\mathbb{1}$ – наибольший элемент (относительно $\leq$).

Поэтому если $(-a \sqcup b) \sqcap (-b \sqcup a) = \mathbb{1}$, то $-a \sqcup b = -b \sqcup a = \mathbb{1}$.

По лемме (3.2) имеем: $-a \sqcup b = \mathbb{1} \;\Leftrightarrow\; a \leq b$; $\quad -b \sqcup a = \mathbb{1} \;\Leftrightarrow\; b \leq a$. Значит, $a = b$.

2) Это частный случай пункта (1) этой леммы при $B = \top$. $\square$

Лекция 4

Булевы алгебры (продолжение)

Оценки в булевой алгебре (продолжение)

Теорема 4.1. *Для любой нетривиальной булевой алгебры $\mathcal{B}$ (то есть $\mathcal{B} \neq 1$) и формулы A верно:*

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

Доказательство:

Пусть $\mathcal{B} \vDash A$. Возьмём оценку $f : Var \to \mathcal{2}$, и рассмотрим «такую же» оценку в $\mathcal{B}$, то есть $F : Var \to \mathcal{B}$, где $F(P_i) = \mathbb{1} \;\Leftrightarrow\; f(P_i) = 1 \;\; \forall i$.

Из свойств булевых алгебр получаем:

$$\mathbb{0} \sqcup \mathbb{1} = \mathbb{1} \sqcup \mathbb{0} = \mathbb{1}, \quad \mathbb{0} \sqcup \mathbb{0} = \mathbb{0}, \quad \mathbb{1} \sqcup \mathbb{1} = 1,$$
$$\mathbb{0} \sqcap \mathbb{1} = \mathbb{1} \sqcap \mathbb{0} = \mathbb{0}, \quad \mathbb{0} \sqcap \mathbb{0} = \mathbb{0}, \quad \mathbb{1} \sqcap \mathbb{1} = 1,$$
$$-\mathbb{0} = \mathbb{1}, \text{ так как } \mathbb{1} = \mathbb{0} \sqcup -\mathbb{0} = -\mathbb{0},$$
$$-\mathbb{1} = \mathbb{0}, \text{ так как } \mathbb{0} = \mathbb{1} \sqcap -\mathbb{1} = -\mathbb{1}.$$

Таким образом, $\mathbb{0}, \mathbb{1}$ образуют подалгебру в $\mathcal{B}$, изоморфную $\mathcal{2}$. Обозначим этот изоморфизм через $\approx$, то есть $\mathbb{1} \approx 1$ и $\mathbb{0} \approx 0$. Тогда $F(P_i) \approx f(P_i) \;\; \forall i$, откуда по индукции можно показать, что $F(B) \approx f(B) \;\; \forall B \in Fm$.

Теперь для исходной формулы A получаем $f(A) = 1$, поскольку $F(A) = \mathbb{1}$. Таким образом, $\mathcal{2} \vDash A$. □

Исчисление высказываний

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

Приведём 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) $A \wedge B \to B$;
5) $A \to (B \to A \wedge B)$;
6) $A \to A \vee B$;
7) $B \to A \vee B$;
8) $(A \to C) \to ((B \to C) \to (A \vee B \to C))$;
9) $(A \to \neg B) \to ((A \to B) \to \neg A)$;
10) $\neg\neg A \to A$.

Здесь A, B, C – произвольные формулы. Поэтому каждая из схем (1)-(10) порождает бесконечную серию аксиом.

Правило вывода только одно, и называется $ModusPonens$ (MP) и записывается так: $\dfrac{A,\ A \to B}{B}$. Эта запись означает, что если доказаны формулы A и $A \to B$, то можно доказать B.

Определение 4.1. *Доказательство* (или *вывод*) формулы A в CL – это конечная последовательность формул, каждая из которых является аксиомой или получается из предыдущих по правилу MP, причём эта последовательность формул заканчивается формулой A.

Точнее: доказательство – это такая последовательность формул $A_1, \ldots, A_n = A$, что для всех k $(1 \le k \le n)$ A_k – аксиома или существуют $i, j < k$, для которых $A_j = A_i \to A_k$.

Определение 4.2. Формула A, для которой существует доказательство в CL, называется *теоремой* CL, или *выводимой в* CL; это записывается так: $\vdash_{CL} A$. Индекс CL не пишем, если ясно, что речь идёт об этой системе.

Приведём примеры.
1) $\vdash A \vee B \to B \vee A$.
Приведём доказательство. 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. $(B \to C) \to (A \vee B \to C)$ (1, 3, MP)
5. $A \vee B \to C$ (2, 4, MP)
2) $\vdash A \to A$.
Приведём доказательство. Для удобства обозначим формулу $A \to A$ через 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)

Определение 4.3. Пусть Γ – какое-то множество пропозициональных формул (гипотез). *Вывод из гипотез* Γ *формулы* A *в* CL – это конечная последовательность формул, каждая из которых является аксиомой, или принадлежит Γ, или получается из предыдущих по правилу MP, причём эта последовательность формул заканчивается формулой A.

То есть это последовательность формул $A_1, \ldots, A_n$, где для всех k $(1 \le k \le n)$ A_k – аксиома, или $A_k \in \Gamma$, или существуют $i, j < k$, для которых $A_j = A_i \to A_k$.

Определение 4.4. Формула A *выводима из гипотез* Γ, если существует вывод из Γ, содержащий A; обозначение: $\Gamma \vdash_{CL} A$. Индекс CL не пишем, если ясно, что речь идёт об этой системе.

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

Лемма 4.1.
1) Если $\Gamma \subseteq \Delta$ *и* $\Gamma \vdash A$, *то* $\Delta \vdash A$.
2) Если $\Gamma \vdash A$, *то существует конечное* $\Delta \subseteq \Gamma$, *для которого* $\Delta \vdash A$.
3) Если $\Gamma \vdash A$, *и* $\Delta \vdash B \ \ \forall B \in \Gamma$, *то* $\Delta \vdash A$.

Доказательство:
1) Очевидно из определения.
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 пункта (2) этой леммы следует, что можно заменить Γ на его конечное подмножество Γ_1, то есть 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. Возьмём вывод A из Γ_1; в нём встречаются какие-то гипотезы B_i: $\ldots, B_{i_1}, \ldots, B_{i_2}, \ldots, A$. Заменим в этом выводе каждую B_i на её вывод Π_i: $\ldots, \Pi_{i_1}, \ldots, \Pi_{i_2}, \ldots, A$.

Получится вывод A из Δ. Действительно, все формулы из исходного вывода, кроме гипотез B_i, являются аксиомами CL или получаются из предыдущих по MP. А в каждом вставном выводе Π_i все формулы являются аксиомами CL, или входят в Δ, или получаются по MP из предыдущих (внутри того же вывода). □

Замечание 4.1. Утверждения пункта (3) леммы (4.1) называют «транзитивность выводимости» или «сечение». Если условие $\Delta \vdash B \ \ \forall B \in \Gamma$ обозначить как $\Delta \vdash \Gamma$, то утверждение этого пункта запишется так: если $\Delta \vdash \Gamma$ и $\Gamma \vdash A$, то $\Delta \vdash A$. Отсюда название «транзитивность».

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.

Определение 4.5. Если $\Gamma \vdash A$, то говорят, что $\dfrac{\Gamma}{A}$ – *производное правило* CL.

Определение 4.6. Если из выводимости формул из Γ следует выводимость A, то говорят, что $\dfrac{\Gamma}{A}$ – *допустимое правило* CL.

Лемма 4.2. *Всякое производное правило* CL *допустимо.*

Доказательство:
Пусть $\Gamma \vdash A$. Тогда по транзитивности выводимости (пункт (3) леммы (4.1)) получаем: если $\varnothing \vdash \Gamma$, то $\varnothing \vdash B$. □

Приведём пример.
Допустимо правило введения конъюнкции: $\dfrac{A, B}{A \wedge B}$.
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 дедукции для CL

Теорема 4.2 (Теорема дедукции для CL)**.**
$\Gamma, A \vdash B \Leftrightarrow \Gamma \vdash A \to B$.
Здесь Γ, A *обозначает множество* $\Gamma \cup \{A\}$.

Доказательство:

Докажем $\Leftarrow$. 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 (пункт (3) леммы (4.1)) $\Gamma, A \vdash B$.

Докажем $\Rightarrow$. Доказывать будем индукцией по длине вывода B из Γ, A.

Если этот вывод длины 1, то B – аксиома или гипотеза.

1) Если B – аксиома, то имеем вывод $A \to B$ (из $\varnothing$):
1. B (аксиома)
2. $B \to (A \to B)$ (аксиома 1)
3. $A \to B$ (1, 2, MP)

2) Если $B \in \Gamma$, то имеем такой же вывод $A \to B$ из Γ:
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, то есть 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 пунктам (1)-(3) этого доказательства.

Остаётся случай, когда B получается по MP из формул $C, C \to B$, причём $\Gamma, A \vdash C$ 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 $\Gamma \vdash A \to C$, $A \to (C \to B)$ и $A \to C$, $A \to (C \to B) \vdash A \to B$ по транзитивности получаем: $\Gamma \vdash A \to B$. □

Приведём пример.

Допустимо правило силлогизма $\dfrac{A \to B,\ B \to C}{A \to C}$. Покажем, что это – производное правило, то есть $A \to B$, $B \to C \vdash A \to C$.

По теореме дедукции это равносильно $A \to B$, $B \to C$, $A \vdash C$. Последнее утверждение очевидно: надо два раза применить MP.

Корректность CL для булевых алгебр

Теорема 4.3. *Если $\vdash_{CL} A$, то $\mathcal{B} \vDash A$ для любой булевой алгебры $\mathcal{B}$.*

Доказательство:

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

1) A – аксиома.

2) A получается по MP из формул B, $B \to A$ с более короткими выводами.

Начнём с более простого случая (2). По предположению индукции, $\mathcal{B} \vDash B$, $B \to A$. Рассмотрим произвольную оценку f в $\mathcal{B}$; пусть $f(A) = a$. Докажем, что $a = \mathbb{1}$.

Поскольку $\mathcal{B} \vDash B$, $B \to A$, имеем: $f(B) = f(B \to A) = \mathbb{1}$. Тогда $\mathbb{1} = f(B \to A) = = -f(B) \sqcup f(A) = -\mathbb{1} \sqcup a = \mathbb{0} \sqcup a = a$.

В случае (1) надо доказывать общезначимость всех 10 аксиом. Это мы рассмотрим на следующей лекции. □

Лекция 5

Корректность CL для булевых алгебр (продолжение)

Для продолжения доказательства теоремы (4.3) нам понадобится следующая лемма о булевых алгебрах.

Лемма 5.1. *В любой булевой алгебре:*
1) $x \le x \sqcup y$, $y \le x \sqcup y$;
2) если $x \le z$ *и* $y \le z$, *то* $x \sqcup y \le z$;
3) если $x \le x'$ *и* $y \le y'$, *то* $x \sqcup y \le x' \sqcup y'$.

Доказательство:
1) $x \sqcap (x \sqcup y) = x$ – поглощение и коммутативность; аналогично получаем $y \sqcap (x \sqcup \sqcup y) = y$.
2) Если $x \sqcap z = x$, $y \sqcap z = y$, то по дистрибутивности $(x \sqcup y) \sqcap z = (x \sqcap z) \sqcup (y \sqcap z) = = x \sqcup y$.
3) Пусть $x \le x'$ и $y \le y'$. Тогда из пункта (1) этого доказательства получаем: $x \le x' \le x' \sqcup y'$, $y \le y' \le x' \sqcup y'$. Теперь, применяя (2) этого доказательства, имеем: $x \sqcup y \le x' \sqcup y'$. □

Теперь продолжим доказательство теоремы (4.3).

Доказательство:
Нам надо доказать общезначимость аксиом CL в произвольной булевой алгебре $\mathcal{B}$.
Докажем общезначимость аксиомы 1: $A \to (B \to A)$.
Пусть дана оценка f в $\mathcal{B}$; пусть $f(A) = a$, $f(B) = b$. Нам надо доказать, что $a \to (b \to a) = \mathbb{1}$. По лемме (3.2) это равносильно $a \le b \to a$, то есть $a \le -b \sqcup a$. Тогда по пункту (1) леммы (5.1) получаем, что аксиома 1 общезначима.
Докажем общезначимость аксиомы 2: $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$.
Пусть дана оценка f в $\mathcal{B}$, $f(A) = a$, $f(B) = b$, $f(C) = c$. Надо доказать, что $(a \to (b \to c)) \to ((a \to b) \to (a \to c)) = \mathbb{1}$. По лемме (3.2) это равносильно $a \to (b \to \to c) \le (a \to b) \to (a \to c)$, то есть $-a \sqcup (-b \sqcup c) \le -(-a \sqcup b) \sqcup (-a \sqcup c)$. Применяя закон де Моргана и ассоциативность, получаем: $-a \sqcup -b \sqcup c \le (a \sqcap -b) \sqcup -a \sqcup c$. По пункту (3) леммы (5.1), достаточно проверить, что $-b \le (a \sqcap -b) \sqcup -a$. А это получается так: $-b = \mathbb{1} \sqcap (-b) = (a \sqcup -a) \sqcap (-b) = (a \sqcap -b) \sqcup (-a \sqcap -b) \le (a \sqcap -b) \sqcup -a$.
Докажем общезначимость аксиомы 8: $(A \to C) \to ((B \to C) \to (A \vee B \to C))$.
Пусть дана оценка f в $\mathcal{B}$, $f(A) = a$, $f(B) = b$, $f(C) = c$. Надо доказать, что $(a \to c) \to ((b \to c) \to ((a \sqcup b) \to c)) = \mathbb{1}$. По лемме (3.2) это равносильно $a \to c \le \le (b \to c) \to ((a \sqcup b) \to c)$, то есть $-a \sqcup c \le -(-b \sqcup c) \sqcup -(a \sqcup b) \sqcup c$. Применяя закон де Моргана, получаем: $-a \sqcup c \le (b \sqcap -c) \sqcup (-a \sqcap -b) \sqcup c$. По пункту (3) леммы (5.1), достаточно проверить, что $-a \le (b \sqcap -c) \sqcup (-a \sqcap -b) \sqcup c$. При доказательстве общезначимости аксиомы аксиомы 2 было доказано неравенство $-b \le (a \sqcap -b) \sqcup -a$. Другими формами этого же неравества являются $-a \le (-a \sqcap -b) \sqcup b$ и $b \le (b \sqcap -c) \sqcup c$. Тогда по лемме (5.1) получаем: $-a \le (-a \sqcap -b) \sqcup b \le (-a \sqcap -b) \sqcup (b \sqcap -c) \sqcup c$.
Докажем общезначимость аксиомы 9: $(A \to \neg B) \to ((A \to B) \to \neg A)$.

Пусть дана оценка f в $\mathcal{B}$, $f(A) = a$, $f(B) = b$, $f(C) = c$. Надо доказать, что $(a \to -b) \to ((a \to b) \to -a) = \mathbb{1}$. Заметим, что $a \to \mathbb{0} = -a \sqcup \mathbb{0} = -a$. Значит, надо проверить, что $(a \to (b \to \mathbb{0})) \to ((a \to b) \to (a \to \mathbb{0})) = \mathbb{1}$. Но это мы установили при проверке аксиомы 2: надо взять $c = \mathbb{0}$.

Упражнение 5.1. Проверить общезначимость аксиом 3, 4, 5, 6, 7, 10.

□

Запишем следствие теоремы (4.3).

Утверждение 5.1. *CL непротиворечиво, то есть нет такой формулы A, что $\vdash_{CL} A, \neg A$.*

Доказательство:
Иначе обе формулы $A, \neg A$ окажутся тавтологиями. □

Полнота исчисления высказываний

Теорема 5.1 (Теорема о полноте CL)**.** *Все тавтологии выводимы в CL: $2 \vDash A \Rightarrow \Rightarrow \vdash_{CL} A$.*

Доказательство:
Пусть $\nvdash_{CL} A$. Докажем, что $2 \nvDash A$.

Определение 5.1. Множество формул $\Gamma \subseteq Fm$ называется *противоречивым* (в CL), если $\Gamma \vdash B, \neg B$ для некоторой формулы B.

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:
1) Докажем $\Leftarrow$. Это очевидно, так как $\Gamma \cup \{B\} \vdash B, \neg B$.
Докажем $\Rightarrow$. Пусть $\Gamma \cup \{B\} \vdash C, \neg C$. Тогда по теореме дедукции $\Gamma \vdash B \to \to C, B \to \neg C$. С другой стороны, $B \to C, B \to \neg C \vdash \neg B$. Это получается из аксиомы 9 $((B \to \neg C) \to ((B \to C) \to \neg B))$, если 2 раза применить MP. Тогда по транзитивности $\Gamma \vdash \neg B$.
2) Если Γ противоречиво, то и подавно $\Gamma \cup \{\neg B\}$ противоречиво. Тогда по пункту (1) доказываемой леммы $\Gamma \vdash \neg\neg B$. Добавив к этому выводу аксиому 10 $(\neg\neg B \to B)$ и применив MP, получаем $\Gamma \vdash B$. □

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

Определение 5.2. Множество $\Gamma \subseteq \Phi$ назовём *максимально непротиворечивым* (или просто – *максимальным*), если оно непротиворечиво, а всякое его собственное расширение внутри Φ (то есть 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 пункту (1) леммы (5.2)), 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. Так как $\Phi \backslash \Gamma$ конечно, через конечное число шагов получится максимальное множество.

Вообще говоря, это рассуждение (его можно провести точнее, в рамках формальной теории множеств) показывает, что всякое конечное частично упорядоченное множество имеет максимальный элемент. В нашем случае это множество всех непротиворечивых подмножеств Φ, содержащих Γ, упорядоченное по включению. □

Лемма 5.4 (Свойства максимальных множеств)**.** *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 $\Gamma \subset \subset \Gamma \cup \{B\} \subseteq \Phi$, поэтому $\Gamma \cup \{B\}$ противоречиво (так как Γ максимально). Тогда по пункту (1) леммы (5.2) $\Gamma \vdash \neg B$, и следовательно, $\Gamma \nvdash B$, так как иначе бы Γ было противоречиво.

1) Докажем $\Rightarrow$. Это очевидно, так как Γ непротиворечиво.

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

(2) Нам дано, что $(B \wedge C) \in \Phi$. Тогда $(B \wedge C)$ – подформула A, поэтому и B, C являются подформулами A и лежат в Φ.

Докажем $\Rightarrow$. Пусть $(B \wedge C) \in \Gamma$. Тогда $\Gamma \vdash B, C$ (по аксиомам 3 $(B \wedge C \to B)$, 4 $(B \wedge C \to C)$ и MP). Значит, по пункту (0) доказываемой леммы получаем, что $B, C \in \Gamma$.

Докажем $\Leftarrow$. Пусть $B, C \in \Gamma$. Тогда $\Gamma \vdash B \wedge C$ (так как $B, C \vdash B \wedge C$ – см. пример о допустимости правила введения конъюнкции $\dfrac{A, B}{A \wedge B}$ из лекции 4). Отсюда по пункту (0) доказываемой леммы получаем, что $(B \wedge C) \in \Gamma$.

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

Докажем $\Leftarrow$. Если $B \in \Gamma$, то $\Gamma \vdash B \vee C$ (по аксиоме 6 $(B \to B \vee C)$ и MP), и тогда по пункту (0) доказываемой леммы получаем, что $(B \vee C) \in \Gamma$. Если $C \in \Gamma$, рассуждаем аналогично (с аксиомой 7 $(C \to B \vee C)$).

Докажем $\Rightarrow$. Доказываем от противного. Допустим $(B \vee C) \in \Gamma$, но $B, C \notin \Gamma$. Тогда $\neg B$, $\neg C \in \Gamma$ – по пункту (1) доказываемой леммы.

Вспомним теперь, что из противоречивого множества выводится любая формула (пункт (2) леммы (5.2)), 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 $((B \to \bot) \to ((C \to \bot) \to (B \vee C \to$ $\to \bot)))$ и MP (трижды). 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 $B, C \in \Phi$.

Докажем $\Rightarrow$. Если $(B \to C)$, $B \in \Gamma$, то $\Gamma \vdash C$ по MP, и тогда по пункту (0) доказываемой леммы получаем, что $C \in \Gamma$.

Докажем $\Leftarrow$. Разбираем 2 случая.

Если $B \notin \Gamma$, то $\neg B \in \Gamma$ по пункту (1) доказываемой леммы. Но $\neg B$, $B \vdash C$ (пункт (2) леммы (5.2)), откуда по теореме дедукции $\neg B \vdash B \to C$. Значит, по пункту (0) доказываемой леммы получаем, что $\Gamma \vdash B \to C$, и $(B \to C) \in \Gamma$.

Если $C \in \Gamma$, то $\Gamma \vdash B \to C$ по аксиоме 1 $(C \to (B \to C))$ и MP, и опять по пункту (0) доказываемой леммы получаем, что $(B \to C) \in \Gamma$. $\square$

Закончим теперь доказательство теоремы. Исходное непротиворечивое множество $\neg A$ расширим до максимального Γ (лемма (5.3)). Возьмём оценку $f : Var \to \{0, 1\}$ такую, что для всех переменных P_i из Φ выполнено $f(P_i) = \begin{cases} 1, \text{ если } P_i \in \Gamma \\ 0, \text{ если } P_i \notin \Gamma \end{cases}$.

Утверждение 5.2. $f(B) = 1 \Leftrightarrow B \in \Gamma$ *для всех* $B \in \Phi$.

