

Математическая логика

Михайлов Максим

22 октября 2022 г.

Оглавление

Лекция 1	12 февраля	4
0	Мотивация	4
0.1	Математикам	4
0.2	Программистам	5
1	Исчисление высказываний	5
1.1	Язык	5
1.2	Метаязык и предметный язык	5
1.3	Сокращения записи	6
1.4	Теория моделей	6
1.5	Теория доказательств	7
1.6	Правило Modus Ponens и доказательство	7
Лекция 2	19 февраля	8
2	Интуиционистская логика	11
2.1	ВНК-интерпретация (Brouwer–Heyting–Kolmogorov)	11
Лекция 3	26 февраля	13
2.2	Естественный (натуральный) вывод	13
2.3	Теория решеток	14
Лекция 4	5 марта	17
2.4	Табличные модели	17
2.5	Модели Крипке	18
Лекция 5	12 марта	20
3	Изоморфизм Карри-Ховарда	20
3.1	Алгебраические типы	20
3.2	Применение восьмой аксиомы интуиционистской логики	21
4	Исчисление предикатов	22
4.1	Язык исчисления предикатов	22
4.2	Теория моделей	23
4.3	Теория доказательств	24
Лекция 6	19 марта	25
4.4	Вхождение	25
4.5	Свобода для подстановки	26
Лекция 7	2 апреля	28
4.6	Полнота исчисления предикатов	28
Лекция 8	9 апреля	32

4.7	Теорема Гёделя о полноте исчисления предикатов	32
4.8	Неразрешимость исчисления предикатов	34
Лекция 9	16 апреля	36
5	Теория первого порядка	36
5.1	Аксиоматика Пеано	36
5.2	Формальная арифметика	38
Лекция 10	30 апреля	40
6	Арифметизация математики	40
6.1	Рекурсивные функции	40
6.2	Проблема останова	42
Лекция 11	7 мая	45
7	Гёделева нумерация	45
7.1	Самоприменение	46
Лекция 12	14 мая	49
8	Теория множеств	49
Лекция 13	21 мая	53
8.1	Аксиома выбора	53
8.2	Мощность множеств	54

Лекция 1

12 февраля

0 Мотивация

0.1 Математикам

Аксиома (Архимеда). Для любого $k > 0$ найдётся n , такое что $kn > 1$.

Под эту аксиому не подходят бесконечно малые числа и это является проблемой. Например, $\lim_{x \rightarrow +\infty} \frac{1}{x} = 0 = \lim_{x \rightarrow +\infty} \frac{1}{x^2}$, но мы хотим уметь различать эти два числа. Ньютон предложил идею бесконечно малых чисел, откуда пошли последовательности. Возникает вопрос — что такое последовательность и что такое число?

Общепринятое определение целых чисел \mathbb{N} происходит из теории множеств. Однако эта теория содержит в себе множество фундаментальных парадоксов, от которых нельзя избавиться.

Возникает вопрос — а что такое множество? Посмотрим на некоторое множество $A = \{x \mid x \notin x\}$. Содержит ли оно себя, $A \in A$? На этот вопрос нельзя ответить, это называется парадокс Рассела. Есть простой способ его разрешить — запретить ставить такой вопрос. Нет вопроса — нет парадокса. Существование такого парадокса ставит под вопрос существование любого множества — а существует ли \mathbb{N} ? Может быть его существование парадоксально, просто мы не нашли этот парадокс. Пришло чуть более умное решение парадокса — запретим множества, содержащие себя. Таким образом вывели аксиоматику теории множеств (Цермело — Френкеля).

Пример. Рассмотрим множество всех чисел, которые можно задать в ≤ 1000 слов русского языка. Фраза “наименьшее число, которое нельзя задать в ≤ 1000 слов” содержит ≤ 1000 слов, т.е. такое число принадлежит искомому множеству — парадокс.

Возникает идея — человеческий язык порождает парадоксы, поэтому нужно задать новый язык, который их не порождает. Этот язык и является математической логикой.

0.2 Программистам

Математическая логика применяется в двух областях (*для программистов*):

1. Языки программирования
2. Формальные доказательства

Для языков программирования матлогика применима как теория типов (*переменных*).

Формальные доказательства нужны например для smart-контрактов, где корректность программы критически важна, т.к. если в нём есть ошибка, у вас злоумышленник заберет все деньги, а вы не сможете этот контракт откатить.

1 Исчисление высказываний

1.1 Язык

Определение. Язык содержит в себе:

1. Пропозициональные переменные

A_i — большая буква начала латинского алфавита, возможно с индексом и/или штрихом.

2. Связки

Пусть α, β — высказывания. Тогда $(\alpha \rightarrow \beta), (\alpha \& \beta), (\alpha \vee \beta), (\neg \alpha)$ — высказывания.

α, β называются **метапеременными**.

Примечание. Математическая логика алгеброподобна (*а не анализоподобна*), т.к. в ней много определений и мало доказательств.

1.2 Метаязык и предметный язык

У нас есть два различных языка — **предметный язык** и **метаязык**. Метаязык — русский, предметный язык мы определили выше.

Пример. $\alpha \rightarrow \beta$ — метавыражение; $A \rightarrow (A \rightarrow A)$ — предметное выражение.

Обозначение. Метапеременные обозначаются различными способами в зависимости от того, что они обозначают:

- Буквы греческого алфавита ($\alpha, \beta, \gamma, \dots, \varphi, \psi$) — выражения
- Заглавные буквы конца латинского алфавита (X, Y, Z) — произвольные переменные

Пример. $X \rightarrow Y \Rightarrow A \rightarrow B$ — подстановка переменных. Этот синтаксис не формален, мы будем записывать так:

$$(X \rightarrow Y)[X := A, Y := B] \equiv A \rightarrow B$$

Соглашение. символы логических операций не пишутся в метаязыке.

Пример.

$$\begin{aligned} (\alpha \rightarrow (A \rightarrow X))[\alpha := A, X := B] &\equiv A \rightarrow (A \rightarrow B) \\ (\alpha \rightarrow (A \rightarrow X))[\alpha := (A \rightarrow P), X := B] &\equiv (A \rightarrow P) \rightarrow (A \rightarrow B) \end{aligned}$$

1.3 Сокращения записи

- $\vee, \&, \neg$ — скобки слева направо (*лево-ассоциативные операции*) (*не коммутативные*)
- \rightarrow — правоассоциативная.

Примечание. Здесь операторы записаны в порядке их приоритета

Пример. Расставим скобки в следующем выражении:

$$\begin{aligned} A \rightarrow B \& C \rightarrow D \\ A \rightarrow ((B \& C) \rightarrow D) \end{aligned}$$

1.4 Теория моделей

Модель состоит из:

Обозначение.

- P — некоторое множество предметных переменных
 - τ — множество высказываний предметного языка
 - V — множество истинностных значений. Классическое — $\{\text{П}, \text{Л}\}$
 - $\llbracket \cdot \rrbracket : \tau \rightarrow V$ — оценка высказывания (*высказывание ставится в скобки*).
1. $\llbracket x \rrbracket : P \rightarrow V$ — задается при оценке.
 2. $\llbracket \alpha \star \beta \rrbracket = \llbracket \alpha \rrbracket \star \llbracket \beta \rrbracket$, где \star есть логическая операция ($\vee, \&, \neg, \rightarrow$), а \star определено естественным образом как элемент метаязыка.

1.5 Теория доказательств

Определение. Схема высказывания — строка, соответствующая определению высказывания + метапеременные.

Пример.

$$(\alpha \rightarrow (\beta \rightarrow (A \rightarrow \alpha)))$$

10 схем аксиом:

1. $\alpha \rightarrow \beta \rightarrow \alpha$
2. $(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \gamma)$
3. $\alpha \rightarrow \beta \rightarrow \alpha \& \beta$
4. $\alpha \& \beta \rightarrow \alpha$
5. $\alpha \& \beta \rightarrow \beta$
6. $\alpha \rightarrow \alpha \vee \beta$
7. $\beta \rightarrow \alpha \vee \beta$
8. $(\alpha \rightarrow \gamma) \rightarrow (\beta \rightarrow \gamma) \rightarrow (\alpha \vee \beta \rightarrow \gamma)$
9. $(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \neg \beta) \rightarrow \neg \alpha$
10. $\neg \neg \alpha \rightarrow \alpha$

1.6 Правило Modus Ponens и доказательство

Определение. Доказательство (вывод) есть конечная последовательность высказываний $\alpha_1 \dots \alpha_n$, где α_i — либо аксиома, либо $\exists k, l < i : \alpha_k \equiv \alpha_l \rightarrow \alpha_i$ (*правило Modus Ponens*)

Пример. $\vdash A \rightarrow A$

- | | |
|--|------------|
| 1. $A \rightarrow A \rightarrow A$ | сх. акс. 1 |
| 2. $A \rightarrow (A \rightarrow A) \rightarrow A$ | сх. акс. 1 |
| 3. $(A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow (A \rightarrow A) \rightarrow A) \rightarrow (A \rightarrow A)$ | сх. акс. 2 |
| 4. $(A \rightarrow (A \rightarrow A) \rightarrow A) \rightarrow (A \rightarrow A)$ | М.Р. 1, 3 |
| 5. $A \rightarrow A$ | М.Р. 2, 4 |

Определение. Доказательство $\alpha_1 \dots \alpha_n$ доказывает выражение β , если $\alpha_n \equiv \beta$

Лекция 2

19 февраля

Обозначение. Большая греческая буква середины греческого алфавита (Γ, Δ, Σ) — список высказываний.

Определение (следование). α следует из Γ (обозначается $\Gamma \models \alpha$), если $\Gamma = \gamma_1 \dots \gamma_n$ и всегда, когда все $\llbracket \gamma_i \rrbracket = \text{И}$, то $\llbracket \alpha \rrbracket = \text{И}$.

Пример. $\models \alpha \rightarrow \alpha$ общезначимо.

Определение. Теория Исчисление высказываний **корректно**, если при любом α из $\vdash \alpha$ следует $\models \alpha$.

Определение. Исчисление **полно**, если при любом α из $\models \alpha$ следует $\vdash \alpha$.

Теорема 1 (о дедукции).

$$\Gamma, \alpha \vdash \beta \Leftrightarrow \Gamma \vdash \alpha \rightarrow \beta$$

Доказательство.

\Leftarrow Пусть $\Gamma \vdash \alpha \rightarrow \beta$, т.е. существует доказательство $\delta_1 \dots \delta_n$, где $\delta_n \equiv \alpha \rightarrow \beta$

Построим новое доказательство: $\delta_1 \dots \delta_n, \alpha$ (гипотеза), β (М.Р.). Эта новая последовательность — доказательство $\Gamma, \alpha \vdash \beta$

\Rightarrow Рассмотрим $\delta_1 \dots \delta_n, \Gamma, \alpha \vdash \beta$. Рассмотрим последовательность $\sigma_1 = \alpha \rightarrow \delta_1 \dots \sigma_n = \alpha \rightarrow \delta_n$. Это не доказательство.

Но эту последовательность можно дополнить до доказательства, так что каждый σ_i есть аксиома, гипотеза или получается через М.Р. Докажем это.

Доказательство. База: $n = 0$ — очевидно.

Переход: пусть $\sigma_0 \dots \sigma_n$ — доказательство. Покажем, что между σ_n и σ_{n+1} можно добавить формулы так, что σ_{n+1} будет доказуемо.

У нас есть 3 варианта обоснования δ_{n+1}

1. δ_{n+1} — аксиома или гипотеза, $\neq \alpha$

Будем нумеровать дробными числами, потому что нам ничто это не запрещает, т.к. нам нужна только упорядоченность.

$n + 0.2$ δ_{n+1} — верно, т.к. это аксиома или гипотеза

$n + 0.4$ $\delta_{n+1} \rightarrow \alpha \rightarrow \delta_{n+1}$ (аксиома 1)

$n + 1$ $\alpha \rightarrow \delta_{n+1}$ (М.Р. $n + 0.2, n + 0.4$)

2. $\delta_{n+1} \equiv \alpha$

$n + 0.2, 0.4, 0.6, 0.8, 1$ — доказательство $\alpha \rightarrow \alpha$

3. $\delta_k \equiv \delta_l \rightarrow \delta_{n+1}, k, l \leq n$

k $\alpha \rightarrow (\delta_l \rightarrow \delta_{n+1})$

l $\alpha \rightarrow \delta_l$

$n + 0.2$ $(\alpha \rightarrow \delta_l) \rightarrow (\alpha \rightarrow (\delta_l \rightarrow \delta_{n+1})) \rightarrow (\alpha \rightarrow \delta_{n+1})$ (аксиома 2)

$n + 0.4$ $(\alpha \rightarrow \delta_l \rightarrow \delta_{n+1}) \rightarrow (\delta \rightarrow \delta_{n+1})$ (М.Р. $n + 2, l$)

$n + 1$ $\alpha \rightarrow \delta_{n+1}$ (М.Р. $n + 0.4, k$)

□

□

Теорема 2. Пусть $\vdash \alpha$. Тогда $\models \alpha$.

Доказательство. Индукция по длине доказательства: каждая $\llbracket \delta_i \rrbracket = \text{И}$, если $\delta_1 \dots \delta_n$ — доказательство α

Рассмотрим n и пусть $\llbracket \delta_1 \rrbracket = \text{И}, \dots, \llbracket \delta_n \rrbracket = \text{И}$.

Тогда рассмотрим основание δ_{n+1}

1. δ_{n+1} — аксиома. Это упражнение.

Пример. $\delta_{n+1} \equiv \alpha \rightarrow \beta \rightarrow \alpha$

$$\triangleleft \llbracket \alpha \rightarrow \beta \rightarrow \alpha \rrbracket^{\llbracket \alpha \rrbracket := a, \llbracket \beta \rrbracket := b} = \text{И}$$

a	b	$\beta \rightarrow \alpha$	$\alpha \rightarrow \beta \rightarrow \alpha$
Л	Л	И	И
Л	И	Л	И
И	Л	И	И
И	И	И	И

Аналогично можно доказать для остальных аксиом.

2. $\delta_{n+1} - \text{М.Р. } \delta_k = \delta_l \rightarrow \delta_{n+1}$

Фиксируем оценку. Тогда $\llbracket \delta_k \rrbracket = \llbracket \delta_l \rrbracket = \text{И}$. Тогда:

$\llbracket \delta_k \rrbracket$	$\llbracket \delta_{n+1} \rrbracket$	$\llbracket \delta_k \rrbracket = \llbracket \delta_l \rightarrow \delta_{n+1} \rrbracket$
Л	Л	И
Л	И	И
И	Л	Л
И	И	И

Первых трёх вариантов не может быть в силу $\llbracket \delta_k \rrbracket = \llbracket \delta_l \rrbracket = \text{И}$. Таким образом, $\llbracket \delta_{n+1} \rrbracket = \text{И}$.

□

Теорема 3 (о полноте). Пусть $\models \alpha$. Тогда $\vdash \alpha$.

Фиксируем набор переменных из α : $P_1 \dots P_n$.

Рассмотрим $\llbracket \alpha \rrbracket^{P_1 := x_1 \dots P_n := x_n} = \text{И}$

Обозначение. $_{[\beta]} \alpha \equiv \begin{cases} \alpha, & \llbracket \beta \rrbracket = \text{И} \\ \neg \alpha, & \llbracket \beta \rrbracket = \text{Л} \end{cases}$ и $_{[x]} \alpha \equiv \begin{cases} \alpha, & x = \text{И} \\ \neg \alpha, & x = \text{Л} \end{cases}$

Докажем, что $\underbrace{_{[x_1]} P_1, \dots, _{[x_n]} P_n}_{\Pi} \vdash _{[\alpha]} \alpha$

Доказательство. По индукции по длине формулы:

База: $\alpha = P_i$ $_{[P_i]} P_i \vdash _{[P_i]} P_i$, значит $\Pi \vdash _{[P_i]} P_i$

Переход: пусть $\eta, \zeta : \Pi \vdash _{[\eta]} \eta, \Pi \vdash _{[\zeta]} \zeta$ (по индукционному предположению). Покажем, что $\Pi \vdash _{[\eta \star \zeta]} \eta \star \zeta$, где \star — все связи

Это упражнение.

□

Лемма 1. $\Gamma, \eta \vdash \zeta, \Gamma, \neg \eta \vdash \zeta$. Тогда $\Gamma \vdash \zeta$.

Доказательство.

1. α ($\in \Gamma$)
2. $\alpha \rightarrow (\neg\beta \rightarrow \alpha)$ (a. 1)
3. $\neg\beta \rightarrow \alpha$ (M.P. 1,2)
4. $\neg\alpha$ ($\in \Gamma$)
5. $\neg\alpha \rightarrow (\neg\beta \rightarrow \neg\alpha)$ (a. 1)
6. $\neg\beta \rightarrow \neg\alpha$ (M.P. 4,5)
7. $(\neg\beta \rightarrow \alpha) \rightarrow (\neg\beta \rightarrow \neg\alpha) \rightarrow \neg\neg\beta$ (a. 9)
8. $(\neg\beta \rightarrow \neg\alpha) \rightarrow \neg\neg\beta$ (M.P. 3,7)
9. $\neg\neg\beta$ (M.P. 6,8)
10. $\neg\neg\beta \rightarrow \beta$ (a. 10)
11. β (M.P. 9,10)

□

Доказательство теоремы о полноте. $\models \alpha$, т.е. $[x_1]P_1 \dots [x_n]P_n \vdash_{[\alpha]} \alpha$. Но $\llbracket \alpha \rrbracket = \Pi$ при любой оценке. Тогда $[x_1]P_1 \dots [x_n]P_n \vdash \alpha$ при все x_i .

Лемма 2 (об исключении допущения). Если $[x_1]P_1 \dots [x_n]P_n \vdash \alpha$ и $[x_1]P_1 \dots [x_n]\neg P_n \vdash \alpha$, то $[x_1]P_1 \dots [x_{n-1}]P_{n-1} \vdash \alpha$

$$\left. \begin{array}{l} [x_1]P_1 \dots [x_{n-1}]P_{n-1}, P_n \vdash \alpha \\ [x_1]P_1 \dots [x_{n-1}]P_{n-1}, \neg P_n \vdash \alpha \end{array} \right\} \xrightarrow{\text{по лемме}} [x_1]P_1 \dots [x_{n-1}]P_{n-1} \vdash \alpha$$

□

2 Интуиционистская логика

2.1 ВНК-интерпретация (Brouwer–Heyting–Kolmogorov)

Определим выражения:

- $\alpha \& \beta$ — есть α и β
- $\alpha \vee \beta$ — есть α либо β и мы знаем, какое
- $\alpha \rightarrow \beta$ — есть способ перестроить α в β
- \perp — конструкция без построения (*bottom*)
- $\neg\alpha \equiv \alpha \rightarrow \perp$

Теория доказательств есть классическая логика без десятой схемы аксиомы, вместо нее $\alpha \rightarrow \neg\alpha \rightarrow \beta$

Теория моделей — теория, в которой $\llbracket \alpha \rrbracket$ — открытое множество в Ω — топологическом пространстве.