Доказательство:

Это утверждение доказывается индукцией по длине B.

Если $B \in Var$, то утверждение верно по определению.

Если $B = (B_1 \wedge B_2)$, то $B_1, B_2 \in \Phi$, и по предположению индукции $f(B_1) = 1 \Leftrightarrow$ $\Leftrightarrow B_1 \in \Gamma$, $f(B_2) = 1 \Leftrightarrow B_2 \in \Gamma$. Тогда $f(B) = 1 \Leftrightarrow f(B_1) = f(B_2) = 1 \Leftrightarrow (B_1 \in$ $\in \Gamma$ и $B_2 \in \Gamma) \Leftrightarrow B = (B_1 \wedge B_2) \in \Gamma$ по лемме (5.4) о свойствах максимальных множеств.

Если $B = (B_1 \vee B_2)$, то $B_1, B_2 \in \Phi$, и по предположению индукции $f(B_1) = 1 \Leftrightarrow$ $\Leftrightarrow B_1 \in \Gamma$, $f(B_2) = 1 \Leftrightarrow B_2 \in \Gamma$. Тогда $f(B) = 1 \Leftrightarrow f(B_1) = 1$ или $f(B_2) =$ $= 1 \Leftrightarrow (B_1 \in \Gamma$ или $B_2 \in \Gamma) \Leftrightarrow B = (B_1 \vee B_2) \in \Gamma$ по лемме (5.4) о свойствах максимальных множеств.

Если $B = \neg B_1$, то $B_1 \in \Phi$, и по предположению индукции $f(B_1) = 1 \Leftrightarrow B_1 \in \Gamma$. Тогда $f(B) = 1 \Leftrightarrow f(B_1) = 0 \Leftrightarrow B_1 \notin \Gamma \Leftrightarrow B = \neg B_1 \in \Gamma$ по лемме (5.4) о свойствах максимальных множеств.

Если $B = (B_1 \to B_2)$, то $B_1, B_2 \in \Phi$, и по предположению индукции $f(B_1) = 1 \Leftrightarrow$ $\Leftrightarrow B_1 \in \Gamma$, $f(B_2) = 1 \Leftrightarrow B_2 \in \Gamma$. Тогда $f(B) = 1 \Leftrightarrow f(B_1) = 0$ или $f(B_2) =$ $= 1 \Leftrightarrow (B_1 \notin \Gamma$ или $B_2 \in \Gamma) \Leftrightarrow B = (B_1 \to B_2) \in \Gamma$ по лемме (5.4) о свойствах максимальных множеств. $\square$

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

Сформулируем следствие из теоремы (5.1) о полноте CL.

Теорема 5.2. *Для любой пропозициональной формулы A и нетривиальной булевой алгебры $\mathcal{B}$ следующие утверждения эквивалентны.*

1) $\vdash_{CL} A$;

2) $\mathcal{B} \vDash A$;

3) $\mathcal{2} \vDash A$.

Доказательство:

(1) $\Rightarrow$ (2) – это теорема (4.3) о корректности CL для булевых алгебр.

(2) $\Rightarrow$ (3) – теорема (4.1).

(3) $\Rightarrow$ (1) – теорема (5.1) о полноте CL. □

Лекция 6

Логика предикатов

Языки первого порядка: синтаксис

Отличия языка 1-го порядка от языка логики высказываний:
1) вместо пропозициональных переменных используются атомарные формулы;
2) для индуктивного построения формул, кроме логических связок, применяются кванторы.

Определение 6.1. *Сигнатурой (первого порядка)* называется четвёрка вида $\Omega = (Pred_\Omega, Fun_\Omega, Const_\Omega, \nu)$, в которой:

- $Pred_\Omega$, Fun_Ω, $Const_\Omega$ – попарно не пересекающиеся множества;
- $Pred_\Omega \neq \varnothing$;
- $\nu : Pred_\Omega \cup Fun_\Omega \to \mathbb{N}_+ = \{1, 2, \ldots\}$.

Множества $Pred_\Omega$, Fun_Ω, $Const_\Omega$ называются соответственно множеством *предикатных символов*, множеством *функциональных символов* и множеством *(предметных) констант* 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 6.2. Алфавит языка первого порядка сигнатуры Ω состоит из:

- всех предикатных символов, функциональных символов и констант Ω;
- счётного множества свободных (предметных) переменных $FVar = \{a_0, a_1, \ldots\}$;
- счётного 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 символов v_i.

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

Определение 6.3. *Термы сигнатуры* Ω (обозначение: Tm_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 (обозначение: Tm_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 6.4. *Атомарные формулы сигнатуры* Ω (обозначение: AFm_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 6.5. *Формулы сигнатуры* Ω (обозначение: Fm_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).

Замечание 6.1. В любой формуле кванторы по одной и той же переменной могут встречаться только в непересекающихся подформулах. Например, если $P^1 \in Pred_\Omega$ и $x \in BVar$, то $\exists x P(x) \wedge \exists x \neg P(x)$ – формула, а $\exists x(P(x) \wedge \exists x \neg P(x))$ – не формула.

Существуют и другие варианты определения формулы. Самый распространённый 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.

Приведём 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 – чётное число (если речь идёт 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.

Приведём ещё примеры формул: $\forall x \forall y(x \cdot y = 0 \to (x = 0 \vee y = 0))$; $\forall x(x = 0 \to \to x = 0)$; $1 + 1 = 0$.

Лемма 6.1 (Лемма об однозначном анализе термов и формул)**.** *Для данной сигнатуры Ω:*

1) Каждый терм есть либо константа, либо свободная переменная, либо имеет вид $f(t_1, \ldots, t_n)$ для единственного функционального символа f^n и термов $t_1, \ldots, t_n$.

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

3) Для любой формулы A выполнено ровно одно из условий:

- *A – атомарная;*
- *существует единственная пара формул B, C, такая что $A = (B \wedge C)$;*
- *существует единственная пара формул B, C, такая что $A = (B \vee C)$;*
- *существует единственная пара формул B, C, такая что $A = (B \to C)$;*
- *существует единственная формула B, такая что $A = \neg B$;*
- *$A = \exists x[x/a]B$ для некоторой формулы B и $a \in FVar$, $x \in BVar$;*
- *$A = \forall x[x/a]B$ для некоторой формулы B и $a \in FVar$, $x \in BVar$.*

Доказательство пропускаем. Отметим, что в последних двух случаях формула B 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 6.6. *Модель сигнатуры* Ω, или Ω*-структура*, – это пара вида $M = (\underline{M}, \mathcal{I})$, где:

$\underline{M}$ – непустое множество (*носитель модели*);

$\mathcal{I}$ – функция, определённая на множестве $Const_\Omega \cup Fun_\Omega \cup Pred_\Omega$ (*интерпретирующая функция*), причём:

- если $c \in Const_\Omega$, то $\mathcal{I}(c) \in \underline{M}$;

- если $f^n \in Fun_\Omega$, то $\mathcal{I}(f) : \underline{M}^n \to \underline{M}$ (то есть $\mathcal{I}(f)$ – *n-местная операция на* $\underline{M}$);
- если $P^n \in Pred_\Omega$, то $\mathcal{I}(P) : \underline{M}^n \to \{0,1\}$ (то есть $\mathcal{I}(P)$ – *n-местный предикат на* $\underline{M}$).

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

Определение 6.7. Терм, не содержащий переменных (то есть построенный из констант и функциональных символов), называется *замкнутым*. Для сигнатуры Ω множество всех замкнутых термов обозначается CTm_Ω.

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

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

Лемма 6.2. *Пусть M – модель сигнатуры Ω. Значения замкнутых термов в M определены корректно. Это означает, что существует единственное отображение $t \to |t|_M$ из CTm_Ω в $\underline{M}$, удовлетворяющее условиям из определения (6.7):*

- $|c|_M = c_M$ *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 доказательству леммы (2.1). Индукцией по длине t доказываем, что $|t|_M$ определяется однозначно.

Базис индукции: если t – константа, то всё 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, значения $|t_1|_M, \ldots, |t_n|_M$ определены однозначно, и тогда $|t|_M = f_M(|t_1|_M, \ldots, |t_n|_M)$ тоже задаётся однозначно. □

Определение 6.8. *Замкнутая атомарная формула* имеет вид $P^n(t_1, \ldots, t_n)$, где $t_1, \ldots, t_n$ – замкнутые термы.

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

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

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

Определение 6.9. Очевидное следствие лемм (6.1) и (6.2).

Определение 6.10. Модель M сигнатуры, содержащей 2-местный предикатный символ равенства $=$, называется *нормальной*, если для всех m_1, m_2 из M

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

Приведём пример.

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

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

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

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

Определение 6.11. Формула, не содержащая свободных переменных, называется *замкнутой*, или *предложением*. Для сигнатуры Ω множество всех замкнутых формул обозначается CFm_Ω.

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

Определение 6.12. Пусть M – модель сигнатуры Ω, A – замкнутая формула сигнатуры Ω. Говорят, что A *истинна* (или *выполнима*) в M, если $|A|_M = 1$. В этом случае также говорят, что M – *модель* A и пишут $M \vDash A$.

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

Общезначимые формулы выражают законы логики.

Приведём пример общезначимой формулы: $\forall x \forall y [x/a][y/b]A \to \forall y \forall x [x/a][y/b]A$.

Приведём пример выполнимой формулы: $\exists x P(x) \wedge \exists x \neg P(x)$.

Определение 6.13. *Теорией первого порядка* в сигнатуре Ω называется любое множество замкнутых формул этой сигнатуры; элементы теории называются также её *аксиомами*.

Определение 6.14. 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.

Приведём пример.

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

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

Определение 6.15. Пусть T – теория, A – замкнутая формула в её сигнатуре. Говорят, что A *логически* (или *семантически*) *следует из* T (обозначение: $T \vDash A$), если A истинна во всех моделях T.

Очевидны следующие свойства:
1. Если T не выполнима, то $T \vDash A$ для всех A.
2. $T \nvDash A \Leftrightarrow T \cup \{\neg A\}$ выполнима.

Определение 6.16. Теория T называется *полной*, если для любой замкнутой формулы A в её сигнатуре хотя бы одна из формул A, $\neg A$ логически следует из T.

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

Приведём примеры.

Чистая теория равенства Eq неполна. Чтобы в этом убедиться, рассмотрим формулу $A_{=1} := \forall x \forall y(x = y)$. Заметим, что в нормальной модели M имеем: $M \vDash A_{=1} \Leftrightarrow$ $\Leftrightarrow |M| = 1$ (где $|M|$ – мощность модели M, то есть мощность её носителя). Поэтому:

- $Eq \nvDash \neg A_{=1}$, так как теория $Eq \cup \{A_{=1}\}$ выполнима: у неё есть 1-элементная нормальная модель.
- $Eq \nvDash A_{=1}$, так как теория $Eq \cup \{\neg A_{=1}\}$ выполнима: у неё есть (например) 10-элементная нормальная модель.

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

Определение 6.17. *Элементарной теорией* модели M называется множество всех замкнутых формул в её сигнатуре, истинных в M; обозначение: $Th(M)$.

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

Определение 6.18. Модели M_1, M_2 одной сигнатуры называются *элементарно эквивалентными*, если в них истинны одни и те же замкнутые формулы, то есть $Th(M_1) = Th(M_2)$; обозначение: $M_1 \equiv M_2$.

Лекция 7

Логика предикатов (продолжение)

Языки первого порядка: семантика (продолжение)

Определение 7.1. *Логическое (семантическое) замыкание* $[T]$ – множество всех логических следствий теории T, то есть $[T] := \{A \mid T \vDash A\}$, где A – замкнутая формула.

T полна, если для любой замкнутой формула A выполняется $A \in [T]$ или $\neg A \in \in [T]$.

Определение 7.2. Теории T_1, T_2 одной сигнатуры называются *эквивалентными (равносильными)*, если у них одни и те же модели; обозначение: $T_1 \sim T_2$.

Лемма 7.1. $T_1 \sim T_2 \;\Leftrightarrow\; [T_1] = [T_2]$.

Доказательство:

Докажем $\Rightarrow$. Если модели у теорий T_1, T_2 одинаковые, то и формулы, которые верны в этих моделях – одни и те же, то есть $[T_1] = [T_2]$.

Докажем $\Leftarrow$. Если следствия у теорий одинаковые, то любая формула из T_2 является следствием T_1, то есть верна во всех моделях T_1. Значит, всякая модель T_1 оказывается моделью T_2. Аналогично, всякая модель T_2 является моделью T_1. $\square$

Лемма 7.2. *Пусть T – выполнимая теория. Следующие условия эквивалентны:*

1) T полна;

2) любое выполнимое расширение теории T эквивалентно T, то есть $\forall T' \supseteq T$ имеем: $T' \sim T$ или T' невыполнима.

3) $[T] = Th(M)$ для некоторой модели M.

4) Все модели T элементарно эквивалентны.

Доказательство:

Докажем (1) $\Rightarrow$ (2). Пусть T полна, докажем пункт (2). Пусть $T' \supseteq T$; тогда очевидно, что $[T'] \supseteq [T]$. Предположим, что $T' \not\sim T$, тогда $T' \supset T$ и $[T'] \supset [T]$. Тогда найдётся формула $A \in ([T']\backslash[T])$. Поскольку $T \nvDash A$ и T полна, получаем $T \vDash \neg A$. Но тогда и $T' \vDash \neg A$. С другой стороны, $T' \vDash A$. Значит, T' невыполнима.

Докажем (2) $\Rightarrow$ (3). Предположим, что пункт (2) выполнен. Если $M \vDash T$, то $T \subseteq Th(M)$. Теория $Th(M)$ выполнима, поэтому она эквивалентна T (в силу пункта (2)). Тогда $[T] = [Th(M)]$. Но $[Th(M)] = Th(M)$, так как все логические следствия $Th(M)$ истинны в M. Получаем: $[T] = Th(M)$.

Докажем (3) $\Rightarrow$ (4). Предположим, что пункт (3) выполнен. Тогда из $M' \vDash T$ следует $M' \vDash Th(M)$. Значит, всякая замкнутая формула, истинная в M, будет истинной в M'. И наоборот, если $M \nvDash A$, то есть $M \vDash \neg A$, то $M' \vDash \neg A$, то есть $M' \nvDash A$. Итак, $M \equiv M'$.

Докажем (4) $\Rightarrow$ (1). Предположим, что пункт (4) выполнен. Допустим, что T неполна. Тогда для некоторой замкнутой формулы A имеем: $T \nvDash A$ и $T \nvDash \neg A$. Это означает, что обе теории $T \cup \{\neg A\}$, $T \cup \{A\}$ выполнимы. Их модели оказываются моделями T, которые не элементарно эквивалентны. Получили противоречие, значит, T полна. $\square$

Определение истинности в модели

Определение 7.3. Пусть M – модель сигнатуры Ω; предполагаем, что её носитель $\underline{M}$ состоит из совершенно новых элементов, которые не являются словами, содержащими символы из Ω. Через $\Omega \cup M$ обозначим *расширенную сигнатуру модели* M, которая получается из Ω добавлением множества новых констант $\underline{M}$; то есть $Const_{\Omega \cup M} = Const_\Omega \cup \underline{M}$, в остальном же $\Omega \cup M$ не отличается от Ω.

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», то есть 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.

Определение 7.4. Пусть M – модель сигнатуры Ω. *Терм, оценённый в* M, – это замкнутый терм расширенной сигнатуры M; аналогично, *формула, оценённая в* M – это замкнутая формула сигнатуры $\Omega \cup M$.

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

Определение 7.5. Для терма t, оценённого в модели M, индукцией по длине определяется его *значение* $|t|_M$:

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

Определение 7.6. Для формулы C, оценённой в модели M, её «логической длиной» назовём число вхождений в неё логических связок и кванторов. Индукцией по логической длине формулы C определяется её *значение* $|C|_M$:

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

Здесь $[m/a]A$ обозначает оценённую формулу, полученную из A заменой всех вхождений a на m.

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

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

- $|\exists x[x/a]A|_M = \max\limits_{m\in\underline{M}} |[m/a]A|_M$;
- $|\forall x[x/a]A|_M = \min\limits_{m\in\underline{M}} |[m/a]A|_M$.

Приведём пример.

Рассмотрим сигнатуру колец, содержащую равенство ($=$), константы 0, 1 и функциональные символы: $\cdot$, $+$ (2-местные). В термах записываем их привычным образом: $t_1 \cdot t_2$, $t_1 + t_2$.

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

Имеем: $\mathbb{R} \vDash \exists x(x\cdot x = 1+1)$, так как $\mathbb{R} \vDash \sqrt{2}\cdot\sqrt{2} = 1+1$ (или $\mathbb{R} \vDash (-\sqrt{2})\cdot(-\sqrt{2}) = 1+1$). Отметим, что здесь возникает оценённая формула $\sqrt{2}\cdot\sqrt{2} = 1+1$ (или $(-\sqrt{2})\cdot(-\sqrt{2}) = 1+1$), с константами двух видов: 1 берётся из исходной сигнатуры, а $\sqrt{2}$ (или $-\sqrt{2}$) – из модели; в сигнатуре колец такого символа нет.

С другой стороны, $\mathbb{Q} \vDash \neg\exists x(x\cdot x = 1+1)$, так как $\mathbb{Q} \nvDash r\cdot r = 1+1$ для всех $r \in \mathbb{Q}$.

Лемма 7.3.

1) $|t|_M$ определено корректно для любого оценённого терма t. То есть для любой модели M существует единственное отображение $t \to |t|_M$ оценённых в M термов в $\underline{M}$, удовлетворяющее условиям из определения (7.5).

2) $|A|_M$ определено корректно для любой оценённой формулы A. То есть для любой модели M существует единственное отображение $A \to |A|_M$ оценённых в M формул в $\{0,1\}$, удовлетворяющее условиям из определения (7.6).

Доказательство:

1) Рассуждаем, как в доказательстве леммы (6.2). Лемма (6.1) об однозначном анализе термов и формул сохраняется для оценённых термов с небольшим отличием: они бывают 3 видов. При этом важно, что элементы M не являются константами Ω и не представляются в виде $f(t_1, \ldots, t_n)$. Но это уже было оговорено.

2) Аналогично лемме (2.1) о продолжении оценки на формулы. Применим лемму (6.1) об однозначном анализе термов и формул (для оценённых формул она не меняется).

- Если $A = P(t_1, \ldots, t_n)$ – атомарная, то $|A|_M$ однозначно определено – по лемме (6.3).
- Если $A = (B \wedge C)$, то надо положить $|A|_M = \min(|B|_M, |C|_M)$. Формулы B, C единственны по лемме (6.1) об однозначном анализе термов и формул, а $|B|_M$,

$|C|_M$ определены однозначно по предположению индукции (B, C – меньшей длины, чем A). Поэтому $|A|_M$ задаётся однозначно.

- Аналогично рассуждаем в случаях $A = \neg B$, $(B \vee C)$, $(B \to C)$.
- 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 $|A|_M$ задаётся 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', причём 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'). То есть $B' = [a'/a]B$.

  Отсюда получаем, что при всех $m \in M$ имеем: $[m/a']B' = [m/a'][a'/a]B = = [m/a]B$. Поэтому если мы определили $|A|_M = \max\limits_{m \in M} |[m/a]B|_M$, то также получаем и $|A|_M = \max\limits_{m \in M} |[m/a']B'|_M$. Таким образом, $|A|_M$ и в этом случае определено однозначно – независимо от того, используем мы B или B' для построения A.
- Случай $A = \forall x[x/a]B$ рассматривается аналогично.

□

Изоморфизмы моделей

Определим теперь точно, какие модели будут считаться «одинаковыми».

Определение 7.7. Пусть M, M' – модели сигнатуры Ω. Отображение $\alpha : \underline{M} \to \underline{M'}$ называется *изоморфизмом M на M'*, если:

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

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

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

Можно записать это определение короче. Обозначим $\vec{m} \coloneqq (m_1, \ldots, m_k)$. Тогда можно писать так:

- $\alpha(f_M(\vec{m})) = f_{M'}(\alpha\vec{m})$;
- $P_M(\vec{m}) = P_{M'}(\alpha\vec{m})$.

Определение 7.8. Модели M, M' называются *изоморфными* (обозначение: $M \cong M'$), если существует изоморфизм $\alpha : M \cong M'$.

Приведём пример.

Рассмотрим сигнатуру $(+, <, =)$. Приведём две изоморфных модели такой сигнатуры: $(\mathbb{N}_+, +_{\mathbb{N}_+}, <_{\mathbb{N}_+}, =_{\mathbb{N}_+}) \cong (\mathbb{N}_-, +_{\mathbb{N}_-}, >_{\mathbb{N}_-}, =_{\mathbb{N}_-})$.

Лемма 7.4. *Изоморфность – это отношение эквивалентности на моделях.*

Упражнение 7.1. Доказать лемму (7.4).

Посмотрим, как изменяются значения термов и формул при изоморфизме.

Пусть M, M' – модели сигнатуры Ω, $\alpha : M \cong M'$. Для терма t, оценённого в M, обозначим через $\alpha \cdot t$ терм, полученный заменой всех констант m из M на их образы $\alpha(m)$. Формально $\alpha \cdot t$ надо определять по индукции и доказывать, что $\alpha \cdot t$ – терм, оценённый в M'.

Упражнение 7.2. Докажите это, что $\alpha \cdot t$ – терм, оценённый в M'.

Аналогично по формуле A, оценённой в M, строится формула $\alpha \cdot A$, оценённая в M'.