В ней определено следующее:

$$\begin{aligned}\llbracket \alpha \ \&\ \beta \rrbracket &= \llbracket \alpha \rrbracket \cap \llbracket \beta \rrbracket \\ \llbracket \alpha \ \vee \ \beta \rrbracket &= \llbracket \alpha \rrbracket \cup \llbracket \beta \rrbracket \\ \llbracket \alpha \rightarrow \beta \rrbracket &= ((X \setminus \llbracket \alpha \rrbracket) \cup \llbracket \beta \rrbracket)^\circ \\ \llbracket \perp \rrbracket &= \emptyset \\ \llbracket \neg\alpha \rrbracket &= (X \setminus \llbracket \alpha \rrbracket)^\circ\end{aligned}$$

Лекция 3

26 февраля

2.2 Естественный (натуральный) вывод

Рассмотрим новый способ записи доказательств — в виде деревьев, называемый естественным выводом.

Тогда язык будет состоять из переменных $A \dots Z, \vee, \&, \perp, \vdash, -$

У нас используются следующие правила вывода:

1. $\frac{}{\Gamma \vdash \gamma, \gamma \in \Gamma}$ (аксиома)
2. $\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \rightarrow \psi}$ (введение \rightarrow)
3. $\frac{\Gamma \vdash \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \& \psi}$ (введение $\&$)
4. $\frac{\Gamma \vdash \varphi \rightarrow \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi}$ (удаление \rightarrow)
5. $\frac{\Gamma \vdash \varphi \& \psi}{\Gamma \vdash \varphi}$ (удаление $\&$)
6. $\frac{\Gamma \vdash \varphi \& \psi}{\Gamma \vdash \psi}$ (удаление $\&$)
7. $\frac{\Gamma \vdash \varphi}{\Gamma \vdash \psi \vee \varphi}$ (введение \vee)
8. $\frac{\Gamma \vdash \psi}{\Gamma \vdash \psi \vee \varphi}$ (введение \vee)
9. $\frac{\Gamma \vdash \perp}{\Gamma \vdash \varphi}$ (удаление \perp)

$$10. \frac{\Gamma, \varphi \vdash \rho \quad \Gamma, \psi \vdash \rho \quad \Gamma \vdash \varphi \vee \psi}{\Gamma \vdash \rho}$$

$$\text{Пример. } \frac{\overline{A \vdash A} \text{ (акс.)}}{\vdash A \rightarrow A} \text{ (введение } \rightarrow \text{)}$$

$$\text{Пример. } \frac{\overline{A \& B \vdash A \& B} \text{ (акс.)} \quad \overline{A \& B \vdash A \& B} \text{ (акс.)}}{\frac{A \& B \vdash B \quad A \& B \vdash A}{A \& B \vdash B \& A} \text{ (введение } \rightarrow \text{)}} \vdash A \& B \rightarrow B \& A$$

2.3 Теория решеток

Определение.

- **Частичный порядок** — рефлексивное, транзитивное, антисимметричное отношение.
- **Линейный порядок** — сравнимы любые два элемента.
- **Наименьший элемент** S — такой $k \in S$, что если $x \in S$, то $k \leq x$
- **Минимальный элемент** S — такой $k \in S$, что нет $x \in S$, что $x \leq k$
- **Множество верхних граней** a и b : $\{x \mid a \leq x \& b \leq x\}$.
- **Множество нижних граней** a и b : $\{x \mid x \leq a \& x \leq b\}$.
- $a + b$ — наименьший элемент множества верхних граней (может не существовать).
- $a \cdot b$ — наибольший элемент множества нижних граней.
- **Решетка** — множество + отношение, где для каждого a, b есть как $a + b$, так и $a \cdot b$.
- **Дистрибутивная решетка** — если всегда $a \cdot (b + c) = a \cdot b + a \cdot c$

Лемма 3. В дистрибутивной решетке $a + b \cdot c = (a + b)(a + c)$

Определение.

- **Псевдодополнение** a и b обозначается $a \rightarrow b$ и равно наибольшему элементу множества $\{c \mid a \cdot c \leq b\}$
- **Импликативная решетка** — решетка, где $\forall a, b \exists a \rightarrow b$
- 0 — наименьший элемент решетки.
- 1 — наибольший элемент решетки.
- **Псевдобулева алгебра (алгебра Гейтинга)** — импликативная решетка с нулём.
- **Булева алгебра** — псевдобулева алгебра, такая что $a + (a \rightarrow 0) = 1$

Пример.

$$\begin{array}{ccc} 1 & \longrightarrow & b \\ \downarrow & & \downarrow \\ a & \longrightarrow & 0 \end{array}$$

$$a \cdot 0 = 0$$

$$1 \cdot b = b$$

$$a \cdot b = 0$$

$$a + b = 1$$

Лемма 4. В импликативной решетке всегда есть 1.

Доказательство. Возьмём $a \rightarrow a = 1$ для некоторого a .

$$a \rightarrow a = \mathbf{n}\{x \mid a \cdot x \leq a\} = \mathbf{n}(A)$$

Таким образом, A имеет наибольший элемент и это $a \rightarrow a$ □

Теорема 4.

- Любая алгебра Гейтинга — модель интуиционистского исчисления высказываний.
- Любая булева алгебра — модель классического исчисления высказываний.

Определение (топология). Рассмотрим множество X , называемое “носитель” и $\Omega \subset \mathcal{P}(X)$ — подмножество подмножеств X , называемое “топология”, такое что:

1. $\bigcup_{\alpha} x_i \in \Omega$, где $x_i \in \Omega$
2. $\bigcap_{i=1}^n x_i \in \Omega$, где $x_i \in \Omega$
3. $\emptyset \in \Omega, X \in \Omega$

Пример. Пусть X — узлы дерева, Ω — все множества узлов, которые содержат узлы вместе со всеми потомками.

Определение.

$$X^{\circ} \stackrel{\text{def}}{=} \text{наиб}\{w \mid w \subseteq X, w \text{ — открыто}\}$$

Теорема 5. Пусть (X, Ω) — топологическое пространство, $a + b = a \cup b$, $a \cdot b = a \cap b$, $a \rightarrow b = ((X \setminus a) \cup b)^{\circ}$, $a \leq b \Leftrightarrow a \subseteq b$, тогда (Ω, \leq) есть алгебра Гейтинга.

Пример. Дискретная топология — $\Omega = \mathcal{P}(X)$. Тогда (Ω, \leq) — булева алгебра.

1. $X^\circ = X$

2. $a \rightarrow 0 = (X \setminus a \cup \emptyset) = X \setminus a$

Таким образом, $a + (a \rightarrow 0) = a + X \setminus a = X$

Определение. Пусть X — все формулы логики. Определим отношение порядка $\alpha \leq \beta$ это $\alpha \vdash \beta$. Будем говорить, что $\alpha \approx \beta$, если $\alpha \vdash \beta$ и $\beta \vdash \alpha$.

$(X/\approx, \leq)$ есть алгебра Гейтинга.

Определение. $(X/\approx, \leq)$ — алгебра Линденбаума, где X, \approx из интуиционистской логики.

Теорема 6. Алгебры Гейтинга — полная модель интуиционистской логики.

Доказательство. $\models \alpha$ — истинно в любой алгебре Гейтинга, в частности в $(X/\approx, \leq)$. $\llbracket \alpha \rrbracket = 1$, т.е. $\llbracket \alpha \rrbracket = \llbracket A \rightarrow A \rrbracket$, т.е. $\alpha \in [A \rightarrow A]_{\approx}$, т.е. $A \rightarrow A \vdash \alpha$. \square

Лекция 4

5 марта

Определение. Полный порядок — линейный, где в каждом подмножестве есть наименьший элемент. Множество с полным порядком называют **вполне упорядоченным**.

Пример. \mathbb{N} — вполне упорядоченное множество

\mathbb{R} — не вполне упорядоченное множество, т.к. (a, b) не имеет наименьшего $\forall a, b$. Кроме того, \mathbb{R} не имеет наименьшего.

Определение. Предпорядок — транзитивное, рефлексивное отношение.

Как мы знаем из домашнего задания, по предпорядку можно построить частичный порядок, сжав компоненты связности в классы эквивалентности.

2.4 Табличные модели

Определение. Табличная модель для интуиционистского исчисления высказываний:

- V — множество истинностных значений
- $f_{\rightarrow}, f_{\&}, f_{\vee} : V^2 \rightarrow V$
- Выделенное истинное значение $T \in V$
- Оценка переменных $\llbracket P_i \rrbracket \in V, f_{\mathcal{P}} : P_i \rightarrow V$

И $\llbracket P_i \rrbracket = f_{\mathcal{P}}(P_i), \llbracket \alpha \star \beta \rrbracket = f_{\star}(\llbracket \alpha \rrbracket, \llbracket \beta \rrbracket), \llbracket \neg \alpha \rrbracket = f_{\neg}(\llbracket \alpha \rrbracket)$

$\models \alpha$ означает, что $\llbracket \alpha \rrbracket = T$ при любой $f_{\mathcal{P}}$

Определение. Конечная табличная модель — табличная модель с конечным V .

Теорема 7. У интуиционистского исчисления высказываний не существует корректной полной конечной табличной модели.

Неформально эта теорема говорит, что нельзя считать, что в интуиционистской логике есть три значения — истинна, ложь и “неизвестно”.

2.5 Модели Крипке

Идея моделей Крипке следующая: общезначимое утверждение истинно во всех мирах.

Определение (модели Крипке).

1. $W = \{W_i\}$ — множество миров
2. \leq — частичный порядок на W
3. Отношение вынужденности $W_j \Vdash P_i$, где P_i — переменная, т.е. $(\Vdash) \subset W \times \mathcal{P}$

При этом, если $W_j \Vdash P_i$ и $W_j \leq W_k$, то $W_k \Vdash P_i$

Определение.

- $W_i \Vdash \alpha$ и $W_i \Vdash \beta$, тогда (*и только тогда*) $W_i \Vdash \alpha \& \beta$
- $W_i \Vdash \alpha$ или $W_i \Vdash \beta$, тогда (*и только тогда*) $W_i \Vdash \alpha \vee \beta$
- Пусть во всех $W_i \leq W_j$ всегда, когда $W_j \Vdash \alpha$, имеет место $W_j \Vdash \beta$. Тогда $W_i \Vdash \alpha \rightarrow \beta$
- $W_i \Vdash \neg \alpha$ значит, что α не вынуждено нигде, начиная с W_i : $W_i \leq W_j \Rightarrow W_j \nVdash \alpha$

Теорема 8. Если $W_i \Vdash \alpha$ и $W_i \leq W_j$, то $W_j \Vdash \alpha$

Определение. Если $W_i \Vdash \alpha$ при всех $W_i \in W$, то $\models \alpha$

Теорема 9. ИИВ корректно в моделях Крипке.

Доказательство. Рассмотрим (W, Ω) — топологию, где $\Omega = \{w \subset W \mid \text{если } w_i \in w, w_i \leq w_j, \text{ то } w_j \in w\}$. Это можно представить как множество подлесов, где любая вершина входит со своими потомками.

$\{W_k \mid W_k \Vdash P_j\}$ — открытое множество, что очевидно из определения Ω и \Vdash .

Примем $\llbracket P_i \rrbracket = \{W_k \mid W_k \Vdash P_j\}$ и аналогично $\llbracket \alpha \rrbracket = \{W_k \mid W_k \Vdash \alpha\}$. Корректность этого определения докажем в ДЗ.

Поскольку любая топология является корректной моделью ИИВ, искомое доказано. \square

Доказательство теоремы о нетабличности. Предположим обратное, т.е. существует конечная табличная модель, $|V| = n$.

Рассмотрим следующую формулу:

$$\varphi_n = \bigvee_{\substack{1 \leq i, j \leq n+1 \\ i \neq j}} (P_i \rightarrow P_j \& P_j \rightarrow P_i)$$

1. $\not\models \varphi_n$. Почему? Рассмотрим последовательность миров, таких что $W_i \models P_i$, состоящую из $n + 1$ мира. Тогда $W_i \not\models (P_i \rightarrow P_j) \& (P_j \rightarrow P_i)$, т.к. $W_i \not\models P_j$, но $W_i \models P_i$, таким образом $\not\models (P_i \rightarrow P_j) \& (P_j \rightarrow P_i)$ и $\not\models \bigvee (P_i \rightarrow P_j) \& (P_j \rightarrow P_i)$, а значит $\not\models \varphi_n$
2. $\models \varphi_n$ в V по принципу Дирихле: $\exists i \neq j : \llbracket P_i \rrbracket = \llbracket P_j \rrbracket$, а значит $\llbracket P_i \rightarrow P_j \rrbracket = \text{И}$, и соответственно $\llbracket \varphi_n \rrbracket = \text{И}$.

Т.к. $\models \varphi_n$, то $\vdash \varphi_n$, но это не так — противоречие. \square

Теорема 10 (Дизъюнктивность ИИВ). $\vdash \alpha \vee \beta$ влечет $\vdash \alpha$ или $\vdash \beta$

Определение. Алгебра Гёделя — алгебра Гейтинга, в которой из $a + b = 1$ следует $a = 1$ или $b = 1$

Определение. Пусть \mathcal{A} — алгебра Гейтинга. Тогда $\Gamma(\mathcal{A})$ получается переименовыванием 1 в ω и добавлением нового элемента $1_{\Gamma(\mathcal{A})}$, являющегося единицей для новой алгебры.

Теорема 11. $\Gamma(\mathcal{A})$ есть алгебра Гейтинга и $\Gamma(\mathcal{A})$ Гёделева.

Доказательство. Очевидно. \square

Определение. Гомоморфизм алгебр Гейтинга — отображение $\varphi : \mathcal{A} \rightarrow \mathcal{B}$, где \mathcal{A}, \mathcal{B} — алгебры Гейтинга, $\varphi(a \star b) = \varphi(a) \star \varphi(b)$, $\varphi(1_{\mathcal{A}}) = 1_{\mathcal{B}}$, $\varphi(0_{\mathcal{A}}) = 0_{\mathcal{B}}$

Теорема 12. Если $a \leq b$, то $\varphi(a) \leq \varphi(b)$

Определение. Пусть α — формула ИИВ, f, g — оценки ИИВ, где $f : \text{ИИВ} \rightarrow \mathcal{A}$, $g : \text{ИИВ} \rightarrow \mathcal{B}$. Тогда φ **согласовано** с f, g , если $\varphi(f(\alpha)) = g(\alpha)$

Теорема 13. Если $\varphi : \mathcal{A} \rightarrow \mathcal{B}$ согласована с f, g и $\llbracket \alpha \rrbracket_g \neq 1_{\mathcal{B}}$, то $\llbracket \alpha \rrbracket_f \neq 1_{\mathcal{A}}$

Доказательство теоремы 10. Рассмотрим алгебру Линденбаума \mathcal{L} , $\Gamma(\mathcal{L})$ и $\varphi : \Gamma(\mathcal{L}) \rightarrow \mathcal{L}$ — гомоморфизм.

$$\varphi(x) = \begin{cases} 1_{\mathcal{L}}, & x = \omega \\ 1_{\mathcal{L}}, & x = 1_{\Gamma(\mathcal{L})} \\ x, & \text{иначе} \end{cases}$$

Пусть $\vdash \alpha \vee \beta$. Тогда $\llbracket \alpha \vee \beta \rrbracket_{\Gamma(\mathcal{L})} = 1_{\Gamma(\mathcal{L})}$, но по Гёделевости $\Gamma(\mathcal{L})$ $\llbracket \alpha \rrbracket = 1$ или $\llbracket \beta \rrbracket = 1$.

Пусть $\not\models \alpha$ и $\not\models \beta$. Тогда $\varphi(\llbracket \alpha \rrbracket) \neq 1_{\mathcal{L}}$ и $\varphi(\llbracket \beta \rrbracket) \neq 1_{\mathcal{L}}$. Тогда $\llbracket \alpha \rrbracket_{\Gamma(\mathcal{L})} \neq 1_{\mathcal{L}}$, $\llbracket \beta \rrbracket \neq 1_{\mathcal{L}}$ — противоречие. \square

Лекция 5

12 марта

3 Изоморфизм Карри-Ховарда

Примечание. Эта тема в нашем курсе рукомахательная.

Пусть p — программа, т.е. функция, принимающая α и возвращающая β , т.е. $p : \alpha \rightarrow \beta$

Можем посмотреть на это с другой стороны: p доказательство, что из α следует β , например в Haskell $f\ a = a$ гласит, что f доказывает, что $A \rightarrow A$, где подразумевается $\forall A$.

Такое сопоставление программам доказательств и высказываниям типов называется изоморфизмом Карри-Ховарда:

логическое исчисление	типизированное λ -исчисление
логическая формула	тип
доказательство	программа
доказуемая формула	обитаемый тип
\rightarrow	функция
$\&$	упорядоченная пара
\vee	алгебраический тип (<i>тип-сумма</i>)

Примечание. Обитаемый тип — тип, у которого есть хотя бы один экземпляр.

Несложно заметить, что логика, соответствующая λ -исчислению, является интуиционистской, поэтому мы её в основном изучаем.

3.1 Алгебраические типы

Рассмотрим следующее определение списка в Pascal:

```

type list : record
  nul : boolean;
  case nul of
    true: ;
    false: next ^list
  end
end;

```

Рассмотрим то же самое в C, опустив bool и скажем, что `nul = (next == null)` (это в какой-то степени костыльно):

```

struct list {
  next: *list;
}

```

Определим таким же способом дерево:

```

struct tree {
  tree* left;
  tree* right;
  int value;
}

```

Это ещё более костыльно, т.к. то, является ли вершина листом, закодировано в неявном виде.

Определение. Отмеченное (дизъюнктивное) объединение множеств A, B обозначается $A \sqcup B$ или $A \uplus B$ ¹ и равно $\{\langle "A", a \rangle \mid a \in A\} \cup \{\langle "B", b \rangle \mid b \in B\}$.

Примечание. Это определение интуиционистское по своей сути, т.к. если дано $s \in A \sqcup B$, то мы знаем, из какого множества s .

Определение. Тип, соответствующий такому объединению множеств, называется **алгебраическим**

Пример. В C++ такой тип реализован как `std::variant<...>`

Пример. Список в Haskell:

```

data List a = nil | Cons a (List a)

```

3.2 Применение восьмой аксиомы интуиционистской логики

Вспомним восьмую аксиому интуиционистской² логики и запишем её как правило натурального вывода:

¹ или ещё десятком других символов

² и классической

$$\frac{\Gamma \vdash \alpha \rightarrow \gamma \quad \Gamma \vdash \beta \rightarrow \gamma \quad \Gamma \vdash \alpha \vee \beta}{\Gamma \vdash \gamma}$$

Рассмотрим программу в Haskell, которая преобразует список в строку:

```
let rec string_of_list l =
  match l with
  | Nil -> "Nil"
  | Cons(head, tail) -> head ^ ":" ^ string_of_list tail
```

Подставим в рассматриваемую аксиому соответствующие значения:

$$\frac{\Gamma \vdash Nil \rightarrow string \quad \Gamma \vdash list \rightarrow string \quad \Gamma \vdash Nil \vee list}{\Gamma \vdash string}$$

Несложно заметить, что эта аксиома описывает match в Haskell — мы даем выражения после “->”, т.е. правила Nil -> string, list -> string и элемент Nil или list, а match возвращает string.

4 Исчисление предикатов

4.1 Язык исчисления предикатов

Выражения в этом языке бывают двух видов:

1. Логические выражения, называемые “предикаты” или “формулы”
2. Предметные выражения, называемые “термы”

θ — метaperменная для термов.

Термы бывают двух видов:

- Атомы:
 - Предметные переменные обозначаются буквами $a, b, c \dots$
 - Метaperменные обозначаются буквами x, y, z
- Применение функциональных символов:
 - Функциональные символы: f, g, h и записывается $f(\theta_1 \dots \theta_n)$
 - Метaperменная тоже обозначается f

Логические выражения:

- Применение предикатных символов $P(\theta_1, \dots \theta_n)$, где P — метaperменная для предикатных символов, а предикатный символ — $A, B, C \dots$
- Связки $\&, \vee, \neg, \rightarrow$ с правилами из языка классической логики.