Теорема 7.1. *Пусть M, M' – модели сигнатуры Ω, $\alpha : M \cong M'$.*
1) Если $t \in CTm_{\Omega \cup M}$, то $|\alpha \cdot t|_{M'} = \alpha(|t|_M)$.
2) Если $A \in CFm_{\Omega \cup M}$, то $|\alpha \cdot A|_{M'} = |A|_M$.

Доказательство:

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

1.1) (Базис индукции). $t = c$, для $c \in Const_\Omega$. Тогда $\alpha \cdot t = t = c$. Имеем: $|\alpha \cdot t|_{M'} = c_{M'} = \alpha(c_M) = \alpha(|t|_M)$ по определению значения терма (7.5) и определению изоморфизма (7.7).

1.2) (Базис индукции). $t = m$, для $m \in \underline{M}$. Тогда $\alpha \cdot t = \alpha(m)$, и утверждение очевидно: $|\alpha \cdot t|_{M'} = \alpha(m) = \alpha(|t|_M)$ по определению значения терма (7.5).

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

Получаем: $|\alpha \cdot t|_{M'} = f_{M'}(|\alpha \cdot t_1|_{M'}, \ldots, |\alpha \cdot t_n|_{M'}) = f_{M'}(\alpha(|t_1|_M), \ldots, \alpha(|t_n|_M))$ по определению значения терма (7.5) и предположению индукции для термов t_i. Далее, $f_{M'}(\alpha(|t_1|_M), \ldots, \alpha(|t_n|_M)) = \alpha(f_M(|t_1|_M, \ldots, |t_n|_M)) = \alpha(|t|_M)$ по определению значения терма (7.5) и определению изоморфизма (7.7). Таким образом, $|\alpha \cdot t|_{M'} = \alpha(|t|_M)$.

Пункт (2) докажем на следующей лекции. □

Лекция 8

Изоморфизмы моделей (продолжение)

Продолжаем доказательство теоремы (7.1).

Доказательство:

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

2.1) (Базис индукции). $A = P(t_1, \ldots, t_n)$ – атомарная (P^n – предикатный символ, $t_1, \ldots, t_n$ – термы). $|A|_M = P_M(|t_1|_M, \ldots, |t_n|_M)$ (определение значения терма (7.5)). С другой стороны, $|\alpha \cdot A|_{M'} = P_{M'}(|\alpha \cdot t_1|_{M'}, \ldots, |\alpha \cdot t_n|_{M'}) = = P_{M'}(\alpha(|t_1|_M), \ldots, \alpha(|t_n|_M)) = P_M(|t_1|_M, \ldots, |t_n|_M))$ по пункту (1) доказываемой теоремы и определению изоморфизма (7.7). Отсюда получаем: $|\alpha \cdot A|_{M'} = |A|_M$.

Упражнение 8.1. Доказать теорему для случаев:

2.2) $A = (B \wedge C)$;

2.3) $A = (B \vee C)$;

2.4) $A = (B \to C)$;

2.5) $A = \neg B$.

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

По определению истинности $|\alpha \cdot A|_{M'} = |\exists x[x/a](\alpha \cdot B)|_{M'} = \max\limits_{m' \in M'} |[m'/a](\alpha \cdot B)|_{M'} = = \max\limits_{m \in M} |[\alpha(m)/a](\alpha \cdot B)|_{M'}$. Последнее равенство следует из сюръективности α: все $m' \in M'$ – это в точности α-образы всех $m \in M$.

Также по определению истинности и предположению индукции для $[m/a]B$ имеем: $|A|_M = |\exists x[x/a]B|_M = \max\limits_{m \in M} |[m/a]B|_M = \max\limits_{m \in M} |\alpha \cdot [m/a]B|_{M'}$.

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

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

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

Этот случай совершенно аналогичен доказательству пункта (2.6) с заменой max на min. □

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

Доказательство:

Пусть $\alpha : M \cong M'$. Если A – замкнутая формула данной сигнатуры, то $\alpha \cdot A = A$, так как A не содержит констант из M. По пункту (2) теоремы (7.1) $|A|_M = |A|_{M'}$, или $M \vDash A \Leftrightarrow M' \vDash A$. Это выполняется для любой замкнутой A, а потому $Th(M) = Th(M')$, то есть $M \equiv M'$. □

Определимость и автоморфизмы

Определение 8.1. *Параметрами* формулы A (некоторой сигнатуры) называются входящие в неё свободные переменные. $FV(A)$ обозначает множество всех параметров формулы A.

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

Определение 8.2. *k-местный предикат, определимый формулой $A(\vec{b})$ в модели M* – это отображение $A_M : \underline{M}^k \to \{0,1\}$ такое, что для всех $m_1, \ldots, m_k$ имеем: $A_M(m_1, \ldots, m_k) \coloneqq |[m_1, \ldots, m_k/b_1, \ldots, b_k]A|_M$.

Здесь использовано обозначение многократной подстановки: $[m_1, \ldots, m_k/b_1, \ldots, b_k]A$ получается из A заменой $b_1, \ldots, b_k$ соответственно на $m_1, \ldots, m_k$. В сокращённых обозначениях определение записывается так: $A_M(\vec{m}) \coloneqq \coloneqq |A(\vec{m})|_M$ для всех $\vec{m} \in \underline{M}^k$.

Определение 8.3. k-местный предикат $\gamma : M^k \to \{0,1\}$ *определим в* M, если $\gamma = A_M$ для некоторой формулы A.

Любому k-местному предикату на множестве M, то есть отображению $\gamma : M^k \to \to \{0,1\}$, соответствует k-местное отношение на множестве M – это множество $R \subseteq M^k$, определяемое следующим образом: $R = \{\vec{m} \mid \gamma(\vec{m}) = 1\}$.

И наоборот, любому k-местному отношению $R \subseteq M^k$ соответствует k-местный предикат – его характеристическая функция $\chi_R : M^k \to \{0,1\}$, имеющая вид $\chi_R = = \begin{cases} 1, \text{ если } \vec{m} \in R \\ 0, \text{ иначе} \end{cases}$.

Приведём пример.

Рассмотрим опять сигнатуру колец и её модель $\mathbb{N}$ – множество натуральных чисел с обычными сложением, умножением, нулём и единицей. Рассмотрим в этой модели 2-местный предикат $M_1 \leq m_2$. Он определим формулой $\exists x(b_1 + x = b_2)$. Действительно, $\mathbb{N} \vDash \exists x(m_1 + x = m_2) \;\Leftrightarrow\; m_1 \leq m_2$.

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

Для того, чтобы задать порядок на множестве действительных чисел $\mathbb{R}$, сложения уже не хватит, то есть в $\mathbb{R}$ как модели сигнатуры $\{+, =\}$ предикат $m_1 \leq m_2$ не определим – это мы установим чуть позже. Но легко доказать определимость в сигнатуре колец: $\mathbb{R} \vDash \exists x(m_1 + x \cdot x = m_2) \;\Leftrightarrow\; m_1 \leq m_2$.

Определение 8.4. *Автоморфизм* модели – это её изоморфизм на себя.

Теорема 8.2. *Пусть α – автоморфизм модели M сигнатуры Ω, $A(\vec{b})$ – формула той же сигнатуры. Тогда $A_M(\alpha\vec{m}) = A_M(\vec{m})$ для всех $\vec{m} \in M$.*

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

Доказательство:

По определению (8.2) и теореме (7.1) имеем: $A_M(\alpha\vec{m}) = |A(\alpha\vec{m})|_M = |A(\vec{m})|_M = = A_M(\vec{m})$. □

Поскольку предикаты соответствуют отношениям, мы можем говорить и об определимости отношений.

Определение 8.5. k-местное отношение R *определимо в* M формулой $A(\vec{b})$, если определим соответствующий предикат, то есть для всех $\vec{m} \in M^k$ выполняется: $M \vDash A(\vec{m}) \Leftrightarrow \vec{m} \in R$.

Теорема (8.2) означает, что определимые отношения инвариантны при автоморфизмах: $\vec{m} \in R \Leftrightarrow \alpha\vec{m} \in R$.

В частности, при $k = 1$ подмножество $S \subseteq M$ определимо формулой $A(b)$, если для всех $m \in M$ выполняется: $M \vDash A(m) \Leftrightarrow m \in S$. Тогда $m \in S \Leftrightarrow \alpha(m) \in S$.

Приведём примеры.

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

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

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

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

3) Однако, если добавить в сигнатуру умножение, $\mathbb{N}$ станет определимым. Для этого можно применить теорему Лагранжа о представимости всякого натурального числа в виде суммы 4 квадратов: $\mathbb{Z} \vDash \exists x_1 \exists x_2 \exists x_3 \exists x_4 (x_1^2 + x_2^2 + x_3^2 + x_4^2 = m) \Leftrightarrow m \in \mathbb{N}$, где x^2 обозначает $x \cdot x$.

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

4) Более того, $\mathbb{N}$ определимо в модели $\mathbb{Q}$ сигнатуры $\{=^2_{\mathbb{Q}}, +^2_{\mathbb{Q}}, \cdot^2_{\mathbb{Q}}, 0_{\mathbb{Q}}\}$, но доказать это сложно.

Определение 8.6. Подмножества $\mathbb{N}$, определимые в сигнатуре колец (она же – сигнатура арифметики), называются *арифметическими*.

Как и в случае $\mathbb{Z}$, множество таких подмножеств счётно. Однако теорема (8.2) никак не помогает построить конкретные неарифметические множества: легко видеть, что единственный автоморфизм модели $\mathbb{N}$ – тождественный.

Стандартные теории равенства и нормальные модели

Пусть $A = A(b_1, \ldots, b_n)$ – формула. 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: например, последовательное навешивание кванторов $\forall x_n, \ldots, \forall x_1$ даёт формулу $\forall x_1 \ldots \forall x_n A(x_1, \ldots, x_n)$.)

Лемма 8.1. *Пусть $A(b_1, \dots, b_n)$ – формула сигнатуры Ω, $x_1, \dots, x_n$ – (различные) связанные переменные, не входящие в A. Тогда для любой модели M сигнатуры Ω имеем:*

$$M \vDash \forall \vec{x} A(\vec{x}) \;\Leftrightarrow\; \text{для любого } \vec{m} \in M^n \;\; M \vDash A(\vec{m});$$

$$M \vDash \exists \vec{x} A(\vec{x}) \;\Leftrightarrow\; \text{существует } \vec{m} \in M^n \;\; M \vDash A(\vec{m}).$$

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 $B(b_1) \coloneqq \forall x_2 \dots \forall x_n A(b_1, x_2, \dots, x_n)$. И тогда $M \vDash A \;\Leftrightarrow$ для любого $m_1 \in M \;\; M \vDash B(m_1)$.

Но $B(m_1) = \forall x_2 \dots \forall x_n A(m_1, x_2, \dots, x_n)$ – это формула в сигнатуре $\Omega \cup M$. Применим к ней предположение индукции: $M \vDash \forall x_2 \dots \forall x_n A(m_1, x_2, \dots, x_n) \;\Leftrightarrow$ для любых $m_2, \dots, m_n \in M \;\; M \vDash A(m_1, m_2, \dots, m_n)$.

Таким образом, получаем утверждение леммы. Это – шаг индукции, а базис (при $n = 1$) очевиден. □

Теперь рассмотрим сигнатуру Ω, содержащую предикатный символ равенства $(= {}^2)$ (и, возможно, другие символы). В этой сигнатуре рассмотрим теорию Eq_Ω со следующими *стандартными аксиомами равенства*:

0) аксиомы теории Eq: рефлексивность, симметричность и транзитивность;

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

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

Запишем аксиомы (1) и (2) в сокращённом виде:

1) $\forall \vec{x} \forall \vec{y} (\vec{x} = \vec{y} \to f^n(\vec{x}) = f^n(\vec{y}))$ для всех $f^n \in Fun_\Omega$;

2) $\forall \vec{x} \forall \vec{y} (\vec{x} = \vec{y} \to (P^n(\vec{x}) \leftrightarrow P^n(\vec{y})))$ для всех $P^n \in Pred_\Omega$.

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

Лемма 8.2. *Если M – нормальная модель сигнатуры с равенством Ω, то $M \vDash Eq_\Omega$.*

Доказательство:

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

По лемме (8.1) аксиомы (1) верны в M, если и только если для всех $\vec{m}, \vec{m}' \in \in M^n$ выполнено: $M \vDash \vec{m} = \vec{m}' \to f(\vec{m}) = f(\vec{m}')$ (где $\vec{m} = \vec{m}'$ – сокращение для $m_1 = m_1' \wedge \dots \wedge m_n = m_n'$).

Но последнее утверждение очевидно: в нормальной модели $M \vDash \vec{m} = \vec{m}'$ означает, что $\vec{m}$ и $\vec{m}'$ совпадают; тогда и $f_M(\vec{m}) = f_M(\vec{m}')$.

Аналогично рассуждаем для аксиом (2): $M \vDash \vec{m} = \vec{m}' \to (P(\vec{m}) \leftrightarrow P(\vec{m}'))$, так как из совпадения $\vec{m}$ и $\vec{m}'$ следует, что $|P(\vec{m})|_M = |P(\vec{m}')|_M$, а потому $|P(\vec{m}) \leftrightarrow \leftrightarrow P(\vec{m}')|_M = 1$. □

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

Пусть $M \vDash Eq_\Omega$. Тогда предикат $=_M$ задаёт отношение эквивалентности на M, которое мы обозначим $\approx$. То есть $m_1 \approx m_2 \Leftrightarrow =_M(m_1, m_2) = 1 \Leftrightarrow M \vDash m_1 = m_2$. Это действительно отношение эквивалентности, благодаря аксиомам Eq. Класс эквивалентности элемента m по $\approx$ обозначим через $\widetilde{m}$.

На фактор-множестве $\underline{M}/\approx$ зададим нормальную модель $\widetilde{M}$ сигнатуры Ω следующим образом:

$$c_{\widetilde{M}} \coloneqq \widetilde{c_M};$$
$$f^k_{\widetilde{M}}(\widetilde{m}_1, \dots, \widetilde{m}_k) \coloneqq \widetilde{f^k_M(m_1, \dots, m_k)};$$
$$P^k_{\widetilde{M}}(\widetilde{m}_1, \dots, \widetilde{m}_k) \coloneqq P^k_M(m_1, \dots, m_k)$$

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

Лемма 8.3. *Пусть $M \vDash Eq_\Omega$. Тогда $\widetilde{M}$ корректно определена.*

Доказательство:

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

Действительно, пусть $m_1 \approx m'_1, \ \dots, \ m_k \approx m'_k$. Это означает, что $M \vDash m_i = m'_i$ для $i \le k$, и тогда, в обозначениях из доказательства леммы (8.2), $M \vDash \vec{m} = \vec{m}'$, где $\vec{m} = (m_1, \dots, m_k)$, $\vec{m}' = (m'_1, \dots, m'_k)$. Как уже мы видели в доказательстве леммы (8.2), из аксиом (1) тогда следует, что $M \vDash f(\vec{m}) = f(\vec{m}')$, то есть $f_M(\vec{m}) = f_M(\vec{m}')$ (так как модель нормальна).

Аналогично, из аксиом (2) получаем: $M \vDash P(\vec{m}) \leftrightarrow P(\vec{m}')$, то есть $P_M(\vec{m}) = = P_M(\vec{m}')$. □

Лекция 9

Стандартные теории равенства и нормальные модели (продолжение)

На прошлой лекции по модели M стандартной теории равенства Eq_Ω мы построили модель $\widetilde{M}$ с носителем $\underline{M}/\approx$. Тогда имеется сюръекция $\alpha : \underline{M} \to \underline{M}/\approx$, переводящая каждый элемент $m \in M$ в его класс эквивалентности $\widetilde{m}$. Благодаря определению $\widetilde{M}$, α – сильный гомоморфизм, то есть

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

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

Лемма 9.1 (Лемма о нормализации)**.**
1) Для любого оценённого терма $t \in CTm_{\Omega\cup M}$ имеем: $|\alpha \cdot t|_{\widetilde{M}} = \alpha(|t|_M) = \widetilde{|t|_M}$.
2) Для любой оценённой формулы $A \in CFm_{\Omega\cup M}$ имеем: $|\alpha \cdot A|_{\widetilde{M}} = |A|_M$.
3) $M \equiv \widetilde{M}$.

Доказательство:
См. доказательство теоремы (7.1). В доказательстве используется только то, что α – сюръекция. □

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

Определение 9.1. Пусть T – теория в сигнатуре с равенством Ω, содержащая Eq_Ω. Теория T называется *сильно категоричной*, если все её нормальные модели изоморфны.

Теорема 9.1. *Если теория T сильно категорична, то она полна.*

Доказательство:
По лемме (7.2) достаточно доказать, что все модели T элементарно эквивалентны.
Рассмотрим модели $M, M' \vDash T$. По лемме (8.3) $M \equiv \widetilde{M}$, $M' \equiv \widetilde{M'}$. Поэтому $\widetilde{M}, \widetilde{M'} \vDash T$. Так как эти модели нормальны, по условию они изоморфны. Следовательно, $\widetilde{M} \equiv \widetilde{M'}$ (теорема (8.1)). В итоге имеем $M \equiv M'$. □

Приведём примеры.
1) В сигнатуре $\{=\}$ рассмотрим теорию $Eq \cup \{A_{=n}\}$ (ещё один вариант записи: $Eq + \{A_{=n}\}$), где

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

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

Эта аксиома утверждает, что в (нормальной) модели ровно n элементов: $M \vDash A_{=n} \Leftrightarrow |M| = n$. Очевидно, что данная теория сильно категорична.

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

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

$\forall x \forall y \forall z(x < y \wedge y < z \to x < z)$ (транзитивность);

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

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

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

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

Рассмотрим в этой сигнатуре *теорию групп* Gr со следующими аксиомами;

1) стандартные аксиомы равенства;

2) 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).

Теории $Gr + A_{=p}$, где p – простое, сильно категоричны (так как группа простого порядка – циклическая), а потому полны.

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

Теория конечной модели

Определение 9.2. Теория T называется *конечно аксиоматизируемой*, если она эквивалентна некоторой конечной теории.

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

Теорема 9.2. *В конечной сигнатуре с равенством элементарная теория конечной модели конечно аксиоматизируема и сильно категорична.*

Доказательство:

Пусть M – конечная модель конечной сигнатуры Ω. Мы построим формулу A_M, которая полностью описывает M.

Пусть $\underline{M} = \{m_1, \ldots, m_n\}$. Положим $A_M \coloneqq \exists v_1 \ldots \exists v_n \psi_M(v_1, \ldots, v_n)$, где

$$\psi_M(a_1, \ldots, a_n) \coloneqq \bigwedge_{1 \le i < j \le n} (a_i \neq a_j) \wedge \forall v_{n+1} \bigvee_{i=1}^{n} (v_{n+1} = a_i) \wedge$$
$$\wedge \bigwedge \{c = a_i \mid c \in Const_\Omega,\ c_M \text{ равно } m_i\} \wedge$$
$$\wedge \bigwedge \{f^k(a_{i_1}, \ldots, a_{i_k}) = a_j \mid f^k \in Fun_\Omega,\ f^k_M(m_{i_1}, \ldots, m_{i_k}) \text{ равно } m_j\} \wedge$$
$$\wedge \bigwedge \{P^k(a_{i_1}, \ldots, a_{i_k}) \mid P^k \in Pred_\Omega,\ M \vDash P^k(m_{i_1}, \ldots, m_{i_k})\} \wedge$$
$$\wedge \bigwedge \{\neg P^k(a_{i_1}, \ldots, a_{i_k}) \mid P^k \in Pred_\Omega,\ M \vDash \neg P^k(m_{i_1}, \ldots, m_{i_k})\}.$$

Лемма 9.2. *Для нормальной модели M' сигнатуры Ω имеем:*

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

Доказательство:

Докажем $\Leftarrow$. Заметим, что $M \vDash \psi_M(m_1, \ldots, m_n)$. Действительно,

$$\psi_M(m_1, \ldots, m_n) = \bigwedge_{1 \le i < j \le n} (m_i \neq m_j) \wedge \forall v_{n+1} \bigvee_{i=1}^{n} (v_{n+1} = m_i) \wedge$$
$$\wedge \bigwedge \{c = m_i \mid c \in Const_\Omega,\ c_M \text{ равно } m_i\} \wedge$$
$$\wedge \bigwedge \{f^k(m_{i_1}, \ldots, m_{i_k}) = m_j \mid f^k \in Fun_\Omega,\ f^k_M(m_{i_1}, \ldots, m_{i_k}) \text{ равно } m_j\} \wedge$$
$$\wedge \bigwedge \{P^k(m_{i_1}, \ldots, m_{i_k}) \mid P^k \in Pred_\Omega,\ M \vDash P^k(m_{i_1}, \ldots, m_{i_k})\} \wedge$$
$$\wedge \bigwedge \{\neg P^k(m_{i_1}, \ldots, m_{i_k}) \mid P^k \in Pred_\Omega,\ M \vDash \neg P^k(m_{i_1}, \ldots, m_{i_k})\}.$$

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

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

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

3) $M \vDash \bigwedge\{c = m_i \mid c \in Const_\Omega,\ c_M \text{ равно } m_i\}$, так как для всякой константы c имеем: $M \vDash c = m_i$, если c_M равно m_i – это очевидно, по определению истинности (см. определения (7.5) и (7.6)).

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

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

6) Также очевидно.