- Кванторы ³ $\forall x.\varphi$ или $\exists x.\varphi$, где φ — любое логическое выражение.

Мы используем жадность кванторов. ⁴ Это значит, что квантор берет в φ все, пока не встретит конец выражения или скобку, которая оканчивает этот квантор.

Пример. $\forall x.P(x) \& \forall y.P(y) \equiv \forall x.(P(x) \& (\forall y.P(y)))$

4.2 Теория моделей

Определим оценку формулы в исчислении предикатов:

1. Фиксируем D — предметное множество, $V = \{\text{И}, \text{Л}\}$
2. Каждому $f_i(x_1 \dots x_n)$ сопоставим функцию $f_{f_i} : D^n \rightarrow D$
3. Каждому $P_j(x_1 \dots x_m)$ сопоставим функцию ⁵ $f_{p_m} : D^m \rightarrow V$
4. Каждой x_i сопоставим $f_{x_i} \in D$
 - $\llbracket x \rrbracket = f_{x_i}$
 - $\llbracket \alpha \star \beta \rrbracket$ — так же, как в исчислении высказываний.
 - $\llbracket P_i(\theta_1 \dots \theta_n) \rrbracket = f_{p_i}(\llbracket \theta_1 \rrbracket \dots \llbracket \theta_n \rrbracket)$
 - $\llbracket f_j(\theta_1 \dots \theta_n) \rrbracket = f_{f_j}(\llbracket \theta_1 \rrbracket \dots \llbracket \theta_m \rrbracket)$
 - $\llbracket \forall x.\varphi \rrbracket = \begin{cases} \text{И}, & \text{если } \llbracket \varphi \rrbracket = \text{И при всех } k \in D \\ \text{Л}, & \text{иначе} \end{cases}$
 - $\llbracket \exists x.\varphi \rrbracket = \begin{cases} \text{И}, & \text{если } \llbracket \varphi \rrbracket = \text{И при некотором } k \in D \\ \text{Л}, & \text{иначе} \end{cases}$

Пример. $\forall x.\forall y.E(x, y)$

Пусть $D = \mathbb{N}$, $E(x, y) = \begin{cases} \text{И}, & x = y \\ \text{Л}, & x \neq y \end{cases}$

$\llbracket \forall x.\forall y.E(x, y) \rrbracket_{x:=1, y:=2} = \text{Л}$, т.к. $\llbracket E(x, y) \rrbracket = \text{Л}$.

Вспомним определение предела последовательности из матанализа:

$$\forall \varepsilon > 0 \quad \exists N \quad \forall n > N \quad |a_n - a| < \varepsilon$$

³ По записи кванторов нет общепринятого соглашения.

⁴ В отношении жадности кванторов также нет соглашения; встречается запись, где квантор — унарная операция, аналогичная \neg

⁵, называемую предикат

Перепишем это определение с богомерзкого языка матанализа на православный язык исчисления предикатов.⁶

Пусть $(>)(a, b) = G(a, b)$, $|a| = m_+(a)$, $(-)(a, b) = m_-(a, b)$, $m_a : n \mapsto a_n$, $0() = m_0$

$$\forall \varepsilon. \varepsilon \rightarrow 0 \exists N. \forall n. (n > N) \rightarrow (|a_n - a| < \varepsilon)$$

$$\forall \varepsilon. \varepsilon \rightarrow 0 \exists N. \forall n. (n > N) \rightarrow (|a_n - a| < \varepsilon)$$

$$\forall e. G(e, m_0) \exists n_0. \forall n. G(n, n_0) \rightarrow G(e, m_+(m_-(m_a(n), a)))) < \varepsilon)$$

4.3 Теория доказательств

Все аксиомы исчисления высказываний + Modus Ponens + две схемы аксиом + два правила:

1. $(\forall x. \varphi) \rightarrow \varphi[x := \theta]$
2. $\varphi[x := \theta] \rightarrow \exists x. \varphi$

Обе эти схемы применимы только если θ свободен для подстановки вместо x в φ , т.е. никакое свободное вхождение x в θ не станет связным.

Пример.

```
int f(int x) {
    x = y;
}
```

После замены $y := x$ код станет следующим:

```
int f(int x) {
    x = x;
}
```

И код потеряет свой смысл.

Правила следующие:

1. $\frac{\varphi \rightarrow \psi}{\varphi \rightarrow (\forall x. \psi)}$ (правило \forall)
2. $\frac{\psi \rightarrow \varphi}{(\exists x. \psi) \rightarrow \varphi}$ (правило \exists)

⁶ Это термины лектора, все претензии от адептов матанализа и других религий — к нему.

Лекция 6

19 марта

Пример. $\frac{\varphi \rightarrow \psi}{\exists x.(\varphi \rightarrow \psi)}$ — возможно доказуемо, но это не правило вывода для \exists .

Определение. $\alpha_1 \dots \alpha_n$ — **доказательство**, если выполняется одно из:

1. α_i — аксиома
2. Существует $j, k < i$, такие что $\alpha_k = \alpha_j \rightarrow \alpha_i$
3. Существует j , такое что $\alpha_j = \varphi \rightarrow \psi$ и $\alpha_i = (\exists x.\varphi) \rightarrow \psi$, причём x не входит свободно в ψ .
4. Существует j , такое что $\alpha_j = \psi \rightarrow \varphi$ и $\alpha_i = \psi \rightarrow \forall x.\varphi$, причём x не входит свободно в ψ .

4.4 Вхождение

Рассмотрим некоторую формулу и рассмотрим вхождения x в неё:

$$(P(\underbrace{x}_1) \vee Q(\underbrace{x}_2)) \rightarrow (R(\underbrace{x}_3) \& (\overbrace{\forall \underbrace{x}_4. P_1(\underbrace{x}_5)}))$$

Область действия \forall по x

- Вхождение 4 связывающее
- Вхождение 5 связано вхождением 4
- Вхождения 1-3 свободны.

Случай множественного связывания:

$$\underbrace{\forall x. \forall y. \overbrace{\forall x. \forall y. \underbrace{\forall x. P(x)}}}_{\text{Область действия } \forall \text{ по } x}$$

Область действия \forall по x

Определение. Вхождение **свободно**, если не связано.

Примечание. Свободно входящие переменные нельзя переименовывать, т.к. к формуле могут приписать кванторы, которые используют данные имена переменных. Это ограничение не распространяется на связанные переменные.

Любая аксиома есть предикат.

4.5 Свобода для подстановки

Определение. θ **свободен для подстановки** вместо x в φ , если никакая свободная переменная в θ не станет связанной в $\varphi[x := \theta]$

Обозначение. $\varphi[x := \theta]$ — заменить все свободные вхождения x в φ на θ

Пример.

$$\begin{aligned} (\forall x. \forall y. \forall x. P(x))[x := y] &\equiv \forall x. \forall y. \forall x. P(x) \\ P(x) \vee \forall x. P(x)[x := y] &\equiv P(y) \vee \forall x. P(x) \\ (\forall y. x = y)[x := y] &\equiv \forall y. y = y \end{aligned}$$

В этой формуле новый y связался.

Примечание. В определении можно опустить “свободная” в нашем исчислении, но это не верно в достаточно извращенных исчислениях.

Лемма 5. Пусть $\vdash \alpha$. Тогда $\vdash \forall x. \alpha$

Доказательство. Т.к. $\vdash \alpha$, то существует $\gamma_1 \dots \gamma_n : \gamma_n \equiv \alpha$

Создадим новое доказательство.

$$\begin{array}{ll} (1) & \gamma_1 \\ & \vdots \\ (n) & \gamma_n \\ (n+1) & A \& A \rightarrow A \quad (\text{акс.}) \\ (n+2) & \alpha \rightarrow ((A \& A \rightarrow A) \rightarrow \alpha) \quad (\text{акс.}) \\ (n+3) & (A \& A \rightarrow A) \rightarrow \alpha \quad (\text{М.Р. } n, n+2) \\ (n+4) & (A \& A \rightarrow A) \rightarrow \forall x. \alpha \quad (\text{введение } \forall) \\ (n+5) & \forall x. \alpha \quad (\text{М.Р. } n+1, n+4) \end{array}$$

□

Лемма 6. $(\alpha \rightarrow \varphi \rightarrow \psi) \rightarrow \alpha \& \varphi \rightarrow \psi$

Лемма 7. $(\alpha \& \varphi \rightarrow \psi) \rightarrow (\alpha \rightarrow \varphi \rightarrow \psi)$

Доказательство двух лемм. По теореме о полноте исчисления высказываний.

□

Теорема 14 (о дедукции). Пусть даны Γ, α, β .

1. Если $\Gamma, \alpha \vdash \beta$, то $\Gamma \vdash \alpha \rightarrow \beta$ при условии, если в доказательстве $\Gamma, \alpha \vdash \beta$ не применялись правила для \forall, \exists по переменным, входящим свободно в α .
2. Если $\Gamma \vdash \alpha \rightarrow \beta$, то $\Gamma, \alpha \vdash \beta$.

Доказательство. По индукции. Пусть доказано $\alpha \rightarrow \delta_i$ для $i \in [1, n]$, докажем $\alpha \rightarrow \delta_{n+1}$.

Рассмотрим случаи:

1. Схемы аксиом 1-10 — аналогично¹.
2. М.Р. — аналогично
3. Аксиомы 11-12 — аналогично первому пункту.
4. Пусть δ_{n+1} получено правилом $\forall : \delta_{n+1} \equiv \varphi \rightarrow \forall x.\psi$ и существует $\delta_k \equiv \varphi \rightarrow \psi$ и $k \leq n$, причём x не входит свободно в φ .

При этом в новом доказательстве уже доказано $\alpha \rightarrow \delta_k$

$$\begin{array}{lll}
 (1) & \alpha \rightarrow \delta_1 & \\
 & \vdots & \\
 (k) & \alpha \rightarrow (\varphi \rightarrow \psi) & \\
 & \vdots & \\
 (n) & \alpha \rightarrow \delta_n & \\
 & \vdots & \\
 (n+0.1) & (\alpha \rightarrow \varphi \rightarrow \psi) \rightarrow \alpha \& \varphi \rightarrow \psi & \text{(лемма 6)} \\
 (n+0.2) & \alpha \& \varphi \rightarrow \psi & \text{(М.Р.)} \\
 (n+0.3) & \alpha \& \varphi \rightarrow \forall x.\psi & \text{(введение } \forall) \\
 (n+0.4) & (\alpha \& \varphi \rightarrow \forall x.\psi) \rightarrow (\alpha \rightarrow \varphi \rightarrow \forall x.\psi) & \text{(лемма 7)} \\
 (n+1) & \alpha \rightarrow \varphi \rightarrow \forall x.\psi & \text{(М.Р.)}
 \end{array}$$

□

Примечание. Доказательство пункта 2 аналогично исходному доказательству для исчисления высказываний.

¹ доказательству ИВ

Лекция 7

2 апреля

Определение. Будем говорить, что $\Gamma \models \alpha$, т.е. α следует из Γ , если при всех оценках, таких что все $\gamma \in \Gamma$ $\llbracket \gamma \rrbracket = \text{И}$, выполнено $\llbracket \alpha \rrbracket = \text{И}$

Пример (странный случай). $x = 0 \vdash \forall x.x = 0$, но $x = 0 \not\models \forall x.x = 0$

Условие для корректности: правила для кванторов по свободным переменным из Γ запрещены. Тогда $\Gamma \vdash \alpha$ влечёт $\Gamma \models \alpha$ и $\llbracket \alpha[x := \Theta] \rrbracket = \llbracket \alpha \rrbracket^{x := \llbracket \Theta \rrbracket}$

Примечание. Здесь и далее мы предполагаем условие корректности.

4.6 Полнота исчисления предикатов

Определение. Γ — непротиворечивое, если $\Gamma \not\vdash \alpha \ \& \ \neg\alpha$ ни при каком α

Пример.

- Непротиворечивое: $\emptyset, A \vee \neg A$
- Противоречивое: $A \ \& \ \neg A$

Мы будем рассматривать непротиворечивое множество замкнутых бескванторных формул и обозначать (\dots) .

Пример.

- $\{A\}$
- $\{0 = 0\}$

Определение. Моделью для (\dots) Γ называется такая модель, что каждая формула из Γ оценивается в И.

Определение. (\dots) Γ называется **полным**, если для каждой замкнутой бескванторной формулы α либо $\alpha \in \Gamma$, либо $\neg\alpha \in \Gamma$.

Аналогично определяется для не бескванторного множества.

Теорема 15. Если $\Gamma (\dots)$ и α — замкнутая бескванторная формула, то либо $\Gamma \cup \{\alpha\}$, либо $\Gamma \cup \{\neg\alpha\} — (\dots)$

Аналогичное верно для не бескванторного множества.

Доказательство. Пусть и $\Gamma \cup \{\alpha\}$, и $\Gamma \cup \{\neg\alpha\}$ — противоречивы, т.е.:

$$\Gamma, \alpha \vdash \beta \ \& \ \neg\beta \quad \Gamma, \neg\alpha \vdash \beta \ \& \ \neg\beta$$

$$\begin{cases} \Gamma \vdash \alpha \rightarrow \beta \ \& \ \neg\beta \\ \Gamma \vdash \neg\alpha \rightarrow \beta \ \& \ \neg\beta \end{cases} \Rightarrow \Gamma \vdash \beta \ \& \ \neg\beta$$

Т.е. Γ — противоречиво. Это противоречие. \square

Теорема 16. Если $\Gamma — (\dots)$ и в языке счётное количество формул¹, то можно построить Δ — полное (\dots) , такое что $\Gamma \subset \Delta$.

Аналогичное верно для не бескванторного множества.

Доказательство. Пусть $\varphi_1, \varphi_2, \dots$ — замкнутые бескванторные формулы исчисления предикатов.

$$\Gamma_0 := \Gamma$$

$$\Gamma_1 := \Gamma_0 \cup \{\varphi_1\} \text{ или } \Gamma_0 \cup \{\neg\varphi_1\} — \text{смотря что непротиворечиво}$$

$$\Gamma_2 := \Gamma_1 \cup \{\varphi_2\} \text{ или } \Gamma_1 \cup \{\neg\varphi_2\} — \text{смотря что непротиворечиво}$$

\vdots

$\Gamma^* := \bigcup_i \Gamma_i$, тогда Γ^* — полное и непротиворечивое. Первое очевидно, покажем второе.

Пусть $\Gamma^* \vdash \beta \ \& \ \neg\beta$. Это конечное доказательство $\delta_1 \dots \delta_s$ использует конечное число гипотез, пусть они $\gamma_1 \dots \gamma_k$ и $\gamma_i \in \Gamma_{R_i}$. Возьмём $\Gamma_{\max(R_i)}$. Тогда $\Gamma_{\max(R_i)} \vdash \beta \ \& \ \neg\beta$ — противоречие. \square

Теорема 17. Любое полное (\dots) Γ имеет модель, т.е. существует оценка $\llbracket \cdot \rrbracket$, такая что если $\gamma \in \Gamma$, то $\llbracket \gamma \rrbracket = \text{И}$

Доказательство. Пусть D — все записи из функциональных символов:

$$\llbracket f_0^n \rrbracket^2 \Rightarrow "f_0^n"$$

¹ В исчислении предикатов это верно.

² константа

$$\llbracket f_k^n(\theta_1 \dots \theta_k) \rrbracket \Rightarrow "f_k^n(" + \llbracket \theta_1 \rrbracket " + \dots + " + \llbracket \theta_n \rrbracket + ")"$$

$$\text{Предикатные символы: } \llbracket P(\theta_1 \dots \theta_n) \rrbracket = \begin{cases} \text{И,} & P(\theta_1 \dots \theta_n) \in \Gamma \\ \text{Л,} & \text{иначе} \end{cases}$$

Свободных предметных переменных нет, поэтому для них не нужно придумывать оценку.

Так построенная модель — модель для Γ . Докажем это по индукции по количеству связок: любая формула α , имеющая $\leq n$ связок, истинно $\Leftrightarrow \alpha \in \Gamma$.

База. Очевидно.

Переход. Рассмотрим случай $\alpha \& \beta$.

1. Если $\llbracket \alpha \rrbracket = \text{И}$ и $\llbracket \beta \rrbracket = \text{И}$, то $\alpha \& \beta \in \Gamma$
2. Если $\llbracket \alpha \rrbracket \neq \text{И}$ или $\llbracket \beta \rrbracket \neq \text{И}$, то $\alpha \& \beta \notin \Gamma$

□

Определение. Предварённая нормальная форма — форма, где $\forall \exists \forall \dots (\tau)$, где τ — формула без кванторов.

Теорема 18. Если φ — формула, то существует ψ в предварённой нормальной форме и при этом $\varphi \rightarrow \psi$ и $\psi \rightarrow \varphi$.

Теорема 19 (Гёделя о полноте исчисления предикатов). Если Γ — полное непротиворечивое множество замкнутых формул, то оно имеет модель.

Доказательство. План таков: рассмотрим Γ — полное непротиворечивое множество замкнутых формул. Построим по нему Γ^Δ — п.н.м. бескванторных з.ф. Построим по нему по теореме о существовании модели модель M^Δ и покажем, что M^Δ — модель для Γ :

$$\begin{array}{ccc} \Gamma & & M \\ \text{без кванторов} \downarrow & & \uparrow id \\ \Gamma^\Delta & \xrightarrow{\text{теорема}} & M^\Delta \end{array}$$

Рассмотрим $\Gamma_0 \subset \Gamma_1 \dots \Gamma_i \dots \subset \Gamma^*$ и $\Gamma^* = \bigcup_i \Gamma_i$, а также $\Gamma_0 = \Gamma$, где все формулы в предварённой нормальной форме. Определим переход $\Gamma_i \rightarrow \Gamma_{i+1}$.

Построим семейство функциональных символов d_j^i , которые нигде ранее не использовались.

Рассмотрим случаи того, чем является $\varphi_j \in \Gamma_i$.

1. φ_j без кванторов — не трогаем.

2. $\varphi_j \equiv \forall x.\psi$ — добавим все формулы вида $\psi[x := \theta]$, где θ — терм, составленный из $f, d_0^l, d_1^{l'}, \dots, d_{i-1}^{l' \dots'}$

3. $\varphi_j \equiv \exists x.\psi$ — добавим формулу $\psi[x := d_i^j]$

Таким образом, мы получим $\Gamma_{i+1} = \Gamma_i \cup \{\text{все добавленные формулы}\}$. \square

Следствие 19.1. Пусть $\models \alpha$ и α замкнута, тогда $\vdash \alpha$.

Доказательство. Пусть $\models \alpha$, но не $\not\models \alpha$. Значит, $\{\neg\alpha\}$ — непротиворечивое множество замкнутых формул.

Почему непротиворечиво? $\neg\alpha \vdash \beta \ \& \ \neg\beta, \beta \ \& \ \neg\beta \vdash \alpha$, следовательно $\neg\alpha \vdash \alpha$, но ещё и $\alpha \vdash \alpha$. Таким образом, $\vdash \alpha$.

Значит, у $\neg\alpha$ есть модель M , $\llbracket \neg\alpha \rrbracket_M = \text{И}$. Значит, $\not\models \alpha$ \square

Теорема 20. Если Γ_i непротиворечиво, то Γ_{i+1} непротиворечиво.