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

Докажем $\Rightarrow$. Предположим, что $M' \vDash A_M$ и построим изоморфизм M на M'. Снова по лемме (8.1), найдутся $m'_1, \ldots, m'_n \in M'$, для которых $M' \vDash \psi_M(m'_1, \ldots, m'_n)$.

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

$$\psi_M(m'_1, \dots, m'_n) = \bigwedge_{1 \le i < j \le n} (m'_i \neq m'_j) \wedge \forall v_{n+1} \bigvee_{i=1}^{n} (v_{n+1} = m'_i) \wedge$$
$$\wedge \bigwedge \{c = m'_i \mid c \in Const_\Omega,\ c_M \text{ равно } m_i\} \wedge$$
$$\wedge \bigwedge \{f^k(m'_{i_1}, \dots, m'_{i_k}) = m'_j \mid f^k \in Fun_\Omega,\ f^k_M(m_{i_1}, \dots, m_{i_k}) \text{ равно } m_j\} \wedge$$
$$\wedge \bigwedge \{P^k(m'_{i_1}, \dots, m'_{i_k}) \mid P^k \in Pred_\Omega,\ M \vDash P^k(m_{i_1}, \dots, m_{i_k})\} \wedge$$
$$\wedge \bigwedge \{\neg P^k(m'_{i_1}, \dots, m'_{i_k}) \mid P^k \in Pred_\Omega,\ M \vDash \neg P^k(m_{i_1}, \dots, m_{i_k})\}.$$

Докажем, что отображение φ, переводящее каждый m_i в m'_i, то есть $\varphi(m_i) := m'_i$, – искомый изоморфизм.

1) φ – инъекция. Это обеспечивает 1-й член конъюнкции: при $i < j$ $M \vDash m'_i \neq m'_j$, то есть m'_i и m'_j не совпадают.

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

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

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

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

6) Если же $M \vDash \neg P^k(m_{i_1}, \dots, m_{i_k})$, то из 6-го члена получаем: $M' \vDash \neg P^k(m'_{i_1}, \dots, m'_{i_k})$. □

Продолжим доказательство теоремы.

Заметим, что $Th(M) \sim \{A_M\}$. (Эквивалентность здесь понимается относительно нормальных моделей. Если рассматривать произвольные модели, то надо добавить ещё Eq_Ω.) Действительно, по лемме (9.2) $A_M \in Th(M)$, значит, $M' \vDash Th(M) \Rightarrow M' \vDash A_M$. Обратно, пусть $M' \vDash A_M$. По той же лемме $M' \cong M$. И тогда $M' \vDash Th(M)$.

Итак, $Th(M)$ конечно аксиоматизируема.

Также $Th(M)$ сильно категорична, так как эквивалентная ей теория $\{A_M\}$ сильно категорична по лемме (9.2). □

Общезначимость и равносильность

Определение 9.3. Замкнутые формулы A, B (в некоторой сигнатуре) называются *равносильными*, если формула $A \leftrightarrow B$ общезначима.

Определение 9.4. Пусть $A(b_1, \dots, b_n) \in Fm_\Omega$. Тогда *универсальным замыканием* формулы A называется формула $\forall x_1 \dots \forall x_n A(x_1, \dots, x_n)$, где $x_1, \dots, x_n$ – различные новые связанные переменные.

Лемма 9.3. *Пусть $A(\vec{b})$ – формула сигнатуры Ω; $\vec{x}, \vec{y}$ – списки (той же длины, что $\vec{b}$) различных связанных переменных, не входящих в A. Тогда $\forall \vec{x} A(\vec{x}) \sim \forall \vec{y} A(\vec{y})$.*

Доказательство:
Из леммы (8.1) получаем:

$$M \vDash \forall \vec{x} A(\vec{x}) \;\Leftrightarrow\; \text{для всех } \vec{m} \in M^n \;\; M \vDash A(\vec{m})$$

и

$$M \vDash \forall \vec{y} A(\vec{y}) \;\Leftrightarrow\; \text{для всех } \vec{m} \in M^n \;\; M \vDash A(\vec{m}).$$

Поэтому $M \vDash \forall \vec{x} A(\vec{x}) \;\Leftrightarrow\; M \vDash \forall \vec{y} A(\vec{y})$. □

Определение 9.5. Формула $A(\vec{b})$ называется *общезначимой* (обозначение: $\vDash A(\vec{b})$), если общезначимо её универсальное замыкание, если для всех моделей M имеем: $M \vDash \forall \vec{x} A(\vec{x})$.

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

Определение 9.6. Формулы $A(\vec{b}), B(\vec{b})$ называются *равносильными* (обозначение: $A(\vec{b}) \sim B(\vec{b})$), если $\vDash \overline{\forall}(A \leftrightarrow B)$.

По лемме (8.1) имеем (подразумевается, что M – в нужной сигнатуре, а $\vec{m}$ – список её элементов нужной длины):

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

Лемма 9.4. *$\sim$ задаёт отношение эквивалентности на Fm_Ω.*

Доказательство:
Если $|A(\vec{m})|_M = |B(\vec{m})|_M$ и $|B(\vec{m})|_M = |C(\vec{m})|_M$, то $|A(\vec{m})|_M = |C(\vec{m})|_M$. □

Определение 9.7. Пусть теперь $F(P_1, \ldots, P_n)$ – пропозициональная формула, построенная из пропозициональных переменных $P_1, \ldots, P_n$, а $A_1, \ldots, A_n$ – формулы сигнатуры Ω. Пусть S – подстановка, заменяющая каждое вхождение P_i на A_i. При этой замене из F получится формула сигнатуры Ω, которую мы обозначим SF, или $F(A_1, \ldots, A_n)$. Такая формула называется *подстановочным примером* формулы F.

Сформулируем две леммы, которые докажем на следующей лекции.

Лемма 9.5 (Лемма о тавтологиях)**.** *Если F – тавтология, то $\vDash SF$.*

Лемма 9.6.
1) Если $F_1 \sim F_2$, то $SF_1 \sim SF_2$.
2) $\neg \forall x[x/a]A \sim \exists x[x/a]\neg A$.
3) $\neg \exists x[x/a]A \sim \forall x[x/a]\neg A$.
Далее Я обозначает квантор $\forall$ или $\exists$.

4) $\forall x[x/a](A \circ B) \sim (\forall x[x/a]A \circ B)$, *если* a *не входит в* B *(и* x *не входит ни в* A*, ни в* B*). Здесь* $\circ$ *– это* $\vee$ *или* $\wedge$*.*

5) Если $A \sim B$*, то* $\neg A \sim \neg B$*.*

6) Если $A \sim A'$ *и* $B \sim B'$ *то* $(A \circ B) \sim (A' \circ B')$*. Здесь* $\circ$ *– это* $\vee$*,* $\wedge$ *или* $\to$*.*

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

8) $\forall x[x/a]A \sim \forall y[y/a]A \sim \forall y[y/b][b/a]A$*, если* x, y, b *не входят в* A *(здесь* $x, y \in BVar$ *и* $a, b \in FVar$*).*

Лекция 10

Общезначимость и равносильность (продолжение)

Докажем лемму (9.5) о тавтологиях.

Доказательство:

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

Рассмотрим произвольную модель M данной сигнатуры и её элементы $m_1, \dots, m_k$. Обозначим $B'_i := B_i(m_1, \dots, m_k)$ (это – оценённые в M формулы), и построим оценку пропозициональных переменных $\theta : Var \to \{0, 1\}$ так: $\theta(P_i) := |B'_i|_M$.

Покажем, что для любой пропозициональной формулы $F(P_1, \dots, P_n)$ имеем: $\theta(F) = |SF(m_1, \dots, m_k)|_M$. Это легко проверяется по индукции (по длине F). Действительно, если $F = P_i$, то это следует из определения θ, так как $SP_i = B_i$. А шаг индукции очевиден: например, при $F = F_1 \wedge F_2$ имеем:

$$\begin{aligned} SF &= SF_1 \wedge SF_2; \\ \theta(F) &= \min(\theta(F_1), \theta(F_2)); \\ |SF(m_1, \dots, m_k)|_M &= \min(|SF_1(m_1, \dots, m_k)|_M, |SF_2(m_1, \dots, m_k)|_M), \end{aligned}$$

и можно применить предположение индукции.

Из доказанного утверждения сразу следует, что если F – тавтология, то $M \vDash SF(m_1, \dots, m_k)$ для любой M и при любом выборе $m_1, \dots, m_k$. Это даёт общезначимость SF. □

Докажем лемму (9.6).

Доказательство:

1) Если $(F_1 \leftrightarrow F_2)$ – тавтология, то по лемме (9.5) о тавтологиях $\vDash S(F_1 \leftrightarrow F_2)$. Но $S(F_1 \leftrightarrow F_2) = (SF_1 \leftrightarrow SF_2)$. Тогда по определению равносильности $SF_1 \sim SF_2$.

2) Запишем A как $A(a, \vec{b})$; надо проверить, что в любой модели M для всех $\vec{m}$ выполняется: $|\neg\forall x A(x, \vec{m})|_M = |\exists x \neg A(x, \vec{m})|_M$.

Но это сразу следует из определения истинности: $|\neg\forall x A(x, \vec{m})|_M = 1 \Leftrightarrow$ $\Leftrightarrow |\forall x A(x, \vec{m})|_M = 0 \Leftrightarrow$ не для всех $k \in M$ $|A(k, \vec{m})|_M = 1 \Leftrightarrow$ найдётся $k \in M$, для которого $|A(k, \vec{m})|_M = 0 \Leftrightarrow$ найдётся $k \in M$, для которого $|\neg A(k, \vec{m})|_M = 1 \Leftrightarrow$ $\Leftrightarrow |\exists x \neg A(x, \vec{m})|_M = 1$.

3) Доказывается аналогично доказательству пункта (2).

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

Запишем A как $A(a, \vec{b})$, а B – как $B(\vec{b})$ (поскольку a не входит в B). Надо доказать, что в любой модели M для любого $\vec{m}$ выполняется: $|\exists x(A(x, \vec{m}) \wedge B(\vec{m}))|_M = 1 \Leftrightarrow$ $\Leftrightarrow |\exists x A(x, \vec{m}) \wedge B(\vec{m})|_M = 1$.

В самом деле, $|\exists x(A(x, \vec{m}) \wedge B(\vec{m}))|_M = 1 \Leftrightarrow$ найдётся k такое, что $|A(k, \vec{m}) \wedge$ $\wedge B(\vec{m})|_M = 1 \Leftrightarrow$ найдётся k такое, что ($|A(k, \vec{m})|_M = 1$ и $|B(\vec{m})|_M = 1$).

Но условие $|B(\vec{m})|_M = 1$ не зависит от k. Поэтому: найдётся k такое, что ($|A(k,\vec{m})|_M = 1$ и $|B(\vec{m})|_M = 1$) $\Leftrightarrow$ (найдётся k такое, что $|A(k,\vec{m})|_M = 1$) и $|B(\vec{m})|_M = 1 \Leftrightarrow |\exists x A(x,\vec{m})|_M = 1$ и $|B(\vec{m})|_M = 1 \Leftrightarrow |\exists x A(x,\vec{m}) \wedge B(\vec{m})|_M = 1$.

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

7) Рассмотрим случай Я $= \exists$.

Запишем A как $A(a,\vec{b})$ и B – как $B(a,\vec{b})$. По определению истинности, в модели M для любого $\vec{m}$ имеем: $|\exists[x/a]A(a,\vec{m})|_M = \max\limits_{k\in M}|A(k,\vec{m})|_M$. По тому же определению получаем: $|\exists[x/a]B(a,\vec{m})|_M = \max\limits_{k\in M}|B(k,\vec{m})|_M$. Таким образом, равносильность из пункта (7) очевидна, так как $A \sim B$.

8) Рассмотрим случай Я $= \exists$.

Запишем A как $A(a,\vec{e})$, где $\vec{e}$ – список всех параметров, кроме a. По определению истинности, в модели M для любого $\vec{m}$ имеем: $|\exists x A(x,\vec{m})|_M = \max\limits_{k\in M}|A(k,\vec{m})|_M$. По тому же определению получаем: $|\exists y A(y,\vec{m})|_M = \max\limits_{k\in M}|A(k,\vec{m})|_M$. Таким образом, первая равносильность из пункта (8) очевидна.

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

Упражнение 10.1. Доказать оставшиеся пункты теоремы (9.6).

□

Предваренная нормальная форма

Определение 10.1. *Формула с тесными отрицаниями (ТО)* – это формула, построенная из литералов (то есть атомарных формул и их отрицаний) с помощью конъюнкции, дизъюнкции и кванторов.

Точное определение – индуктивное:

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

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

Доказательство:

Идея доказательства состоит в том, что импликацию можно выразить через отрицание и дизъюнкцию, а все отрицания можно задвинуть вглубь, используя законы Де Моргана и пункты (2), (3) леммы (9.6).

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

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

1) A – атомарная. Тогда A – ТО-формула, и доказывать нечего.

2) $A = (B \circ C)$, где $\circ$ – это $\wedge$ или $\vee$. Формулы B, C короче, и по предположению индукции найдутся ТО-формулы B_1, C_1 такие, что $B \sim B_1$, $C \sim C_1$. Тогда по пункту (6) леммы (9.6) имеем: $A \sim (B_1 \circ C_1)$, а по определению (10.1) ТО-формулы имеем: $(B_1 \circ C_1)$ – ТО-формула. Переменные в ней те же, что в A, так как по предположению индукции они не изменяются при переходе от B к B_1 и от C к C_1.

3) $A = (B \to C)$. Из логики высказываний (пункт (1) леммы (9.6)) получаем: $A \sim (\neg B \vee C)$. Формулы $\neg B$, C короче, чем A, и тогда найдутся ТО-формулы B_1, C_1 такие, что $\neg B \sim B_1$, $C \sim C_1$. По пункту (6) леммы (9.6) имеем: $A \sim (B_1 \vee C_1)$, а по определению (10.1) ТО-формулы имеем: $(B_1 \vee C_1)$ – ТО-формула. Переменные не меняются по предположению индукции (как и в доказательстве пункта (2)).

4) $A = Яx[x/a]B$, где x не входит в B. По предположению индукции $B \sim B_1$ для некоторой ТО-формулы B_1 с теми же переменными. Поэтому x не входит в B_1, и по пункту (7) леммы (9.6) имеем: $A \sim Яx[x/a]B_1$. Ясно, что $Яx[x/a]B_1$ – ТО-формула, и переменные из A в ней сохраняются.

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

5.1) B – атомарная. Тогда A – ТО-формула, и доказывать нечего.

5.2) $B = (C \vee D)$. Из логики высказываний (закон Де Моргана) имеем: $A \sim$ $\sim (\neg C \wedge \neg D)$. Формулы $\neg C$, $\neg D$ – короче, поэтому найдутся ТО-формулы C_1, D_1, для которых $\neg C \sim C_1$, $\neg D \sim D_1$. По пункту (6) леммы (9.6) имеем: $A \sim (C_1 \wedge D_1)$, и снова получаем ТО-формулу. Переменные, как и раньше, сохраняются.

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

5.4) $B = (C \to D)$. Из логики высказываний $A = \neg(C \to D) \sim (C \wedge \neg D)$. Так как C, $\neg D$ короче, чем A, имеем ТО-формулы C_1, D_1, для которых $C \sim C_1$, $\neg D \sim D_1$. По пункту (6) леммы (9.6) имеем: $A \sim (C_1 \wedge D_1)$.

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

5.6) $B = \forall x[x/a]C$, где x не входит в C. По пункту (2) леммы (9.6) имеем: $A =$ $= \neg B \sim \exists x[x/a]\neg C$. Так как $\neg C$ короче, чем A, имеется ТО-формула C_1 такая, что $\neg C \sim C_1$. Из-за сохранения переменных x не входит в C_1. По пункту (7) леммы (9.6) имеем: $\exists x[x/a]\neg C \sim \exists x[x/a]C_1$. Итак, A равносильна ТО-формуле $\exists x[x/a]C_1$ с теми же переменными.

5.7) $B = \exists x[x/a]C$. Этот случай аналогичен доказательству пункта (5.6). □

Определение 10.2. *Предваренная нормальная форма (ПНФ)* – это формула вида

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

где $Я_1, \dots, Я_n$ – кванторы, A – формула без кванторов, $a_1, \dots, a_n$ – (различные) свободные переменные, $x_1, \dots, x_n$ – (различные) связанные переменные, не входящие в A. Формула без кванторов тоже считается ПНФ.

Теорема 10.1. *Любая формула первого порядка равносильна некоторой ПНФ.*

Доказательство:

Благодаря лемме (10.1) достаточно доказать это для ТО-формул. То есть индукцией по длине ТО-формулы A доказываем, что A равносильна ПНФ. По лемме (6.1) об однозначном анализе термов и формул возникают такие случаи.

1) A – литерал. Тогда A – ПНФ по определению.

2) $A = (B \circ C)$, где $\circ$ – это $\vee$ или $\wedge$. По предположению индукции $B \sim B'$, $C \sim C'$ для некоторых ПНФ B', C'. Тогда по пункту (6) леммы (9.6) имеем: $A = (B \circ C) \sim$ $\sim (B' \circ C')$. Теперь нужна ещё одна лемма.

Лемма 10.2. *Если A, B – ПНФ, $\circ$ – это $\vee$ или $\wedge$, то формула $(A \circ B)$ равносильна ПНФ.*

Доказательство:

Доказываем индукцией по числу кванторов в $(A \circ B)$.

Если кванторов нет, то это уже ПНФ, и доказывать нечего.

Если есть кванторы, то мы можем считать, что они есть в A: если они есть только в B, можно переставить A и B, так как $(A \circ B) \sim (B \circ A)$ (логика высказываний).

Итак, пусть $A = \forall x[x/a]A_1$.

Случай 1. a, x не входят в B.

По пункту (4) леммы (9.6) имеем: $(A \circ B) = (\forall x[x/a]A_1 \circ B) \sim \forall x[x/a](A_1 \circ B)$. Число кванторов в $A_1 \circ B$ меньше, чем в $A \circ B$, и по предположению индукции $(A_1 \circ B) \sim C$ для некоторой ПНФ C.

Случай 1.1. Если x не входит в C, то по пункту (7) леммы (9.6) имеем: $\forall x[x/a](A_1 \circ B) \sim \forall x[x/a]C$. Таким образом, $(A \circ B)$ равносильна ПНФ $\forall x[x/a]C$.

Случай 1.2. Если x входит в C, то возьмём новую связанную переменную y, которой нет в A_1, B, C. По пункту (8) леммы (9.6) имеем: $A = \forall x[x/a]A_1 \sim \forall y[y/a]A_1$, и далее $(A \circ B) \sim (\forall y[y/a]A_1 \circ B)$. Теперь, как в случае (1.1): $(\forall y[y/a]A_1 \circ B) \sim$ $\sim \forall y[y/a]C$.

Случай 2. a или x входит в B.

Тогда можно эти переменные переименовать. А именно, выберем $b \in FVar$, $y \in$ $\in BVar$, которые не входят в B. По пункту (8) леммы (9.6) имеем: $A = \forall x[x/a]A_1 \sim$ $\sim \forall y[y/b][b/a]A_1$. Формула $\forall y[y/b][b/a]A_1$ равносильна ПНФ, согласно случаю (1) (где вместо A_1 надо использовать $[b/a]A_1$). □

Возвращаемся к пункту (2) доказательства теоремы. По лемме (10.2) получаем, что $(B' \circ C')$ равносильна ПНФ, поэтому и A равносильна ПНФ.

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

По предположению индукции, имеется ПНФ B', равносильная B. Выберем какую-нибудь связанную переменную y, не входящую ни в B, ни в B'. По пунктам (8), (7) леммы (9.6) получаем: $A = \forall x[x/a]B \sim \forall y[y/a]B \sim \forall y[y/a]B'$. Формула $\forall y[y/a]B'$ – ПНФ. □

Приведём пример.

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

Подробнее, это происходит так: $(\forall x[x/a]P(a) \vee \exists x[x/a]Q(a)) \sim (\forall x[x/a]P(a) \vee \vee \exists y[y/b]Q(b)) \sim \forall x[x/a](P(a) \vee \exists y[y/b]Q(b)) \sim \forall x \exists y[x, y/a, b](P(a) \vee Q(b))$.

Замечание 10.1. В логике высказываний мы можем выяснить, является ли данная формула тавтологией, приведя её к СДНФ. В логике предикатов аналогичный метод не работает: у одной и той же формулы могут быть несколько совершенно разных ПНФ. И по данной ПНФ непонятно, как установить общезначимость. В частности, неверно, что $\vDash Я x_1 \dots Я x_n[x_1, \dots, x_n/a_1, \dots, a_n]A \Rightarrow \vDash A$.

Например, формула $\exists x \forall y(P(x) \to P(y))$ общезначима, так как $\exists x \forall y(P(x) \to \to P(y)) \sim \exists x \forall y(\neg P(x) \vee P(y)) \sim \exists x(\neg P(x) \vee \forall y P(y)) \sim (\exists x \neg P(x) \vee \forall y P(y)) \sim \sim (\neg \forall x P(x) \vee \forall y P(y)) \sim (\neg \forall x P(x) \vee \forall x P(x))$. При этом формула $P(x) \to P(y)$ совсем не общезначима.

Лекция 11

Исчисление предикатов

Определение 11.1. *Исчисление предикатов в сигнатуре* Ω – это аксиоматическая система гильбертовского типа. Она обозначается через PC_Ω и задаётся следующими аксиомами и правилами вывода.

I. 10 схем аксиом исчисления высказываний CL (см. лекцию 4). Но теперь A, B, C могут быть любыми формулами сигнатуры Ω.

II. Предикатные аксиомы:

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

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

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

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

Здесь A, B – произвольные формулы, t – произвольный терм, a – свободная переменная, x – связанная переменная. Формула $[t/a]A$ получается из A заменой всех вхождений a на t. Переменная x не должна входить в A и B. В аксиомах 3, 4 переменная a не должна входить в A.

III. Правила вывода:

ModusPonens (MP): $\dfrac{A,\ A \to B}{B}$;

Gen (правило обобщения): $\dfrac{A}{\forall x[x/a]A}$. Здесь предполагается, что x не входит в A.

Определение вывода в исчислении предикатов аналогично исчислению высказываний, но здесь добавляется ещё правило Gen.

Определение 11.2. Пусть Γ – некоторое множество формул сигнатуры Ω. *Вывод формулы* A *в* PC_Ω *из* Γ – это конечная последовательность формул, каждая из которых – аксиома, или принадлежит Γ, или получается из предыдущих по правилу MP или Gen, а последняя формула есть A.

То есть это последовательность формул $A_1, \ldots, A_n = A$, где для всех k выполняется одно из условий:

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

Определение 11.3. Формула A *выводима из* Γ, если существует её вывод из Γ; обозначение: $\Gamma \vdash_{PC_\Omega} A$.

Для этой выводимости существует аналог леммы (4.1) с тем же доказательством.

Лемма 11.1.
1) Если $\Delta \subseteq \Gamma$ *и* $\Delta \vdash_{PC_\Omega} A$, *то* $\Gamma \vdash_{PC_\Omega} A$.
2) Если $\Gamma \vdash_{PC_\Omega} A$, *то существует конечное* $\Delta \subseteq \Gamma$, *для которого* $\Delta \vdash_{PC_\Omega} A$.
3) Если $\Delta \vdash_{PC_\Omega} \Gamma$ *и* $\Gamma \vdash_{PC_\Omega} A$, *то* $\Delta \vdash_{PC_\Omega} A$.

Лемма 11.2. *Пусть* A – *пропозициональная формула,* SA – *её подстановочный пример в сигнатуре* Ω. *Если* $\vdash_{CL} A$, *то* $\vdash_{PC_\Omega} SA$.

Поскольку теоремы CL – это в точности тавтологии (см. лекцию 5), то лемму можно сформулировать так: все подстановочные примеры тавтологий выводимы в исчислении предикатов.

Доказательство:
Индукция по длине вывода A в CL.
1) Если A – аксиома, то SA – аксиома того же вида. Это получается из того, что подстановка S дистрибутивна относительно логических связок. Например, если A – аксиома 1: $A = B \to (C \to B)$, то $SA = SB \to (SC \to SB)$, и это аксиома I.1 (в исчислении предикатов). Аналогично для других аксиом.
2) Пусть A получается по правилу MP из B и $B \to A$. По предположению индукции в PC_Ω выводимы SB и $S(B \to A)$. Но $S(B \to A) = SB \to SA$. Применив MP в исчислении предикатов, получим $\vdash_{PC_\Omega} SA$. □

Далее будем опусть индекс PC_Ω у символа $\vdash$ там, где понятно, что речь идёт про выводимость в исчислении предикатов.

Лемма 11.3.
1) $\vdash \forall x[x/a]A \to A$ *(*x *не входит в* A*).*
2) $\vdash A \to \exists x[x/a]A$ *(*x *не входит в* A*).*
3) Допустимо правило $\dfrac{A \to B}{A \to \forall x[x/a]B}$ *(*x *не входит в* A, B*;* a *не входит в* A*).*
4) Допустимо правило $\dfrac{B \to A}{\exists x[x/a]B \to A}$ *(*x *не входит в* A, B*;* a *не входит в* A*).*

Правила (3), (4) называются ослабленными правилами Бернайса. В исходной (не ослабленной) форме x может входить в A; этот вариант разберём чуть позже.

Доказательство:
Докажем пункты (1) и (2). Это тривиальные случаи аксиом II.1 и II.2 для $t = a$.
3) Рассматриваем выводы из некоторого множества гипотез Γ. Пусть $\Gamma \vdash A \to B$. По правилу Gen тогда $\Gamma \vdash \forall x[x/a](A \to B)$. По аксиоме II.3 имеем: $\Gamma \vdash \forall x[x/a](A \to \to B) \to (A \to \forall x[x/a]B)$. Теперь $\Gamma \vdash A \to \forall x[x/a]B$ по MP.

Упражнение 11.1. По аналогии с доказательством пункта (3), используя аксиому II.4 вместо аксиомы II.3, доказать пункт (4).

□

Лемма 11.4. $\vdash Жy[y/a]A \to Жx[x/a]A$, *где* Ж – *квантор, а переменные* x, y *не входят в* A.

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Доказательство:

Рассмотрим случай Я $= \forall$.

$\vdash \forall y[y/a]A \to A$ по пункту (1) леммы (11.3). Тогда $\vdash \forall y[y/a]A \to \forall x[x/a]A$ по ослабленному правилу Бернайса.

Случай Я $= \exists$ разбирается аналогично. □

Лемма 11.5 (Ослабленная теорема дедукции)**.** *Если* $\Gamma, A \vdash B$ *без применения правила Gen, то* $\Gamma \vdash A \to B$.

Доказательство:

Доказательство такое же, как для теоремы дедукции для CL (4.2). □

Лемма 11.6. *В исчислении предикатов допустимо правило силлогизма*

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

Доказательство:

Из теоремы дедукции следует, что это правило – производное. См. лекцию 4. □

Лемма 11.7. *Допустимы правила Бернайса:*

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

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

где переменная x *не входит в* B*, переменная* a *не входит в* A.

Доказательство:

Докажем допустимость правила (1); правило (2) рассматривается аналогично.

Пусть $\Gamma \vdash A \to B$. Выберем переменную y, не входящую ни в A, ни в B. Тогда по пункту (3) леммы (11.3) имеем: $\Gamma \vdash A \to \forall y[y/a]B$. По лемме (11.4) имеем: $\vdash \forall y[y/a]B \to \forall x[x/a]B$. Отсюда по правилу силлогизма получаем: $\Gamma \vdash A \to \forall x[x/a]B$. □

Теорема 11.1 (Теорема дедукции)**.** *Если* A *– замкнутая формула, то*

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

Доказательство:

Докажем $\Leftarrow$. Это легко получается по MP (для любой A); см. доказательство теоремы дедукции для CL (4.2).

Докажем $\Rightarrow$ по индукции. Это делается аналогично доказательству теоремы дедукции для CL (4.2), но еще надо рассмотреть случай, когда B получается по правилу Gen.

Итак, пусть $B = \forall x[x/a]C$ и $\Gamma, A \vdash C$. По предположению индукции $\Gamma \vdash A \to C$. Тогда по правилу Бернайса (поскольку A замкнута) получаем $\Gamma \vdash A \to \forall x[x/a]C$, то есть $\Gamma \vdash A \to B$. □

Сформулируем следствие теоремы дедукции (11.1).

Утверждение 11.1. *Для любой конечной теории T и формулы A сигнатуры Ω*

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

где $\bigwedge T$ обозначает конъюнкцию всех формул из T.

Доказательство:

По теореме дедукции (11.1) имеем: $\bigwedge T \vdash A \;\Leftrightarrow \vdash (\bigwedge T) \to A$.

Заметим также, что $T \vdash A \;\Leftrightarrow\; \bigwedge T \vdash A$. Действительно, $T \vdash \bigwedge T$ по допустимому правилу введения $\wedge$ (см. лекцию 5); его надо применить несколько раз. Поэтому из $\bigwedge T \vdash A$ по транзитивности (пункт (3) леммы (11.1)) следует $T \vdash A$. Обратно, $\bigwedge T \vdash T$ по аксиомам I.3 ($T_1 \wedge T_2 \to T_1$), I.4 ($T_1 \wedge T_2 \to T_2$) и MP. Поэтому из $T \vdash A$ по транзитивности следует $\bigwedge T \vdash A$.

Таким образом, $T \vdash A \;\Leftrightarrow\; \bigwedge T \vdash A \;\Leftrightarrow \vdash (\bigwedge T) \to A$, то есть $T \vdash A \;\Leftrightarrow \vdash (\bigwedge T) \to$ $\to A$. □

Корректность исчисления предикатов

Теорема 11.2 (Теорема о корректности исчисления предикатов)**.**

1) Пусть T – теория 1-го порядка в сигнатуре Ω. Тогда для любой формулы A этой сигнатуры имеем:

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

2) Для любой формулы A сигнатуры Ω имеем:

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

то есть все теоремы исчисления предикатов общезначимы.

Доказательство:

Очевидно, что пункт (2) следует из пункта (1): надо взять $T = \varnothing$ и вспомнить, что по определению общезначимость A равносильна общезначимости $\overline{\forall} A$ (определение (9.5)).

Пункт (1) доказывается индукцией по длине вывода A в T аналогично теореме корректности (4.3) для исчисления высказываний.

1.1) Если $A \in T$, то доказывать нечего: A истинна во всех моделях T и $\overline{\forall} A = A$, так как A замкнута.

1.2) Все аксиомы группы I – подстановочные примеры аксиом CL. Например, предикатная формула $A \to (B \to A)$ – пример пропозициональной аксиомы $P_1 \to$ $\to (P_2 \to P_1)$ и так далее. Аксиомы CL – тавтологии (теорема корректности (4.3) для исчисления высказываний). Поэтому аксиомы группы I общезначимы по лемме (9.5) о тавтологиях.

1.3) Пусть A получается по MP из B и $B \to A$. Выводы этих формул короче, и по предположению индукции $T \vDash \overline{\forall} B$, $T \vDash \overline{\forall}(B \to A)$.

Рассмотрим любую модель M теории T и докажем, что $M \vDash \overline{\forall} A$. По лемме (8.1) для этого надо заменить свободные переменные из A (обозначим их список $\vec{a}$) на произвольные элементы из M (обозначим этот список $\vec{m}$) и доказать, что полученная оценённая формула (обозначим её A_1) истинна в M.

Заметим, что при замене $\vec{a}$ на $\vec{m}$ в формуле B могут остаться ещё какие-то свободные переменные; заменим их тоже на элементы из M (как угодно), и получим оценённую формулу B_1. Поскольку $T \vDash \overline{\forall} B$ и $M \vDash T$, имеем: $M \vDash \overline{\forall} B$. Тогда по лемме (8.1) имеем: $M \vDash B_1$.

Аналогично $M \vDash \overline{\forall}(B \to A)$, откуда $M \vDash B_1 \to A_1$ по лемме (8.1).

Теперь из истинности $B_1 \to A_1$ и B_1 следует истинность A_1 (по определению значения импликации; см. лекцию 7).

1.4) Пусть A получается по правилу Gen, то есть $A = \forall x[x/a]B$, $T \vdash B$. Вывод B короче, и по предположению индукции $T \vDash \overline{\forall} B$.

Случай 1. Если a входит в B, то $\overline{\forall} B$ и $\overline{\forall}\forall x[x/a]B$ могут отличаться только порядком кванторов. Из леммы (8.1) следует, что эти формулы равносильны. Поэтому $T \vDash \overline{\forall} A$.

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

В самом деле, пусть $B = B(\vec{b})$, a не входит в $\vec{b}$. Допустим, что $M \vDash \overline{\forall} B$. Тогда для всех наборов $\vec{m}$ элементов из M (той же длины, что $\vec{b}$) $M \vDash B(\vec{m})$. В формуле $A = \forall x[x/a]B(\vec{b})$ остаются все те же свободные переменные $\vec{b}$. Поэтому $M \vDash \overline{\forall}\forall x[x/a]B(\vec{b})$ означает, что для всех $\vec{m}$ из M имеем: $M \vDash \forall x[x/a]B(\vec{m})$. Но это – то же, что $M \vDash B(\vec{m})$, так как переменная a в $B(\vec{m})$ не входит, любая её замена оказывается фиктивной. Итак, $M \vDash \overline{\forall} A$.

1.5) A – аксиома II.3: $A = \forall x[x/a](C \to B) \to (C \to \forall x[x/a]B)$, где x не входит в A и B, a не входит в C. Докажем общезначимость этой формулы. Выберем модель M и возьмём произвольную замену свободных переменных на элементы из M. Получим оценённую формулу $A_1 = \forall x[x/a](C_1 \to B_1) \to (C_1 \to \forall x[x/a]B_1)$.

Так как a не входит в C, здесь C_1 – замкнутая (то есть тоже оценённая) формула, а B_1 может содержать только одну свободную переменную a (поскольку формула $\forall x[x/a]B_1$ замкнута). Запишем B_1 как $B_1(a)$ и соответственно $A_1 = \forall x(C_1 \to \to B_1(x)) \to (C_1 \to \forall x B_1(x))$.

Докажем, что $M \vDash A_1$. Предположим, что $M \vDash \forall x(C_1 \to B_1(x))$, и проверим, что $M \vDash C_1 \to \forall x B_1(x)$. В свою очередь, для этого предположим, что $M \vDash C_1$, и докажем, что $M \vDash \forall x B_1(x)$.

Возьмём любое $m \in M$. Из $M \vDash \forall x(C_1 \to B_1(x))$ следует, что $M \vDash C_1 \to B_1(m)$. Тогда из $M \vDash C_1$ следует, что $M \vDash B_1(m)$. Поскольку m произвольно, получаем $M \vDash \forall x B_1(x)$, что и требовалось.

1.6) A – аксиома II.4. Этот случай аналогичен предыдущему.

Упражнение 11.2. Доказать пункт (1.6).

Оставшиеся аксиомы II.1, II.2 будут рассмотрены на следующей лекции. □

Лекция 12

Корректность исчисления предикатов (продолжение)

Продолжаем доказательство теоремы (11.2) о корректности исчисления предикатов.

Доказательство:

Осталось проверить общезначимость аксиом II.1 и II.2. Рассмотрим аксиому II.1 (общезначимость аксиомы II.2 проверяется аналогично).

Упражнение 12.1. Проверить общезначимость аксиомы II.2.

Рассуждаем как в случае II.3 (лекция 11). Нам надо доказать общезначимость формулы $A(a,\vec{b}) \coloneqq \forall x[x/a]B \to [t/a]B$, где $\vec{b}$ – список дополнительных параметров, кроме a (переменная a в формулу A может попасть из терма t; если она не входит в t (и в A), рассуждение не меняется). Тогда запишем B как $B(a,\vec{b})$, t – как $t(a,\vec{b})$.

Рассмотрим модель M и заменим набор параметров $a,\vec{b}$ на набор произвольных элементов $q,\vec{m}$ из M. Получим оценённую формулу $A(q,\vec{m}) = \forall x[x/a]B(a,\vec{m}) \to \to [t(q,\vec{m})/a]B(a,\vec{m})$. Обозначим $B_1(a) \coloneqq B(a,\vec{m})$, $t_1 \coloneqq t(q,\vec{m})$ и перепишем формулу $A(q,\vec{m})$, получим: $A(q,\vec{m}) = \forall x[x/a]B_1(a) \to B_1(t_1)$. Здесь $B_1(t_1)$ обозначает $[t_1/a]B_1(a)$.

Нам надо доказать, что $M \vDash A(q,\vec{m})$. Для этого предположим, что $M \vDash \forall x[x/a]B_1(a)$, и докажем, что $M \vDash B_1(t_1)$.

Для это достаточно будет доказать следующую лемму.

Лемма 12.1. *Пусть $B_1(a) \in Fm_{\Omega\cup M}$, $r(a) \in Tm_{\Omega\cup M}$, $t_1 \in CTm_{\Omega\cup M}$. Тогда:*

1) $|r(t_1)|_M = |r(|t_1|_M)|_M$;

2) $|B_1(t_1)|_M = |B_1(|t_1|_M)|_M$.

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

Из пункта (2) леммы (12.1) получаем $M \vDash B_1(t_1)$ (в предположении $M \vDash \forall x[x/a]B_1(a)$), поскольку из $M \vDash \forall x[x/a]B_1(a)$ следует $M \vDash B_1(|t_1|_M)$.

Докажем лемму (12.1).

Доказательство:

Индекс M при $|\ldots|$ не пишем. С некоторыми изменениями повторяется доказательство теоремы (7.1).

Докажем пункт (1) индукцией по длине r.

1.1) (Базис индукции). $r = c$ для $c \in Const_\Omega$. Тогда a не входит в r, и доказывать нечего.

1.2) (Базис индукции). $r = m$ для $m \in M$. Опять a не входит в r, и всё очевидно.

1.3) (Базис индукции). $r = a$. Тогда $r(t_1) = t_1$, $r(|t_1|) = |t_1|$, а также $|t_1| = ||t_1||$ по определению значения оценённого терма (определение (7.5)): $|m| = m$ для всех $m \in M$.

1.4) (Шаг индукции). $r(a) = f(r_1(a),\ldots,r_n(a))$. Тогда

$$r(t_1) = f(r_1(t_1),\ldots,r_n(t_n)) \text{ и } r(|t_1|) = f(r_1(|t_1|),\ldots,r_n(|t_n|)).$$

Тогда

$$|r(t_1)| = f_M(|r_1(t_1)|, \ldots, |r_n(t_1)|) \text{ и } |r(|t_1|)| = f_M(|r_1(|t_1|)|, \ldots, |r_n(|t_n|)|).$$

Но по предположению индукции для термов r_i имеем: $|r_i(t_1)| = |r_i(|t_1|)|$. Тогда $|r(t_1)| = |r(|t_1|)|$.

Докажем пункт (2) индукцией по числу связок и кванторов в $B_1(a)$.

2.1) (Базис индукции). $B_1(a) = P(r_1(a), \ldots, r_n(a))$ – атомарная. Доказательство аналогично пункту (1.4).

Упражнение 12.2. Доказать пункт (2.1).

2.2) (Шаг индукции). B_1 получается применением $\wedge$, $\vee$, $\to$ или $\neg$. Эти случаи почти очевидны.

Упражнение 12.3. Доказать пункт (2.2).

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

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

и

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

По предположению индукции, применённому к формуле $C(a, l)$, имеем: $|C(t_1, l)| = |C(|t_1|, l)|$ для каждого $l \in M$. Тогда $|B_1(t_1)| = |B_1(|t_1|)|$.

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

Доказательство аналогично пункту (2.3): $\exists$ заменяется на $\forall$, а max – на min. □

□

Исчисление предикатов с равенством

Определение 12.1. Пусть Ω – сигнатура, содержащая предикатный символ равенства $=$. *Исчисление предикатов с равенством* в сигнатуре Ω получается из обычного исчисления предикатов PC_Ω добавлением аксиом стандартной теории равенства Eq_Ω (см. лекцию 8): $PC^{=}_{\Omega} = PC_\Omega + Eq_\Omega$.

Выводимость из теории T в исчислении предикатов с равенством: $T \vdash_{PC^{=}_{\Omega}} A \Leftrightarrow T \cup Eq_\Omega \vdash_{PC_\Omega} A$.

Для теорий в такой сигнатуре можно рассматривать нормальные модели и логическое следование на них.

Определение 12.2. $T \vDash_{\text{норм}} A$ означает, что (замкнутая) формула A *истинна во всех нормальных моделях теории* T.

Также можно определить нормальную общезначимость.

Определение 12.3. Формула A *нормально общезначима* (обозначение $\vDash_{\text{норм}} A$), если её универсальное замыкание $\overline{\forall} A$ истинно во всех нормальных моделях данной сигнатуры.

Теорема 12.1 (Теорема о корректности исчисления предикатов с равенством)**.**
1) Пусть T – теория 1-го порядка с равенством в сигнатуре Ω. Тогда для любой замкнутой формулы A этой сигнатуры имеем:

$$T \vdash_{PC^{=}_{\Omega}} A \;\Rightarrow\; T \vDash_{норм} A.$$

2) Для любой формулы A сигнатуры Ω имеем:

$$\vdash_{PC^{=}_{\Omega}} A \;\Rightarrow \vDash_{норм} A,$$

то есть все теоремы исчисления предикатов с равенством нормально общезначимы.

Доказательство:
1) Пусть $T \vdash_{PC^{=}_{\Omega}} A$. По определению это означает $T \cup Eq_{\Omega} \vdash_{PC_{\Omega}} A$. По теореме корректности (11.2) имеем: $T \cup Eq_{\Omega} \vDash A$. Если $M \vDash T$ и M нормальна, то $M \vDash Eq_{\Omega}$ (лемма (8.2)). Тогда $M \vDash A$.
2) Как и в теореме (11.2), рассмотрим $T = \varnothing$ и применим пункт (1) для $\overline{\forall} A$. □

Непротиворечивость

Определение 12.4. Теория T в сигнатуре Ω называется *противоречивой*, если для некоторой формулы A в этой сигнатуре $T \vdash_{PC_{\Omega}} A$ и $T \vdash_{PC_{\Omega}} \neg A$.

Определение 12.5. Теория T в сигнатуре Ω с равенством называется *противоречивой*, если для некоторой формулы A в этой сигнатуре $T \vdash_{PC^{=}_{\Omega}} A$ и $T \vdash_{PC^{=}_{\Omega}} \neg A$.

Лемма 12.2. *Если теория T в сигнатуре Ω противоречива, то $T \vdash_{PC_{\Omega}} B$ для любой формулы сигнатуры B; аналогично для теорий с равенством.*

Доказательство:
См. доказательство пункта (2) леммы (5.2). □

Сформулируем следствие.