Теорема 21. Γ^* непротиворечиво.

$\Gamma^\Delta = \Gamma^*$ без формул с \forall, \exists

Лекция 8

9 апреля

4.7 Теорема Гёделя о полноте исчисления предикатов

Теорема 22. Если φ — замкнутая¹ формула исчисления предикатов, то найдётся ψ — замкнутая формула исчисления предикатов, такая что $\vdash \varphi \rightarrow \psi$ и $\psi \rightarrow \varphi$, при этом ψ с поверхностными кванторами.

Доказательство. В домашних заданиях. □

Рассмотрим Γ — непротиворечивое множество замкнутых формул. Рассмотрим Γ' — полное расширение Γ . Пусть φ — формула из Γ' , тогда найдётся $\psi \in \Gamma'$, что ψ — с поверхностными кванторами и $\vdash \varphi \rightarrow \psi, \vdash \psi \rightarrow \varphi$.

Рассмотрим новое множество констант d_j^i . Построим семейство $\{\Gamma_j\}$: $\Gamma' = \Gamma_0 \subset \Gamma_1 \subset \Gamma_2 \subset \dots \subset \Gamma_j \subset \dots$

Опишем переход $\Gamma_j \Rightarrow \Gamma_{j+1}$.

Рассмотрим все формулы из Γ_j : $\{\gamma_1, \gamma_2, \dots\}$.

1. γ_i — формула без кванторов — оставим как есть.
2. $\gamma_i \equiv \forall x. \varphi$ — добавим в Γ_{j+1} все формулы вида $\varphi[x := \theta]$, где θ составлен из всех функциональных символов исчисления предикатов и констант вида $d_1^k \dots d_j^k$.
3. $\gamma_i \equiv \exists x. \varphi$ — добавим $\varphi[x := d_{j+1}^i]$

Утверждение. Γ_{i+1} непротиворечиво, если Γ_i непротиворечиво.

Доказательство. От противного. Пусть $\Gamma_{i+1} \vdash \beta \ \& \ \neg\beta$

$\Gamma_i, \gamma_1 \dots \gamma_n \vdash \beta \ \& \ \neg\beta, \gamma_i \in \Gamma_{i+1} \setminus \Gamma_i$

¹ Слово “замкнутая” не нужно, но мне нравится — Д.Г.

$$\Gamma_i \vdash \gamma_1 \rightarrow \gamma_2 \rightarrow \dots \rightarrow \gamma_n \rightarrow \beta \ \& \ \neg\beta$$

Докажем, что $\Gamma_i \vdash \beta \ \& \ \neg\beta$ по индукции. $\Gamma_i \vdash \gamma \rightarrow \varepsilon^2$, т.е. γ получен из $\forall x.\xi \in \Gamma_i$ или $\exists x.\xi \in \Gamma_i$

Покажем, что $\Gamma_i \vdash \varepsilon$.

Рассмотрим случай $\forall x.\xi$. Заметим, что $\Gamma_i \vdash \forall x.\xi$, т.к. $\forall x.\xi \in \Gamma_i$. По индукционному предположению $\Gamma_i \vdash \gamma \rightarrow \varepsilon$. $\Gamma_i \vdash (\forall x.\xi) \rightarrow \underbrace{(\xi[x := \theta])}_{\substack{\gamma \text{ по} \\ \text{построению } \Gamma_{i+1}}}$ — по аксиоме 11. Очевидно, что

$(\forall x.\xi) \rightarrow \varepsilon$ и у нас есть гипотеза $\forall x.\xi$, поэтому по М.Р. ε .

В случае $\exists x.\xi$ аналогично доказать не получится. Поэтому мы будем делать странное, без этого в теореме Гёделя никак³.

Рассмотрим $\Gamma_i \vdash \underbrace{\xi[x := d_{i+1}^k]}_{\gamma} \rightarrow \varepsilon$. Заметим, что d_{i+1}^k не входит в ε . Заменим все d_{i+1}^k в

доказательстве на y — новую переменную. Это будет доказательством $\Gamma \vdash \xi[x := y] \rightarrow \varepsilon$. Тогда $\exists y.\xi[x := y] \rightarrow \varepsilon^4$. По ДЗ можно заметить, что $(\exists x.\xi x) \rightarrow (\exists y.\xi[x := y])$ и по лемме $(\exists x.\xi) \rightarrow \varepsilon$ и у нас есть гипотеза $\exists x.\xi$, поэтому по М.Р. ε .

Таким образом, $\Gamma_i \vdash \beta \ \& \ \neg\beta$ — противоречие. \square

$$\Gamma^* := \bigcup_i \Gamma_i$$

Утверждение. Γ^* непротиворечиво.

Доказательство. Предположим обратное: $\Gamma_0 \vdash \gamma_1 \rightarrow \dots \rightarrow \gamma_n \rightarrow \beta \ \& \ \neg\beta$, где $\gamma_i \in \Gamma_i$.

$\Gamma_{\max_i} \vdash \beta \ \& \ \neg\beta$, значит Γ_{\max} противоречиво — противоречие. \square

Пусть Γ^Δ — Γ^* без кванторов. По утверждению у Γ^Δ есть модель M .

Утверждение. Если $\gamma \in \Gamma'$, то $\llbracket \gamma \rrbracket_M = \text{И}$.

Доказательство. Докажем по индукции; база очевидна.

Переход — рассмотрим два случая:

$$1. \ \gamma \equiv \forall x.\delta$$

² что-то

³ Это цитата.

⁴ Правило можно применять, т.к. y не входит в правую часть.

$\llbracket \forall x.\delta \rrbracket = \text{И}$, если $\llbracket \delta \rrbracket^{x:=k} = \text{И}$, $k \in D^5$. Рассмотрим $\llbracket \delta \rrbracket^{x:=k}$, $k \in D$. k осмысленно в некотором Γ_p . δ добавлено на шаге q . Рассмотрим шаг $\Gamma_{\max(p,q)}$. В шаге $\Gamma_{\max(p,q)+1}$ добавлено $\delta[x := k]$. $\delta[x := k]$ меньше на один квантор, чем γ , и соответственно $\llbracket \delta[x := k] \rrbracket = \text{И}$.

2. $\gamma \equiv \exists x.\delta$ — аналогично.

□

4.8 Неразрешимость исчисления предикатов

Теорема 23. Исчисление предикатов неразрешимо.

Определение. Язык — множество слов.

Определение. Язык \mathcal{L} разрешим, если существует алгоритм A такой, что по слову w $A(w)$ останавливается в “1”, если $w \in \mathcal{L}$

Проблема останова: не существует алгоритма, который по программе машины Тьюринга ответит, остановится она или нет. Альтернативная формулировка: пусть \mathcal{L}' — язык всех останавливающихся программ для машин Тьюринга. \mathcal{L}' неразрешим.

Доказательство. Вспомним операцию конкатенации элементов cons.

Пусть A — алфавит ленты⁶. Создадим два набора функциональных нульместных символов: S_x , $x \in A$ и e — nil. Также создадим $c(a, b)$ — двухместный функциональный символ, которому соответствует cons.

Пусть S — множество состояний, тогда b_s , если $s \in S$ — функциональный символ для состояния. b_0 — начальное состояние, b_Δ — допускающее.

Создадим предикат $R(\alpha, w, b_s)$, гласящий, придет ли машина Тьюринга в состояние b_s , при этом слева от головки (*и под ней*) строка α , справа строка w . В частности, $R(\alpha, e, b_0)$ истинно, т.к. это начальное состояние при запуске на строке α .

Машина Тьюринга совершает переходы вида $(s_x, b_s) \rightarrow (s_y b_t, a)$, где a — одно из действий “передвинуться влево”, “перевдвинуться вправо”, “не двигаться”. x — буква на ленте, s — текущее состояние. То же самое, но в терминах предиката :

1. Не двигаться:

$$\forall z.\forall w.R(c(s_x, z), w, b_s) \rightarrow R(c(s_x, z), w, b_t)$$

2. Передвинуться влево:

$$\forall z.\forall w.R(c(s_x, z), w, b_s) \rightarrow R(z, c(s_y, w), b_t)$$

⁵ все записи из функциональных символов

⁶ машины Тьюринга

3. Передвинуться вправо:

$$\forall z. \forall w. R(z, (s_y, w), b_s) \rightarrow R(c(s_y, z), w, b_t)$$

Мы опустили некоторые технические шаги — описать начальное и завершающее состояния.

Взяв & по всем формулам, мы получим некоторую формулу φ . Эта формула описывает машину Тьюринга и из неё выводится завершающее состояние: $\varphi \rightarrow \exists z. \exists w. R(z, w, b_\Delta)$. Таким образом, разрешимость этой формулы эквивалентна разрешимости машины Тьюринга. \square

Лекция 9

16 апреля

5 Теория первого порядка

Это исчисление предикатов + нелогические функциональные предикатные символы + нелогические (*математические*) аксиомы.

- Теория нулевого порядка — без кванторов
- Теория первого порядка — кванторы по предметным переменным
- Теория второго порядка — кванторы по предикатам
- Теория третьего порядка — кванторы по предикатам от предикатов

И так далее. Чем больше порядок, тем о большем количестве вещей мы можем судить. Теория нулевого порядка описывает объекты, первого — множества, второго — множества множеств и т.д.

Теория первого порядка нам нужна, чтобы зафиксировать некоторый набор аксиом. Можно их всегда писать перед “ \vdash ”, но мы не хотим. В какой-то степени это похоже на программы, где мы используем стандартную библиотеку *ИП* и навешиваем свои функции.

5.1 Аксиоматика Пеано

Это первая¹ попытка формализации чисел. Будем говорить, что N соответствует аксиоматике Пеано, если:

1. Задана $(') : N \rightarrow N$ — инъективная функция.
2. Задан $0 \in N$: нет такого $a \in N$, что $a' = 0$

¹ рукомахательная

3. Если $P(x)$ — некоторое утверждение, зависящее от $x \in N$, такое, что $P(0)$ и всегда, когда $P(x)$, также и $P(x')$, тогда $P(x)$. Это свойство индукции.