Утверждение 12.1.
1) Если теория 1-го порядка выполнима, то она непротиворечива.
2) Если теория 1-го порядка с равенством нормально выполнима (то есть имеет нормальную модель), то она непротиворечива.

Доказательство:
1) Предположим, что теория T в сигнатуре Ω противоречива. Предположим, что $M \vDash T$. Возьмём какую-нибудь замкнутую формулу B, истинную в M (например, формулу вида $A \to A$). По лемме (12.2) имеем: $T \vdash_{PC_{\Omega}} \neg B$. Тогда по теореме (11.2) о корректности исчисления предикатов имеем: $T \vDash \neg B$. Следовательно, $M \vDash \neg B$, что противоречит выбору B.
2) Аналогично с использованием $PC^{=}_{\Omega}$. □

Пример: арифметика Пеано

Определение 12.6. *Арифметика Пеано* (PA) – это теория 1-го порядка в сигнатуре $\{0, 1, +, \cdot, =\}$ со следующими аксиомами:

1) $\forall x(x + 1 \neq 0)$;
2) $\forall x \forall y(x + 1 = y + 1 \to x = y)$;
3) $\forall x(x \neq 0 \to \exists y(y + 1 = x))$;
4) $\forall x(x + 0 = x)$;
5) $\forall x \forall y(x + (y + 1) = (x + y) + 1)$;
6) $\forall x(x \cdot 0 = 0)$;
7) $\forall x \forall y(x \cdot (y + 1) = x \cdot y + x)$;
8) $\overline{\forall}(A(0) \wedge \forall x(A(x) \to A(x + 1)) \to \forall x A(x))$.

Здесь (1)-(7) – конкретные формулы, а (8) – схема, то есть бесконечное множество аксиом определённого вида. Предполагается, что A – формула с несколькими свободными переменными, то есть $A = A(a, \ldots)$. Записи $A(0)$, $A(x)$ обозначают соответственно $[0/a]A$, $[x/a]A$; запись $\forall x(A(x) \to A(x+1))$ – это формула $\forall x[x/a](A \to$ $\to [a + 1/a]A)$.

(8) называется *схемой аксиом индукции*. Она выражает принцип математической индукции: если какое-то свойство A верно для 0 и из истинности A для x следует истинность для $x + 1$, то A верно для всех x. Однако в теории PA индукция постулируется только для тех свойств, которые можно записать формулами в данной сигнатуре.

Хотя теория PA и называется «арифметика Пеано», она отличается от той, которую рассматривал сам Пеано: в его теории индукция применима ко всем свойствам натуральных чисел. Теория Пеано (в современном понимании) соответствует арифметике 2-го порядка, которая в нашем курсе не изучается.

Теорема 12.2. *PA непротиворечива.*

Доказательство:

PA имеет стандартную модель $\mathbb{N}$: множество натуральных чисел (включая 0), где $+$ интерпретируется как операция сложения, $\cdot$ – как операция умножения, константа 0 – как число нуль, константа 1 – как число единица. Все аксиомы PA верны в этой модели. По утверждению (12.1) получаем, что PA непротиворечива. □

Это – метаматематическое рассуждение; в нём предполагается известным, что такое натуральные числа и какие у них свойства. Чтобы дать строгое математическое доказательство, нужна формальная теория, где мы можем определить множество натуральных чисел. Это делается в аксиоматической теории множеств, о чём будет сказано кратко в лекции 14.

Модальное исчисление $S5$

Некоторые части логики предикатов можно превратить в логики высказываний – так называемые *модальные логики*. В модальных логиках к обычным булевым

связкам добавляются модальные связки, в простейшем случае – одноместная связка «необходимо» ($\Box$).

В отличие от булевых связок, логические свойства связки $\Box$ не очевидны и допускают много вариаций. Первые модальные исчисления были построены К. Льюисом (1918) и названы им $S1, \ldots, S5$. А вообще, имеется огромное число (континуум) различных модальных логик.

В этом курсе мы рассмотрим только исчисление $S5$. Современная формулировка его была дана Гёделем (1933).

Определение 12.7. *Множество модальных формул* MFm строится по следующим правилам:

- если $A \in Var$, то $A \in MFm$;
- если $A, B \in MFm$, то $(A \wedge B) \in MFm$;
- если $A, B \in MFm$, то $(A \vee B) \in MFm$;
- если $A, B \in MFm$, то $(A \to B) \in MFm$;
- если $A \in MFm$, то $\neg A \in MFm$;
- если $A \in MFm$, то $\Box A \in MFm$.

Таким образом, $Fm \subset MFm$.

Также будем использовать связку «возможно» ($\Diamond$), которая определяется как сокращение: $\Diamond := \neg\Box\neg$.

Определение 12.8. *Схемы аксиом S5:*
I) Схемы (1)–(10) из CL, но для модальных формул.
II)
(AK) $\Box(A \to B) \to (\Box A \to \Box B)$,
(AT) $\Box A \to A$,
$(A4)$ $\Box A \to \Box\Box A$,
$(A5)$ $\Diamond\Box A \to \Box A$.

Определение 12.9. *Правила вывода S5:*
$ModusPonens$ (MP);
Правило добавления $\Box$ (Nec): $\dfrac{A}{\Box A}$.

Понятия вывода и выводимости в $S5$ определяются аналогично CL (с учётом дополнительного правила).

Семантика Крипке для $S5$

Определение 12.10. Пусть $W \neq \varnothing$ – множество. *Оценка* (пропозициональных переменных) на W – это отображение $Var \to \mathcal{P}(W)$, где $\mathcal{P}(W)$ – множество всех подмножеств множества W. *Модель Крипке* на W – это пара (W, θ), где θ – оценка на W. W называется *множеством (возможных) миров* этой модели.

Определение 12.11. Для модели Крипке $M = (W, \theta)$, мира $u \in W$ и модальной формулы A определяем *значение* A в u; оно обозначается $|A|_u^M$. Определение даётся индукцией по длине A сразу для всех миров u:

- $|P_i|_u^M := \begin{cases} 1, \text{ если } u \in \theta(P_i) \\ 0, \text{ иначе} \end{cases}$;
- $|A \wedge B|_u^M := \min(|A|_u^M, |B|_u^M)$;
- $|A \vee B|_u^M := \max(|A|_u^M, |B|_u^M)$;
- $|\neg A|_u^M := 1 - |A|_u^M$;
- $|A \to B|_u^M := \max(1 - |A|_u^M, |B|_u^M)$;
- $|\Box A|_u^M := \min\limits_{v \in W} |A|_v^M$.

Вместо $|A|_u^M = 1$ пишут также $M, u \vDash A$ и говорят, что формула A истинна в модели M в мире u.

В этих обозначениях определение (12.11) записывается так:

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

Из определения $\Diamond$ и $|\Box A|_u^M$ получаем: $M, u \vDash \Diamond A \;\Leftrightarrow\; \exists v \in W \;\; M, v \vDash A$. В других обозначениях: $|\Diamond A|_u^M = \max\limits_{v \in W} |A|_v^M$.

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

Определение 12.12. Модальная формула A *общезначима* на (непустом) множестве W (обозначение: $W \vDash A$), если она истинна во всех мирах в любой модели Крипке на W, то есть $\forall \theta \; \forall u \;\; |A|_u^{(W,\theta)} = 1$.

Теорема 12.3 (Теорема корректности для $S5$)**.** *Если* $\vdash_{S5} A$*, то* $W \vDash A$ *для любого* $W \neq \varnothing$.

Это утверждение можно доказать индукцией по длине вывода A. У нас оно получится как следствие другой теоремы на следующей лекции.

Стандартный перевод модальных формул

Определение 12.13. Рассмотрим сигнатуру со счётным множеством одноместных предикатных символов: $P_1^1,\ P_2^1,\ \ldots$. *Стандартный перевод* (или перевод Вайсберга) $A \mapsto A^*$ модальных формул A в формулы 1-го порядка A^* в этой сигнатуре определяется по индукции:

- $P_i^* := P_i^1(a)$;
- $(A \circ B)^* := (A^* \circ B^*)$ для $\circ = \vee, \wedge, \to$;
- $(\neg A)^* := \neg A^*$;
- $(\Box A)^* := \forall x[x/a]A^*$, где x – первая связанная переменная (в общем списке $BVar$ – см. лекцию 6), не входящая в A (можно взять и любую другую переменную, не попавшую в A, но мы выбираем первую для единообразия).

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

Определение 12.14. Каждой модели Крипке $M = (W, \theta)$ поставим в соответствие модель M^* сигнатуры $\{P_1^1, P_2^1, \ldots\}$ с носителем W. А именно, полагаем для каждого $u \in W$ следующее:

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

Это можно записать и так:

$$|P_i^1(u)|_{M^*} := |P_i|_u^M.$$

Лемма 12.3. *Для любой модальной формулы A имеем: $|A^*(u)|_{M^*} = |A|_u^M$.*

Доказательство:

Индукцией по длине A доказываем утверждение для всех u.

Если A – переменная, утверждение следует из определений (12.13), (12.14).

Если A имеет вид отрицания, конъюнкции, дизъюнкции или импликации, утверждение легко следует из определений истинности для модальных формул и формул 1-го порядка.

Упражнение 12.4. Доказать утверждение для случая, когда A имеет вид отрицания, конъюнкции, дизъюнкции или импликации.

Пусть $A = \Box B$. Тогда по определениям (7.6) и (12.11) имеем:

$$|A^*(u)|_{M^*} = |(\forall x[x/a]B^*)(u)|_{M^*} = \min_{v \in W} |B^*(v)|_{M^*}; \qquad |A|_u^M = \min_{v \in W} |B|_v^M.$$

По предположению индукции, $|B^*(v)|_{M^*} = |B|_v^M$. Поэтому утверждение верно для A. $\Box$

Лемма 12.4. *Для любой модальной формулы A и непустого W имеем:*

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

Доказательство:

Докажем $\Rightarrow$ от противного. Пусть $W \not\models A$, тогда для некоторой модели Крипке M на W и какого-то мира $u \in W$ имеем: $M, u \not\models A$. Отсюда по лемме (12.3) имеем: $M^* \not\models A^*(u)$, следовательно, $M^* \not\models \forall x[x/a]A^*$, значит, $W \not\models \forall x[x/a]A^*$.

Докажем $\Leftarrow$ тоже от противного. Пусть $W \not\models \forall x[x/a]A^*$. Тогда найдётся модель μ нашей сигнатуры (с одноместными предикатами) с носителем W такая, что $\mu \not\models \forall x[x/a]A^*$, то есть для некоторого $u \in W$ имеем: $\mu \not\models A^*(u)$.

Но $\mu = M^*$ для некоторой модели Крипке M на W: она однозначно задаётся равенствами $|P_i|_v^M = |P_i^1(v)|_\mu$ для всех v, i. Поэтому из $\mu \not\models A^*(u)$ по лемме (12.3) получаем, что $M, u \not\models A$. Таким образом, $W \not\models A$. $\square$

Лекция 13

Свойства исчисления $S5$

Теорема 13.1. *Следующие утверждения эквивалентны:*
1) $\vdash_{S5} A$*;*
2) $\vdash_{PC} A^*$*;*
3) $\vDash A^*$*;*
4) $W \vDash A^*$ *для всех конечных* W*;*
5) $W \vDash A$ *для всех* W*;*
6) $W \vDash A$ *для всех конечных* W*.*
Здесь PC понимается как исчисление предикатов в сигнатуре с одноместными предикатами P_i^1 *и без равенства.*

Доказательство:
Доказывать будем следующие импликации:

- (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (6);
- (3) $\Rightarrow$ (5) $\Rightarrow$ (6);
- (6) $\Rightarrow$ (1).

(2) $\Rightarrow$ (3) следует из теоремы (11.2) о корректности для PC.
(3) $\Rightarrow$ (4), (5) $\Rightarrow$ (6) очевидны.
(4) $\Rightarrow$ (6), (3) $\Rightarrow$ (5) получается из леммы (12.4).
Осталось доказать (1) $\Rightarrow$ (2) и (6) $\Rightarrow$ (1).
Отметим, что (3) $\Rightarrow$ (2) – это теорема Гёделя о полноте исчисления предикатов.
Докажем (1) $\Rightarrow$ (2) индукцией по длине вывода A в $S5$.

- Если A – аксиома группы (I), то A^* – аксиома PC того же вида (из группы I). Например, если $A = B \to (C \to B)$, то $A^* = B^* \to (C^* \to B^*)$ и так далее.
- Пусть $A = (\Box(B \to C) \to (\Box B \to \Box C))$. Тогда

$$A^* = (\forall x(B^*(x) \to C^*(x)) \to (\forall x B^*(x) \to \forall x C^*(x))).$$

Тогда $\vdash_{PC} A^*$ получим по теореме дедукции (она применима, так как все гипотезы – замкнутые) из следующей выводимости:

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

А это доказывается непосредственно:

1. $\forall x(B^*(x) \to C^*(x))$ – гипотеза.
2. $\forall x(B^*(x) \to C^*(x)) \to (B^*(a) \to C^*(a))$ – аксиома II.1 из PC.
3. $B^*(a) \to C^*(a)$ – 1, 2, MP.
4. $\forall x B^*(x)$ – гипотеза.

5. $\forall x B^*(x) \to B^*(a)$ – аксиома II.1 из PC.

6. $B^*(a)$ – 4, 5, MP.

7. $C^*(a)$ – 3, 6, MP.

8. $\forall x C^*(x)$ – 7, Gen.

- Пусть $A = (\Box B \to B)$. Тогда $A^* = \forall x B^*(x) \to B^*(a)$ – аксиома.
- Пусть $A = (\Box B \to \Box\Box B)$. Тогда $A^* = (\forall x B^*(x) \to \forall y \forall x B^*(x))$ получается из $\forall x B^*(x) \to \forall x B^*(x)$ с помощью первого правила Бернайса из леммы (11.7).
- Пусть $A = (\Diamond\Box B \to \Box B)$. Тогда $A^* = (\exists y \forall x B^*(x) \to \forall x B^*(x))$ получается из $\forall x B^*(x) \to \forall x B^*(x)$ с помощью второго правила Бернайса из леммы (11.7).

  Можно провести доказательство непосредственно из определения $\Diamond$. Тогда $A^* = (\neg\forall y \neg\forall x B^*(x) \to \forall x B^*(x))$.

  Запишем: $\neg\forall x B^*(x) \to \neg\forall x B^*(x)$. Тогда $\neg\forall x B^*(x) \to \forall y \neg\forall x B^*(x)$ по первому правилу Бернайса из леммы (11.7). Применяем допустимое правило, позволяющее менять порядок посылки и заключения, при этом дописывая отрицание. Получим: $\neg\forall y \neg\forall x B^*(x) \to \neg\neg\forall x B^*(x)$. Используя аксиому $\neg\neg\forall x B^*(x) \to$ $\to \forall x B^*(x)$, по правилу силлогизма (11.6) получаем: $\neg\forall y \neg\forall x B^*(x) \to \forall x B^*(x)$, то есть $\vdash_{PC} A^*$.
- Пусть A получается по MP из B, $B \to A$. По предположению индукции $\vdash_{PC} B^*$, $B^* \to A^*$. Тогда $\vdash_{PC} A^*$ по MP.
- Пусть $A = \Box B$ получается по Nec из B. Тогда $A^* = \forall x B^*(x)$. По предположению индукции $\vdash_{PC} B^*(a)$. Отсюда $\vdash_{PC} A^*$ по Gen.

Докажем (6) $\Rightarrow$ (1). Это – теорема о полноте $S5$ относительно конечных моделей Крипке. Её доказательство занимает всю оставшуюся часть лекции.

Определение 13.1. Модальные формулы A, B *доказуемо эквивалентны* в $S5$, если $\vdash_{S5} A \leftrightarrow B$. Обозначение: $A \equiv_{S5} B$.

Далее мы будем опускать индекс $S5$.

Лемма 13.1 (Некоторые синтаксические свойства $S5$)**.**

1) Допустимы правила монотонности: $\dfrac{A \to B}{\Box A \to \Box B}$, $\dfrac{A \to B}{\Diamond A \to \Diamond B}$.

2) $\equiv$ задаёт отношение эквивалентности на MFm.

3) $\equiv$ согласовано со всеми связками:
если $A \equiv A'$, то $\Box A \equiv \Box A'$, $\neg A \equiv \neg A'$;
если $A \equiv A'$ и $B \equiv B'$, то $(A \circ B) \equiv (A' \circ B')$, где $\circ$ – это $\vee$, $\wedge$ или $\to$.

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

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

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

7) $\Diamond(A \wedge \Box B) \equiv \Diamond A \wedge \Box B$.

Доказательство (не слишком трудное) пропускаем.

Определение 13.2. Модальные формулы *глубины 1* определяются по индукции:

- P_i – глубины 1;
- если A – глубины 1, то $\neg A$ – глубины 1;
- если A, B – глубины 1, то $A \circ B$ – глубины 1, где $\circ$ – $\vee$, $\wedge$ или $\to$.
- если $A \in Fm$ (классическая формула), то $\Box A$ – глубины 1.

Лемма 13.2 (О нормальной форме для формул глубины 1)**.** *Если A – глубины 1, то $A \equiv \bigvee\limits_i A_i$, где A_i – вида $\bigwedge\limits_j Q_{ij}$, а каждое Q_{ij} – либо литерал, либо формула вида $\Diamond D$ или $\neg\Diamond D$, где D – классическая.*

Доказательство:

Заметим, что $\Box A \equiv \neg\Diamond\neg A$. Тогда из определения (13.2) следует, что формула A имеет вид $B(P_1, \dots, P_n, \Diamond C_1, \dots, \Diamond C_m)$, где $B(P_1, \dots, P_n, P_{n+1}, \dots, P_{n+m})$ и $C_1, \dots, C_m$ – классические формулы. (Это легко доказывается по индукции.)

Формулу B можно привести к СДНФ: $B \sim \bigvee\limits_i B_i$, где B_i – элементарные конъюнкции. Тогда по теореме (5.1) о полноте CL имеем: $\vdash_{CL} B \leftrightarrow \bigvee\limits_i B_i$. Тогда, подставив формулы $\Diamond C_1, \dots, \Diamond C_m$ вместо $P_{n+1}, \dots, P_{n+m}$ в этот вывод, получим: $\vdash_{S5} A \leftrightarrow \bigvee\limits_i A_i$, где $A_i = B_i(P_1, \dots, P_n, \Diamond C_1, \dots, \Diamond C_m)$. Поскольку B_i – элементарная конъюнкция, A_i окажется конъюнкцией формул $P_1, \dots, P_n, \Diamond C_1, \dots, \Diamond C_m$ или их отрицаний, что и требовалось. □

Лемма 13.3. *Существует лишь конечное число попарно не эквивалентных формул глубины 1 от переменных $P_1, \dots, P_n$.*

Доказательство:

Достаточно рассмотреть нормальные формы из леммы (13.2) о нормальной форме для формул глубины 1.

С точностью до $\equiv$ имеется конечное число конъюнкций A_i. Действительно, каждая из них содержит литералы от $P_1, \dots, P_n$ и формулы вида $\Diamond D, \neg D$, где D – классическая формула от $P_1, \dots, P_n$. Такие формулы D приводятся к СДНФ в CL, и тем более, в $S5$. И если $D \equiv D'$, то $\Diamond D \equiv \Diamond D'$, $\neg\Diamond D \equiv \neg\Diamond D'$ – по лемме (13.1).

Из конечного числа A_i можно построить лишь конечное число их дизъюнкций с точностью до $\equiv$ (здесь снова пользуемся леммой (13.1)). □

Лемма 13.4. *В $S5$ всякая формула эквивалентна формуле глубины 1 (от тех же переменных).*

Доказательство:

Запишем эквивалентную формулу, используя связку $\Diamond$ вместо $\Box$ (это можно сделать, так как $\Box A \equiv \neg\Diamond\neg A$). Далее рассуждаем индукцией по длине формулы.

Нетривиален только шаг индукции для формулы вида $\Diamond A$. По предположению индукции A эквивалентна формуле глубины 1, и значит, нормальной форме из леммы (13.2) о нормальной форме для формул глубины 1. Тогда $\Diamond A \equiv \bigvee\limits_i \Diamond A_i$ (пункты (3) и (5) леммы (13.1)).

Рассмотрим $\Diamond A_i = \Diamond \bigwedge\limits_j Q_{ij}$. Используя пункты (6) и (7) леммы (13.1) (и эквивалентность $\neg\Diamond D \equiv \Box\neg D$), преобразуем эту формулу в конъюнкцию формул вида $\Diamond P_k$, $\Diamond D$, $\Box D$ (где D – классическая), то есть в формулу глубины 1. □

Запишем следствие из лемм (13.3), (13.4).

Утверждение 13.1 (О локальной табличности $S5$)**.** *Существует конечное число формул от переменных $P_1, \ldots, P_n$, попарно не эквивалентных в $S5$.*

Определение 13.3. Для множества модальных формул Γ *выводимость* формулы A (обозначение: $\Gamma \vdash_{S5} A$) означает, что существует вывод A с использованием формул из Γ, аксиом $S5$ и правила MP (но не Gen).

Определение 13.4. Γ *противоречиво в $S5$*, если $\Gamma \vdash_{S5} A, \neg A$ для некоторой формулы A.

Легко видеть, что для этой выводимости сохраняются лемма (5.2) и теорема дедукции (4.2).

Пусть Φ – множество всех модальных формул от $P_1, \ldots, P_n$. Рассматриваем непротиворечивые (в $S5$) подмножества Φ.

Определение 13.5. Множество $\Gamma \subseteq \Phi$ называется *максимальным*, если оно непротиворечиво, а всякое его собственное расширение внутри Φ противоречиво.

Лемма 13.5. *Всякое непротиворечивое множество содержится в максимальном.*

Доказательство:

Если Γ непротиворечиво, но не максимально, то найдётся A такая, что $\Gamma \cup \{A\}$ непротиворечиво. Тогда и $\Gamma \cup \{A' \in \Phi \mid A' \equiv A\}$ непротиворечиво. Действительно, если противоречие выводится из $\Gamma, A, A'_1, \ldots, A'_k$ и все A'_i эквивалентны A, то оно выводится уже из $\Gamma \cup \{A\}$ – поскольку $\vdash_{S5} A \to A'_i$, а тогда $\Gamma \cup \{A\} \vdash A'_i$ (по MP).

Если же мы будем расширять Γ, добавляя вместе с каждой формулой все эквивалентные ей, то за конечное число шагов мы получим все Φ – это следует из локальной табличности $S5$. Значит, за (меньшее) конечное число таких шагов мы можем получить максимальное множество. □

Замечание 13.1. Существует лишь конечное число максимальных множеств, потому что в максимальном множестве вместе с каждой формулой находятся все формулы, которые ей эквивалентны.

Лемма 13.6 (Свойства максимальных множеств)**.**

Для максимального Γ сохраняются свойства из леммы (5.4):

0) $\Gamma \vdash B \;\Rightarrow\; B \in \Gamma$ *для* $B \in \Phi$*;*

1) $\neg B \in \Gamma \;\Leftrightarrow\; B \notin \Gamma$*;*

2) $(B \wedge C) \in \Gamma \;\Leftrightarrow\; (B \in \Gamma$ *и* $C \in \Gamma)$*;*

3) $(B \vee C) \in \Gamma \;\Leftrightarrow\; (B \in \Gamma$ *или* $C \in \Gamma)$*;*
4) $(B \to C) \in \Gamma \;\Leftrightarrow\; (B \notin \Gamma$ *или* $C \in \Gamma)$.

Теперь продолжаем доказательство импликации (6) $\Rightarrow$ (1) из теоремы (13.1): для данной формулы A, не выводимой в $S5$, построим опровергающую конечную модель Крипке.

Так как $\nvdash_{S5} A$, множество $\{\neg A\}$ непротиворечиво. По лемме (13.5) построим максимальное множество Γ_0, содержащее $\neg A$.

Определение 13.6. Определим *отношение достижимости на максимальных множествах*:

$$\Gamma R \Delta \;\Leftrightarrow\; \text{для любой формулы } B \text{ имеем: } \Box B \in \Gamma \;\Rightarrow\; B \in \Delta.$$

Лемма 13.7. R *– отношение эквивалентности.*

Доказательство:

- Рефлексивность.

  Пусть $\Box B \in \Gamma$. Так как $\Box B \to B$ – аксиома $S5$, она лежит в Γ (пункт (0) леммы (13.6)). Тогда $\Gamma \vdash B$ по MP, а потому $B \in \Gamma$ (опять по пункту (0) леммы (13.6)). По определению R имеем $\Gamma R \Gamma$.

- Транзитивность.

  Предположим $\Gamma R \Delta R \Sigma$ и докажем $\Gamma R \Sigma$.

  Пусть $\Box B \in \Gamma$. Так как $\Box B \to \Box\Box B$ – аксиома $S5$, она лежит в Γ. Тогда $\Gamma \vdash \Box\Box B$ по MP, а потому $\Box\Box B \in \Gamma$. Теперь из $\Gamma R \Delta$ получаем, что $\Box B \in \Delta$. И из $\Delta R \Sigma$ получаем, что $B \in \Sigma$.

- Симметричность.

  Предположим $\Gamma R \Delta$ и докажем $\Delta R \Gamma$.

  Пусть $\Box B \in \Delta$. Тогда $\Diamond \Box B = \neg \Box \neg \Box B \in \Gamma$. В самом деле, иначе $\Box \neg \Box B \in \Gamma$ (пункт (1) леммы (13.6)). А тогда $\neg \Box B \in \Delta$ (так как $\Gamma R \Delta$), что даёт противоречие в Δ.

  Таким образом, $\Diamond \Box B \in \Gamma$. Кроме того, $(\Diamond \Box B \to B) \in \Gamma$ – это аксиома $S5$. Отсюда по MP и пункту (0) леммы (13.6) получаем $B \in \Gamma$, что и требовалось.

□

Продолжаем. Пусть $W := \{\Gamma \mid \Gamma_0 R \Gamma\}$. Из утверждения (13.1) о локальной табличности $S5$ и из леммы (13.6) о свойствах максимальных множеств следует, что W конечно. Зададим оценку на W следующим образом: $\theta(P_i) := \{\Gamma \mid P_i \in \Gamma\}$. Рассмотрим модель Крипке $M := (W, \theta)$ (она называется канонической моделью).

Лемма 13.8 (Основная лемма)**.**
Для всех $B(P_1, \ldots, P_n) \in \Phi$ *и* $\Gamma \in W$ *имеем:* $M, \Gamma \vDash B \;\Leftrightarrow\; B \in \Gamma$.

Доказательство:
Индукция по длине B.

- B – переменная. Тогда утверждение верно по определению θ.
- $B = (C \vee D)$. Тогда по определению (12.11), предположению индукции и пункту (3) леммы (13.6) имеем:

  $M, \Gamma \vDash B \Leftrightarrow (M, \Gamma \vDash C$ или $M, \Gamma \vDash D) \Leftrightarrow (C \in \Gamma$ или $D \in \Gamma) \Leftrightarrow (C \vee D) \in \Gamma$,

  что и требовалось.
- Случаи связок $\wedge$, $\to$, $\neg$ разбираются аналогично.

  Упражнение 13.1. Выполнить доказательство для случаев связок $\wedge$, $\to$, $\neg$.
- $B = \Box C$. Проверим эквивалентность $M, \Gamma \vDash \Box C \Leftrightarrow \Box C \in \Gamma$.

  Докажем $\Leftarrow$. Пусть $\Box C \in \Gamma$. Чтобы доказать $M, \Gamma \vDash \Box C$, рассмотрим $\Delta \in \in W$. Поскольку R – отношение эквивалентности и $\Gamma_0 R \Gamma$, $\Gamma_0 R \Delta$, получаем $\Gamma R \Delta$. Тогда $C \in \Delta$ (по определению R). Отсюда $M, \Delta \vDash C$ по предположению индукции.

  Докажем $\Rightarrow$. Предположим $\Box C \notin \Gamma$ и докажем $M, \Gamma \nvDash \Box C$. Для этого надо построить $\Delta \in W$ такое, что $M, \Delta \nvDash C$.

  Рассмотрим множество $V := \{D \mid \Box D \in \Gamma\} \cup \{\neg C\}$. Покажем, что V непротиворечиво. Действительно, иначе бы (по лемме (5.2)) $D_1, \ldots, D_k \vdash_{S5} C$ для некоторых $D_1, \ldots, D_k$, где $\Box D_1, \ldots, \Box D_k \in \Gamma$. Тогда по теореме дедукции $\vdash_{S5} \bigwedge\limits_i D_i \to C$, откуда по правилу монотонности $\vdash_{S5} \Box(\bigwedge\limits_i D_i) \to \Box C$. Но по пункту (5) леммы (13.1) (многократно) $\Box(\bigwedge\limits_i D_i) \equiv \bigwedge\limits_i \Box D_i$.

  Вспоминая, что $\Box D_i \in \Gamma$, получаем $(\bigwedge\limits_i \Box D_i) \in \Gamma$ по лемме (13.6). Из той же леммы следует, что максимальное множество содержит вместе с каждой формулой и все ей эквивалентные. Поэтому $\Box(\bigwedge\limits_i D_i) \in \Gamma$, и из $\vdash_{S5} \Box(\bigwedge\limits_i D_i) \to$ $\to \Box C$ по MP следует $\Box C \in \Gamma$. Это противоречит исходному предположению.

  Итак, V непротиворечиво. Выберем максимальное Δ, содержащее V. Из определения V получается: $\Gamma R \Delta$, $C \notin \Delta$ (так как $\neg C \in \Delta$). Тогда:

  $\Gamma_0 R \Delta$ по транзитивности R (то есть $\Delta \in W$),

  $M, \Delta \nvDash C$ по предположению индукции, так как $C \notin \Delta$.

  □

Наконец, из леммы (13.8) следует $W \nvDash A$, что и требовалось. □

Лекция 14

Полнота исчисления предикатов и её следствия

Определение 14.1. *Мощностью сигнатуры* Ω (обозначение: $|\Omega|$) назовём мощность множества всех её символов, то есть множества $Pred_\Omega \cup Const_\Omega \cup Fun_\Omega$.

Теорема 14.1 (Теорема о существовании модели)**.**

1) Пусть T – непротиворечивая в PC_Ω теория без равенства в сигнатуре Ω. Тогда T имеет модель мощности $|\Omega|$ или счётную, если Ω конечна.

2) Пусть T – непротиворечивая в $PC_\Omega^=$ теория с равенством в сигнатуре Ω. Тогда T имеет нормальную модель мощности $\leq |\Omega|$ или не более, чем счётную, если Ω конечна.

Доказательство:

Утверждение (1) в этом курсе не доказывается.

Докажем (1) $\Rightarrow$ (2).

Напомним, что непротиворечивость теории с равенством T понимается относительно $PC_\Omega^=$, то есть как непротиворечивость теории $T \cup Eq_\Omega$ относительно PC_Ω. Согласно пункту (1), $T \cup Eq_\Omega$ имеет модель M мощности $|\Omega|$ (или счётную). По лемме (9.1) о нормализации, $M \equiv \widetilde{M}$, где $\widetilde{M}$ – нормальная модель с носителем $\underline{M}/\approx$. Тогда $|\widetilde{M}| \leq |M|$. Таким образом, $\widetilde{M}$ – модель T нужной мощности. $\square$

Теорема 14.2 (Теорема Гёделя о полноте)**.**

1) Для теории T и замкнутой формулы A сигнатуры Ω имеем:

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

2) Для любой формулы A сигнатуры Ω имеем:

$$\vDash A \;\Rightarrow \vdash_{PC_\Omega} A.$$

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

$$T \vDash_{норм} A \;\Rightarrow\; T \vdash_{PC_\Omega^=} A.$$

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

$$\vDash_{норм} A \;\Rightarrow \vdash_{PC_\Omega^=} A.$$

Доказательство:

Не будем писать индексы при $\vdash$.

1) Если $T \nvdash A$, то $T \cup \{\neg A\}$ непротиворечива (по лемме (5.2); она переносится на предикатный случай). Тогда по теореме (14.1) о существовании модели теория $T \cup \{\neg A\}$ выполнима, и значит, $T \nvDash A$.

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

1$^=$) Аналогично доказательству пункта (1). Если $T \nvdash A$, то $T \cup \{\neg A\}$ непротиворечива в $PC_\Omega^=$, а потому нормально выполнима по теореме (14.1) о существовании модели. Следовательно, $T \nvDash_{\text{норм}} A$.

2$^=$) получается из пункта (1$^=$) аналогично доказательству пункта (2). $\square$

Теорема 14.3 (Теорема о компактности)**.**

1) Если любая конечная подтеория теории T выполнима, то и T выполнима.

2) Если любая конечная подтеория с равенством теории с равенством T нормально выполнима, то и T нормально выполнима.

Доказательство:

1) Если все конечные подмножества T выполнимы, то они непротиворечивы (утверждение (12.1)). Тогда T непротиворечива (лемма (11.1)) и, следовательно, выполнима (теорема (14.1) о существовании модели).

2) Аналогично доказательству пункта (1). □

Далее мы рассматриваем только теории с равенством и нормальные модели.

Теорема 14.4 (Теорема Лёвенгейма-Сколема о понижении мощности)**.** *Если теория в сигнатуре Ω выполнима, то она имеет модель мощности $\leq \max(|\Omega|, \aleph_0)$.*

Доказательство:

Если теория выполнима, то она непротиворечива (утверждение (12.1)). Тогда по теореме (14.1) о существовании модели она имеет модель нужной мощности. □

Теорема 14.5 (Теорема о повышении мощности)**.**

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

2) Если теория в сигнатуре Ω имеет бесконечную модель, то она имеет модели любой бесконечной мощности $k \geq |\Omega|$.

Доказательство:

1) Пусть T – данная теория. Согласно условию, для любого натурального n теория T имеет конечную модель мощности больше n.

Рассмотрим сигнатуру Ω^+, которая получается из Ω добавлением счётного множества новых констант $\{c_1, c_2, \ldots\}$. В этой сигнатуре построим теорию

$$T^+ \coloneqq T \cup \{c_i \neq c_j \mid i < j\}.$$

Докажем, что T^+ выполнима. По теореме (14.3) о компактности достаточно доказать, что любая конечная $T' \subset T$ выполнима. В самом деле,

$$T' \subset T \cup \{c_i \neq c_j \mid 1 \leq i < j \leq n\}$$

для некоторого n. Пусть M – модель теории T мощности $> n$. Превратим её в модель M' сигнатуры Ω^+, добавив интерпретацию констант $c_1, \ldots, c_n$ какими-нибудь различными элементами, а остальных новых констант – как угодно. Тогда $M' \vDash T \cup \{c_i \neq c_j \mid 1 \leq i < j \leq n\}$, и подавно $M' \vDash T'$.

Итак, T^+ выполнима. Если $M^+ \vDash T^+$, то $M^+ \vDash T$, и она бесконечна, так как все её элементы $(c_i)_{M^+}$ различны. Рассматривая M^+ в сигнатуре Ω, получаем бесконечную модель теории T.

2) Аналогично доказательству пункта (1), рассмотрим сигнатуру Ω^+ с множеством новых констант $\{c_i \mid i \in k\}$, где k – данная бесконечная мощность. В этой сигнатуре построим теорию

$$T^+ \coloneqq T \cup \{c_i \neq c_j \mid i, j \in k;\ i \neq j\}.$$

Любая конечная $T' \subset T^+$ содержится в некоторой теории

$$T \cup \{c_i \neq c_j \mid i, j \in I\},$$

где I – конечное подмножество k. Последняя теория выполнима в бесконечной модели теории T с интерпретацией констант c_i для $i \in I$ какими-нибудь различными элементами, а остальных новых констант – произвольно. Тогда по теореме (14.3) о компактности T^+ выполнима.

Из теории множеств следует, что $|\Omega^+| = k$. По теореме (14.4) Лёвенгейма-Сколема о понижении мощности T^+ имеет модель M^+ мощности $\leq k$. В этой модели интерпретации всех констант c_i различны (см. определение T^+), поэтому её мощность $\geq k$. Значит, $|M^+| = k$. Рассматривая M^+ в сигнатуре Ω, получим модель T мощности k. □

Нестандартные модели арифметики

Пусть $\mathbb{N}$ – стандартная модель PA (см. лекцию 12).

Теорема 14.6. *Существует счётная модель M такая, что $M \equiv \mathbb{N}$, но $M \ncong \mathbb{N}$.*

Доказательство:

Построим теорию в сигнатуре PA с дополнительной новой константой c:

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

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

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

Как и в предыдущих теоремах, докажем выполнимость T, используя теорему (14.3) о компактности. Для этого рассмотрим

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

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

По теореме (14.3) о компактности T выполнима, а по теореме (14.4) Лёвенгейма-Сколема о понижении мощности она имеет не более, чем счётную модель M^+.

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

Кроме того, для всех n имеем: $M^+ \vDash c \neq \underline{n}$, или $M^+ \vDash c_{M^+} \neq \underline{n}$. Рассмотрим теперь M^+ в исходной сигнатуре арифметики. Обозначим эту модель через M. Имеем: $M \vDash c_{M^+} \neq \underline{n}$ для всех n, а также $M \vDash Th(\mathbb{N})$, то есть $M \equiv \mathbb{N}$.

Наконец, докажем, что $M \ncong \mathbb{N}$. Предположим противное, и пусть $\alpha : M \cong \mathbb{N}$. Из $M \vDash c_{M^+} \neq \underline{n}$ по теореме (7.1) получаем $\mathbb{N} \vDash \alpha(c_{M^+}) \neq \underline{n}$, то есть $\alpha(c_{M^+}) \neq |\underline{n}|_{\mathbb{N}}$. Но $|\underline{n}|_{\mathbb{N}} = n$, то есть $\alpha(c_{M^+})$ не равно никакому натуральному числу. Получили противоречие. □

Замечание 14.1. Можно показать, что в модели M новые элементы – бесконечно большие, то есть больше всех натуральных чисел.

Теория множеств

Наивная теория множеств

Будем строить аксиоматику теории множеств в сигнатуре с двумя двуместными предикатными символами $\in, =$.

Определение 14.2. Рассмотрим сначала теорию $\mathcal{N}$ («*наивную теорию множеств*») со следующими аксиомами:

1) аксиома объёмности:

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

2) схема аксиом свёртывания:

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

Здесь $A(x, \ldots)$ – произвольная формула, в которой один параметр (например, a) заменён на связанную переменную x. Отметим, что y не входит в A.

Смысл аксиомы объёмности: если 2 множества состоят из одних и тех же элементов, то они равны.

Смысл аксиомы свёртывания: существует множество y, состоящее из всех x, обладающих свойством A, то есть $y = \{x \mid A(x, \ldots)\}$.

Утверждение 14.1. *Теория $\mathcal{N}$ противоречива.*

Доказательство:

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

1. $\forall x (x \in a \ \leftrightarrow \ x \notin x) \to (a \in a \ \leftrightarrow \ a \notin a)$ – аксиома II.1 исчисления предикатов.
2. $(a \in a \ \leftrightarrow \ a \notin a) \to \exists y (y \in y \ \leftrightarrow \ y \notin y)$ – аксиома II.2 исчисления предикатов.
3. $\forall x (x \in a \ \leftrightarrow \ x \notin x) \to \exists y (y \in y \ \leftrightarrow \ y \notin y)$ – по правилу силлогизма из 1, 2.
4. $\exists y \forall x (x \in y \ \leftrightarrow \ x \notin x) \to \exists y (y \in y \ \leftrightarrow \ y \notin y)$ – 3, второе правило Бернайса.
5. $\exists y \forall x (x \in y \ \leftrightarrow \ x \notin x)$ – аксиома свёртывания для $(a \notin a)$.
6. $\exists y (y \in y \ \leftrightarrow \ y \notin y)$ – 4, 5, MP.
7. $(A \ \leftrightarrow \ \neg A) \to B \wedge \neg B$ – подстановочный пример тавтологии (с любыми A, B). В частности, $(a \in a \ \leftrightarrow \ a \notin a) \to B \wedge \neg B$, где B – любая замкнутая формула.
8. $\exists y (y \in y \ \leftrightarrow \ y \notin y) \to B \wedge \neg B$ – 7, второе правило Бернайса.
9. $B \wedge \neg B$ – 6, 8, MP. □

Утверждение 14.2. *Существует хотя бы одно множество, формально:*

$$\vdash_{PC^=} \exists x (x = x).$$

Доказательство:

Это получается из аксиомы равенства $\forall x (x = x)$ и теоремы $\forall x A \to \exists x A$, которую легко доказать: из $\forall x A(x) \to A(a)$, $A(a) \to \exists x A(x)$ по транзитивности выводимости получаем то, что требовалось. □

Теория множеств Цермело

Самая известная аксиоматическая теория множеств – это теория Цермело-Френкеля с аксиомой выбора (ZFC). В этом курсе мы рассмотрим очень кратко более слабую теорию Цермело (Z).

Определение 14.3. Сигнатура *теории* Z состоит из $\in, =$. Её аксиомы – это аксиома объёмности, некоторые варианты аксиомы свёртывания и ещё 2 особые аксиомы (бесконечности и выбора).

1. Аксиома объёмности – такая же, как в $\mathcal{N}$:

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

Введём обозначение $a \subseteq b \coloneqq \forall z (z \in a \to z \in b)$ («a – подмножество b»). Тогда можем привести равносильную формулировку аксиомы объёмности:

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

2. Аксиома пары.

$$\forall x \forall y \exists z \forall u (u \in z \ \leftrightarrow \ (u = x \vee u = y)).$$

Смысл этой аксиомы: для всех x, y можно построить множество $z = \{x, y\}$ (неупорядоченную пару). Если $x = y$, то получается множество $\{x, x\}$, которое обозначается просто $\{x\}$.

3. Аксиома объединения.

$$\forall x \exists y \forall z (z \in y \ \leftrightarrow \ \exists u (z \in u \wedge u \in x)).$$

То есть $y = \{z \mid \exists u (z \in u \wedge u \in x)\}$. Другими словами, множество y является объединением всех множеств, являющихся элементами множества x, то есть $y = \bigcup\limits_{u \subseteq x} u$. Такое y называется *объединением множества* x и обозначается $\bigcup x$.

Теперь можем определить $x \cup y \coloneqq \bigcup \{x, y\}$, $\{x, y, z\} \coloneqq \{x, y\} \cup \{z\}$ и тому подобное.

4. Аксиома степени.

$$\forall x \exists y \forall z (z \in y \ \leftrightarrow \ z \subseteq x),$$

то есть $y = \{z \mid z \subseteq x\}$ – множество всех подмножеств x. Оно обычно обозначается $\mathcal{P}(x)$.

5. Схема аксиом выделения – ослабленный вариант свёртывания.

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

Здесь $A(z, \ldots)$ – произвольная формула, в которой один параметр (например, a) заменён на связанную переменную z. Отметим, что y не входит в A.

В этой теории мы не можем строить произвольные множества вида $\{x \mid A(x, \ldots)\}$. Однако неформально можно рассматривать такие совокупности (классы). Некоторые классы заведомо не являются множествами (они называются *собственными*). Например, $R \coloneqq \{x \mid x \notin x\}$ – собственный класс; в нашей теории это доказывается, см. предыдущий раздел.

Аксиома выделения утверждает, что пересечение любого класса $\{z \mid A(z, \ldots)\}$ с любым множеством x – множество. Или: подкласс любого множества – множество.

Утверждение 14.3. *Пусть* $V \coloneqq \{x \mid x = x\}$ *– класс всех множеств. Тогда*

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

Доказательство:
Очевидно, что $R \subseteq V$. По аксиоме выделения, если V – множество, то и R – множество. Значит, V – собственный класс. □

Утверждение 14.4 (Существование пустого множества)**.** $Z \vdash \exists y \forall x (x \notin y)$.

Доказательство:
Возьмём множество x из утверждения (14.2). По аксиоме выделения построим $y \coloneqq \{z \mid z \in x \wedge z \neq z\}$. Очевидно, что y пусто. □

Из аксиомы объёмности следует, что все пустые множества равны. Поэтому можно ввести обозначение $\varnothing$.

Определение 14.4. Теперь мы можем последовательно (по индукции) определить *натуральные числа*:

$$0 \coloneqq \varnothing, \quad 1 \coloneqq \{0\}, \quad 2 \coloneqq \{0, 1\}, \quad \ldots, \quad n+1 \coloneqq n \cup \{n\}, \quad \ldots$$

(определение фон Неймана).

То есть получается $n = \{0, 1, \ldots, n-1\}$. Однако для построения множества всех натуральных чисел нужна дополнительная аксиома.

6. Аксиома бесконечности.

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

Определение 14.5. Множество x назовём *индуктивным*, если оно имеет свойства, указанные в аксиоме бесконечности (6), то есть содержит 0 и вместе с каждым y содержит «$y + 1$».

Аксиома бесконечности (6) утверждает, что существует индуктивное множество.

Определение 14.6. Теперь можно определить *множество натуральных чисел* ω как наименьшее индуктивное множество:

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

Этот класс – действительно множество по аксиоме выделения, так как $\omega \subseteq x_0$ для индуктивного множества x_0 (какого-то, которое существует по аксиоме бесконечности).

Дальше можно развивать арифметику в ω и, в частности, превратить его в модель PA.

Определение 14.7. Имея неупорядоченные пары $\{a, b\}$, можно определить упорядоченные пары:

$$(a, b) \coloneqq \{\{a\}, \{a, b\}\}.$$

Если упорядоченные пары равны, то равны их соответственные элементы:

$$(a,b) = (a',b') \to a = a' \wedge b = b'.$$

Определение 14.8. Также можно определить *декартово произведение* (и доказать в Z, что оно всегда существует):

$$a \times b \coloneqq \{(x,y) \mid x \in a \wedge y \in b\}. \tag{14.1}$$

Определение 14.9. *Функция* $f : a \to b$ – это подмножество декартова произведения $f \subseteq a \times b$ такое, что:
1) $\mathrm{pr}_1 f = a$ и $\forall x(x \in a \to \exists y\ (x,y) \in f)$;
2) однозначность: $(x,y), (x,y') \in f \to y = y'$.

После этого можно определить формулы «f – биекция a на b» и «f – инъекция a в b».

Определение 14.10. Теперь определим *сравнение множеств по мощности*:

$$|a| = |b| \coloneqq \exists \text{ биекция } f : a \to b;$$
$$|a| \leq |b| \coloneqq \exists \text{ инъекция } f : a \to b.$$

Теорема 14.7 (Теорема Кантора-Бернштейна)**.**

$$Z \vdash \forall x \forall y(|x| \leq |y| \wedge |y| \leq |x| \to |x| = |y|).$$

Доказательство пропускаем.

Теорема 14.8 (Теорема Кантора)**.**

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

Доказательство:
Имеется инъекция x в $\mathcal{P}(x)$: она отображает каждый $a \in x$ в $\{a\}$. Значит, $|x| \leq$ $\leq |\mathcal{P}(x)|$. Докажем от противного, что $|x| \neq |\mathcal{P}(x)|$.
Предположим, что $f : x \to \mathcal{P}(x)$ – биекция. Тогда для некоторого $y \in x$ имеем: $\{z \in x \mid z \notin f(z)\} = f(y)$. Поэтому для всех $z \in x$ имеем: $z \in f(y) \leftrightarrow z \notin f(z)$. Тогда $y \in f(y) \leftrightarrow y \notin f(y)$. Получили противоречие.
Таким образом, $|x| < |\mathcal{P}(x)|$. □

По теореме кантора для любого множества можно построить множество большей мощности, значит, не существует множества самой большой мощности.

7. Аксиома выбора.

Запишем её (не совсем формально) в двух вариантах.

I) Если x – непустое множество попарно не пересекающихся непустых множеств (разбиение), то

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

II) Если существует отображение x на y (сюръекция), то $|y| \leq |x|$.

Из аксиомы выбора следует теорема о сравнении мощностей:

$$\forall x \forall y (|x| \leq |y| \vee |y| \leq |x|).$$

Кроме того, явно определяются «мощности» – это множества специального вида (кардиналы).

Другое известное следствие аксиомы выбора – лемма Цорна. Она утверждает, что если в частично упорядоченном множестве X каждая цепь (линейно упорядоченное подмножество) ограничена сверху, то X имеет максимальный элемент.

Лекция 15

Алгоритмы

Перечислим свойства алгоритмов (вычислительных устройств) неформально.

1. Алгоритмы работают со словами. *Слово* – это конечная последовательность символов (букв), взятых из некоторого конечного алфавита. Слово может быть пустым.

2. Алгоритм основан на программе. *Программа* – это конечный набор команд, которые записываются словами.

3. Алгоритм содержит «процессор», который обращается к программе и изменяет текущее состояние (слово).

4. Имеется начальное слово (вход) и заключительное слово (выход). Если заключительное слово не появляется, алгоритм работает бесконечно долго (зацикливание).

5. Вычисление разбивается на дискретные шаги.

6. Вычисление детерминированно (то есть каждый следующий шаг однозначно определён) и не обращается к случайным данным.

Имеется несколько точных определений алгоритма (рекурсивные функции, машины Тьюринга, алгоритмы Маркова, системы Поста, абстрактные RAM и другие). Все они оказываются эквивалентными.

Это понятие алгоритма абстрактно, так как предполагается неограниченность ресурсов времени и памяти.

Вычислимые функции

Будем записывать положительные натуральные числа как последовательности единиц, нуль – как 0. Конечный кортеж натуральных чисел $(n_1, \ldots, n_k)$ записывается как $n_1\#\ldots\#n_k$, где $\#$ – специальный символ (разделитель).

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

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

Область определения f обозначается $\operatorname{dom} f$, область значений – $\operatorname{rng} f$. В частности, возможно, что $\operatorname{dom} f = \varnothing$ (пустая функция).

Определение 15.1. Функция $f : \mathbb{N}^k \tilde{\to} \mathbb{N}$ или $f : \Delta^* \tilde{\to} \Delta^*$ называется *вычислимой*, если существует алгоритм M со следующими свойствами:

- если $x \in \operatorname{dom} f$, то M на входе x заканчивает работу и выдаёт $f(x)$. Это записывается так: $M : x \mid\Rightarrow f(x)$;
- если $x \notin \operatorname{dom} f$, то M на входе x зацикливается. Это записывается так: $M : x \mid\Rightarrow ?$.

Утверждение 15.1 (Тезис Чёрча-Тьюринга)**.** *Всякая вычислимая функция вычислима по Тьюрингу.*

Разрешимость и перечислимость

Определение 15.2. Множество слов $A \subseteq \Delta^*$ называется *разрешимым*, если его характеристическая функция χ_A вычислима.

(Функция $\chi_A : \Delta^* \to \{0, 1\}$ принимает значение 1 на A и 0 на его дополнении.)

Аналогично определяются разрешимые подмножества $\mathbb{N}^k$.

Утверждение 15.2.

1) Если A разрешимо, то его дополнение $(-A)$ (до Δ^* или $\mathbb{N}^k$) разрешимо.

2) Если A и B разрешимы, то $A \cap B$, $A \cup B$ разрешимы.

Доказательство:

1) $\chi_{-A} = g \circ \chi_A$, где $g(0) = 1$, $g(1) = 0$. Функция g вычислима, и композиция сохраняет вычислимость, поэтому функция χ_{-A} вычислима, значит, $(-A)$ разрешимо.

2) $\chi_{A\cap B} = 1$, если $\chi_A = 1$ и $\chi_B = 1$ (иначе $\chi_{A\cap B} = 0$).
$\chi_{A\cup B} = 1$, если $\chi_A = 1$ или $\chi_B = 1$ (иначе $\chi_{A\cup B} = 0$). □

Сформулируем следствие.

Утверждение 15.3. *Конечные множества разрешимы.*

Доказательство:

Одноэлементное множество $\{n\}$ разрешимо. Тогда по индукции получаем, что конечное множество разрешимо, так как оно является объединением одноэлементных множеств. □

Приведём примеры разрешимых множеств: $\mathbb{N}$ (так как характеристическая функция – константа, значит, вычислима), $\varnothing$ (как дополнение к $\mathbb{N}$), $2\mathbb{N}$ – множество чётных чисел (так как характеристическая функция зависит от количества единиц в нашей записи числа), P – множество простых чисел (решето Эратосфена).

Утверждение 15.4. *Существуют неразрешимые подмножества* $\mathbb{N}$.

Доказательство:

Каждый алгоритм записывается некоторой программой, то есть множеством слов, состоящих из символов, взятых из некоторого конечного алфавита. Таким образом, множество программ счётно. Значит, мощность множества разрешимых множеств счётна. Таким образом, существуют неразрешимые подмножества $\mathbb{N}$. □

Определение 15.3. Множество слов $A \subseteq \Delta^*$ (или $A \subseteq \mathbb{N}^k$) называется *полуразрешимым*, если его полухарактеристическая функция χ_A^- вычислима.

(Частичная функция $\chi_A^- : \Delta^* \tilde{\to} \{1\}$ принимает значение 1 на A и не определена на его дополнении.)

Утверждение 15.5. *Если A и B полуразрешимы, то $A\cap B$, $A\cup B$ полуразрешимы.*

Доказательство:

$\chi_{A\cap B} = 1$, если $\chi_A = 1$ и $\chi_B = 1$ (иначе $\chi_{A\cap B}$ не определена).
$\chi_{A\cup B} = 1$, если $\chi_A = 1$ или $\chi_B = 1$ (иначе $\chi_{A\cup B}$ не определена). □

Приведём пример множества, про которое нам известно, что оно полуразрешимо, но неизвестно, что оно разрешимо:

$$\{n \mid \text{в разложении } \pi \text{ встретится } n \text{ нулей подряд}\}.$$

Теорема 15.1 (Теорема Поста)**.** *Множество слов $A \subseteq \Delta^*$ разрешимо $\Leftrightarrow$ A и $-A$ полуразрешимы.*

Доказательство:

Докажем $\Rightarrow$. Если χ_A вычислима, то и χ_A^- вычислима, так как $\chi_A^- = h \circ \chi_A$, где $h(1) = 1$, $h(0)$ не определено.

Аналогично, $-A$ полуразрешимо, так как $-A$ разрешимо по утверждению (15.2).

Докажем $\Leftarrow$. Если $\chi_A^-(x) = 1$, то $\chi_A(x) = 1$. Если $\chi_{-A}^-(x) = 1$, то $\chi_A(x) = 0$. Так как $x \in A$ или $x \in (-A)$, то χ_A вычислима, значит, A разрешимо. □

Определение 15.4. Множество $A \subseteq \Delta^*$ (или $A \subseteq \mathbb{N}^k$) называется *перечислимым*, если оно пусто или является множеством значений некоторой вычислимой последовательности, то есть тотальной функции $\mathbb{N} \to \Delta^*$.

Теорема 15.2. *Существуют вычислимые биекции $\mathbb{N} \to \mathbb{N}^k$ и $\mathbb{N} \to \Delta^*$ (для конечного Δ), причём обратные биекции тоже вычислимы.*

Доказательство пропускаем (оно несложное).

Теорема 15.3. *Множество $A \subseteq \Delta^*$ (или $A \subseteq \mathbb{N}^k$) перечислимо $\Leftrightarrow$ A полуразрешимо.*

Доказательство:

Рассмотрим сначала случай $A \subseteq \mathbb{N}$.

Докажем $\Rightarrow$.

$\varnothing$ разрешимо.

Пусть $A = \operatorname{rng} f$ для вычислимой $f : \mathbb{N} \to \mathbb{N}$. Тогда χ_A^- вычислима по следующему алгоритму.

0. Пусть на входе дано n.

1. Полагаем $i := 0$.

2. В цикле по i проверяем, верно ли $f(i) = n$. Если да, выдаём 1 и заканчиваем работу. Если нет, полагаем $i := i + 1$ и продолжаем цикл.

Докажем $\Leftarrow$.

$\varnothing$ перечислимо.

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

Пусть $\gamma : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ – вычислимая биекция (теорема (15.2); например, это может быть канторовская нумерация пар натуральных чисел). Пусть $\gamma(n) = (\alpha(n), \beta(n))$. Тогда α и β тоже вычислимы.

Построим последовательность f, перечисляющую A следующим образом. Для нахождения $f(n)$ делаем $\beta(n)$ шагов в вычислении $\chi_A^-(\alpha(n))$ (или меньше, если вычисление заканчивается раньше). Если за это время вычисление закончилось, полагаем $f(n) := \alpha(n)$. Иначе полагаем $f(n) := a_0$.

Тогда $\operatorname{rng} f = A$. Действительно, включение $\subseteq$ очевидно, так как по построению множество значений функции f формируется только из элементов множества A. Обратно, пусть $a \in A$. Тогда $\chi_A^-(a)$ вычислится через сколько-то (k) шагов. Так как γ – биекция, имеем $\gamma(n) = (a, k)$ для некоторого n. То есть $\alpha(n) = a$, $\beta(n) = k$. По построению тогда $f(n) = a$.

Общий случай сводится к случаю $A \subseteq \mathbb{N}$ с помощью теоремы (15.2). □

Теорема 15.4. *Пусть $h : \Delta^* \to \Delta^*$ – вычислимая тотальная функция.*
1) Если $A \subseteq \Delta^*$ разрешимо, то $h^{-1}(A)$ разрешимо.
2) Если $A \subseteq \Delta^*$ перечислимо, то $h(A)$ и $h^{-1}(A)$ перечислимы.

Доказательство:
1) $x \in h^{-1}(A) \Leftrightarrow h(x) \in A$. Тогда $\chi_{h^{-1}(A)} = \chi_A \circ h$, а композиция вычислимых функций вычислима.

2) Докажем для прообраза. $x \in h^{-1}(A) \Leftrightarrow h(x) \in A$. Тогда $\chi^-_{h^{-1}(A)} = \chi_A^- \circ h$. И используем теорему (15.3).

Докажем для образа. Если $A = \varnothing$, то всё очевидно. Если $A = \operatorname{rng} f$ для вычислимой f, то $h(A) = \operatorname{rng}(h \circ f)$. □

Универсальная вычислимая функция. Неразрешимость

Сформулируем ключевой результат теории алгоритмов.

Теорема 15.5 (Теорема об универсальной вычислимой функции)**.** *Существует вычислимая функция $F : \mathbb{N} \times \mathbb{N} \tilde{\to} \mathbb{N}$ такая, что для любой вычислимой $f : \mathbb{N} \tilde{\to} \mathbb{N}$ существует m такое, что для всех n $f(n) \simeq F(m, n)$.*

Здесь $\simeq$ означает условное равенство, то есть обе части определены одновременно и равны, когда определены.

Идея доказательства: нумеруем программы, работающие с натуральными числами. F вычисляется компьютером, который по номеру программы восстанавливает саму программу и запускает её на различных входах. То есть $F(m, n)$ – результат работы программы с номером m на входе n (если этот результат существует).

Обозначим через φ_m вычислимую функцию с номером m, то есть $\varphi_m(n) \simeq F(m, n)$. Тогда всякая вычислимая $f : \mathbb{N} \tilde{\to} \mathbb{N}$ совпадает с φ_m, где m – номер программы, вычисляющей f.

Теорема 15.6. *Существует перечислимое неразрешимое подмножество в $\mathbb{N}$.*

Доказательство:
Пусть $d(x) \simeq F(x, x) \simeq \varphi_x(x)$. Рассмотрим $K := \operatorname{dom} d$. Ясно, что K полуразрешимо. Докажем, что K неразрешимо. Для этого по теореме Поста (15.1) надо доказать, что $(-K)$ не является полуразрешимым.

Допустим противное. Тогда $-K = \operatorname{dom} \varphi_n$, где $\varphi_n = \chi^-_{-K}$. Тогда для любого x имеем: $x \notin K \Leftrightarrow x \in \operatorname{dom} \varphi_n$. В частности, $n \notin K \Leftrightarrow n \in \operatorname{dom} \varphi_n$. Но по определению K имеем: $n \in K \Leftrightarrow n \in \operatorname{dom} \varphi_n$. Таким образом, $n \in K \Leftrightarrow n \notin K$. Получили противоречие, аналогичное парадоксу Рассела и доказательству теоремы Кантора.

Таким образом, K неразрешимо. □

Разрешимость теорий первого порядка

Рассмотрим теории в конечной сигнатуре Ω.

Лемма 15.1. *Множества Fm_Ω, CFm_Ω разрешимы.*

Доказателсьтво пропускаем.

Для теории $T \subseteq CFm_\Omega$ обозначим через $[T]$ множество всех её замкнутых теорем, то есть $[T] = \{A \in CFm_\Omega \mid T \vdash A\}$.

Теорема 15.7. *Если T – разрешимое множество, то множество $[T]$ перечислимо.*

Доказательство:

Будем записывать доказательства в T в виде $A_1\# \dots \# A_n$. Пусть Док(T) – множество всех этих доказательств.

Заметим, что Док(T) разрешимо: по любой последовательности формул можно узнать, является ли она правильно построенным доказательством, так как элементы T, аксиомы исчисления предикатов и применения правил вывода распознаются алгоритмически.

Имеем: $[T] = h[\text{Док}(T)] \cap CFm_\Omega$, где h – вычислимая функция, выбирающая последний член кортежа. По теореме (15.4) множество $h[\text{Док}(T)]$ перечислимо. По лемме (15.1) CFm_Ω разрешимо и, следовательно, перечислимо. Пересечение сохраняет перечислимость по пункту (2) утверждения (15.2). □

Теорема 15.8. *Если T – разрешимое множество и T полна, то множество $[T]$ разрешимо.*

Доказательство:

По теореме (15.7) это множество перечислимо. Поэтому, учитывая теорему (15.3), достаточно доказать перечислимость его дополнения и применить теорему Поста (15.1).

Имеем: $-[T] = -CFm_\Omega \cup (CFm_\Omega \backslash [T])$. Первое множество перечислимо, ввиду разрешимости CFm_Ω. Поскольку T полна, $CFm_\Omega \backslash [T] = \{A \in CFm_\Omega \mid T \vdash \neg A\}$. Тогда это множество равно $f^{-1}([T])$, где f – вычислимая функция, которая добавляет в начале слова знак $\neg$. По теореме (15.4) оно перечислимо. Объединение сохраняет перечислимость. □

Теорема Гёделя о неполноте

Напомним, что определимые (в арифметической сигнатуре $\{+, \cdot, 0, 1, =\}$) подмножества стандартной модели $\mathbb{N}$ называются *арифметическими*.

Теорема 15.9 (Теорема Гёделя об определимости)**.** *Всякое перечислимое подмножество $\mathbb{N}$ является арифметическим.*

Доказательство пропускаем.

Теорема 15.10 (Первая теорема Гёделя о неполноте)**.** *Пусть T – теория в сигнатуре PA с разрешимым множеством аксиом, причём $\mathbb{N} \models T$. Тогда T неполна.*

В частности, PA неполна.

Доказательство:

Допустим, что T полна. По теореме (15.8) $[T]$ разрешимо. Поскольку $\mathbb{N} \vDash T$, получаем $[T] = Th(\mathbb{N})$, значит, $Th(\mathbb{N})$ разрешима.

Рассмотрим теперь множество K, построенное в доказательстве теоремы (15.6). По теореме (15.9) существует формула A (с одной свободной переменной) такая, что для всех n имеем: $n \in K \Leftrightarrow \mathbb{N} \vDash A(n)$. Здесь $A(n)$ – формула, оценённая в $\mathbb{N}$. Заметим, что $\mathbb{N} \vDash A(n) \Leftrightarrow \mathbb{N} \vDash A(\underline{n})$, где $\underline{n}$ – терм (сумма единиц); это следует из леммы (12.1). Таким образом, $n \in K \Leftrightarrow A(\underline{n}) \in Th(\mathbb{N})$. Поэтому $K = h^{-1}(Th(\mathbb{N}))$, где h – вычислимая функция, переводящая число n в формулу $A(\underline{n})$. По теореме (15.4) K разрешимо. Получили противоречие.

Таким образом, T неполна. □

МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in

ЛЕКЦИИ УЧЕНЫХ МГУ