Примечание. Мы неявно зависим от множества вещей — что такое равенство, что такое утверждение и т.д.

Утверждение. 0 единственный.

Доказательство. Пусть 0 и n нули. Тогда нет $x : x' = 0$ и $x' = n$. Рассмотрим утверждение $P(x) = x = 0$, либо существует $t : t' = x$. Рассмотрим случаи:

1. $P(0) : 0 = 0$ — ок.
2. Пусть $P(x)$ выполнено, докажем $P(x')$. Заметим, что $t = x$.

Таким образом, $P(x)$ при всех $x \in N$. □

Определение.

$$a + b = \begin{cases} a, & b = 0 \\ (a + c)', & b = c' \end{cases}$$

Пример.

$$2 + 2 = 0'' + 0'' = (0'' + 0')' = ((0'' + 0)')' = ((0'')')' = 0''' = 4$$

Определение.

$$a \cdot b = \begin{cases} 0, & b = 0 \\ (a \cdot c) + a, & b = c' \end{cases}$$

$$a^b = \begin{cases} 1, & b = 0 \\ (a^c) \cdot a, & b = c' \end{cases}$$

Утверждение. $a + 0 = 0 + a$

Доказательство. Пусть $P(a) \equiv a + 0 = 0 + a$.

База: $P(0) = 0 + 0 = 0 + 0$

Переход: $P(x) \rightarrow P(x')$

$$0 + x' \stackrel{\text{опр.}}{=} (0 + x)' \stackrel{\text{инд. предп.}}{=} (x + 0)' \stackrel{\text{инд. предп.}}{=} x' + 0$$

□

Утверждение. $a + b' = a' + b$

Доказательство. При $b = 0$:

$$a' + 0 = a' = (a + 0)' = a + 0'$$

При $b = c'$ есть $a + c' = a' + c$. Докажем $a + c'' = a' + c'$

$$(a + c')' = (a' + c)' = a' + c$$

□

Утверждение. $a + b = b + a$

Доказательство. База: $b = 0$ — утверждение 5.1

Переход: $a + c'' = c + a$, если $a + c' = c' + a$

$$a + c'' \stackrel{\text{опр.}}{=} (a + c')' \stackrel{\text{инд. предп.}}{=} (c' + a)' \stackrel{\text{опр.}}{=} c' + a'$$

□

5.2 Формальная арифметика

Рассмотрим следующую теорию первого порядка: исчисление предикатов, в которое добавили следующие символы:

- 0-местный функциональный символ 0
- 1-местный функциональный символ $'$
- 2-местные функциональные символы $(\cdot), (+)$
- 2-местный предикатный символ $(=)$

И добавили следующие 8 аксиом:

1. $a = b \rightarrow a' = b'$
2. $a = b \rightarrow a = c \rightarrow b = c$
3. $a' = b' \rightarrow a = b$
4. $\neg a' = 0$
5. $a + b' = (a + b)'$
6. $a + 0 = a$
7. $a \cdot 0 = 0$
8. $a \cdot b' = a \cdot b + a$

9. Схема аксом индукции:

$$(\psi[x := 0]) \ \& \ (\forall x. \psi \rightarrow (\psi[x := x'])) \rightarrow \psi$$

Если x входит свободно в ψ

Определение. $\exists!x.\varphi(x) \equiv (\exists x.\varphi(x)) \ \& \ \forall p.\forall q.\varphi(p) \ \& \ \varphi(q) \rightarrow p = q$

Определение. $a \leq b$ – сокращение для $\exists n.a + n = b$

Определение.

$$0^{(n)} = \begin{cases} 0, & n = 0 \\ 0^{(n-1)'}, & n > 0 \end{cases}$$

$$\bar{n} = 0^{(n)}$$

Определение. Пусть $W \subset \mathbb{N}_0^n$. W – **выразимое в формальной арифметике отношение, если:** (пусть $k_1 \dots k_n \in \mathbb{N}$)

1. $(k_1 \dots k_n) \in W$, тогда $\vdash w[x_1 := \bar{k}_1 \dots x_n := \bar{k}_n]$
2. $(k_1 \dots k_n) \notin W$, тогда $\vdash \neg w[x_1 := \bar{k}_1 \dots x_n := \bar{k}_n]$

Определение. $f : \mathbb{N}^n \rightarrow \mathbb{N}$ **представима в формальной арифметике**, если найдётся φ – формула с $n + 1$ свободной переменной $k_1 \dots k_{n+1} \in \mathbb{N}$

1. $f(k_1 \dots k_n) = k_{n+1}$, то $\vdash \varphi(\bar{k}_1 \dots \bar{k}_{n+1})$
2. $\vdash \exists!x.\varphi(k_1 \dots k_n, x)$

Лекция 10

30 апреля

6 Арифметизация математики

Это идея того, все содержательное в математике может быть выражено как арифметика. Мы к ней подойдём издалека

6.1 Рекурсивные функции

Рассмотрим следующие примитивы, чтобы определить рекурсивные функции:

1. $Z : \mathbb{N} \rightarrow \mathbb{N} : Z(x) = 0$
2. $N : \mathbb{N} \rightarrow \mathbb{N} : N(x) = x + 1$
3. $S_k : \mathbb{N}^m \rightarrow \mathbb{N}$ — подстановка

$$S_k \langle g, f_1 \dots f_k \rangle (x_1 \dots x_m) = g(f_1(\bar{x}), f_2(\bar{x}) \dots f_k(\bar{x}))$$

, где $\bar{x} \equiv x_1 \dots x_m$ и если $f_1 \dots f_k : \mathbb{N}^m \rightarrow \mathbb{N}$ и $g : \mathbb{N}^k \rightarrow \mathbb{N}$

4. $P_k^l : \mathbb{N}^k \rightarrow \mathbb{N} : P_k^l(x_1 \dots x_k) = x_l$ при $l \leq k$ — проекция
5. $R \langle f, g \rangle : \mathbb{N}^{m+1} \rightarrow \mathbb{N}$, если $f : \mathbb{N}^m \rightarrow \mathbb{N}, g : \mathbb{N}^{m+2} \rightarrow \mathbb{N}$

$$R \langle f, g \rangle (y, x_1 \dots x_m) = \begin{cases} f(x_1 \dots x_m), & y = 0 \\ g(y - 1, R \langle f, g \rangle (y - 1, x_1 \dots x_m), x_1 \dots x_m), & y > 0 \end{cases}$$

R называется **примитивной рекурсией**.

R можно воспринимать как цикл for с переменной цикла y .

Пример.

$$(a) R \langle f, g \rangle x = f(x)$$

$$(b) R \langle f, g \rangle x = g(0, f(x), x)$$

$$(c) R \langle f, g \rangle x = g(1, g(0, f(x), x), x)$$

Определение. $f : \mathbb{N}^m \rightarrow \mathbb{N}$ — **примитивно-рекурсивная**, если найдётся выражение f через примитивы Z, N, S, P, R .

Пример.

$$1. 1(x) = 1$$

$$1 = S \langle N, Z \rangle$$

$$2. (+2)(x) = x + 2$$

$$(+2) = S \langle N, N \rangle$$

$$S \langle N, N \rangle (x) = g(f(x)) = N(N(x)) = x + 2$$

$$3.$$

$$(+3) = S \langle N, S \langle N, N \rangle \rangle$$

$$4. (\times 2)$$

Промежуточная функция:

$$(\times 2_a) = R \langle P_1^1, S \langle N, P_3^2 \rangle \rangle$$

$$(\times 2) = S \langle (\times 2_a), P_1^1, P_1^1 \rangle$$

Добавим новый примитив “минимизация”:

$$6. M \langle f \rangle : \mathbb{N}^m \rightarrow \mathbb{N} \text{ при } f : \mathbb{N}^{m+1} \rightarrow \mathbb{N}$$

$M \langle f \rangle (x_1 \dots x_m) = y$ — минимальный y такой, что $f(y, x_1 \dots x_m) = 0$. Если $f(y, x_1 \dots x_m) > 0$ при всех y , результат неопределён.

Теорема 24. $(+), (\cdot), (x^y), (:), (\sqrt{\cdot})$, деление с остатком, числа Фибоначчи — примитивно-рекурсивные функции.

Пусть $p_1, p_2 \dots$ — простые числа.

Утверждение. $p(i) : \mathbb{N} \rightarrow \mathbb{N}, p(i) = p_i$ — примитивно-рекурсивная функция.

$2^{k_1} \cdot 3^{k_2} \cdot 5^{k_3} \cdot \dots \cdot p_i^{k_i}$ — примитивно-рекурсивно

$$\text{plog}_n k = \max t : k \equiv 0 \pmod{n^t}$$

Пример.

$$1. \text{plog}_5 120 = 1$$

$$2. \text{plog}_2 120 = 3$$

$\text{plog}_k p$ — примитивно-рекурсивная функция.

Тогда мы можем кодировать $\langle k_1 \dots k_n \rangle$ как $2^{k_1} \cdot 3^{k_2} \cdot 5^{k_3} \cdot \dots \cdot p_i^{k_i}$ и перевод в любую сторону примитивно-рекурсивен. С помощью такого подхода проще создавать примитивно-рекурсивные функции.

Определение (Функция Аккермана).

$$A(m, n) = \begin{cases} n + 1, & m = 0 \\ A(m - 1, 1), & m > 0, n = 0 \\ A(m - 1, A(m, n - 1)), & m > 0, n > 0 \end{cases}$$

Утверждение. $A(m, n)$ не примитивно-рекурсивно.

Доказательство. Общая идея: если некоторый текст длины n задал число k , то добавление одного символа не позволяет получить число больше, чем k^k , т.к. R не может совершить больше R итераций. \square

Теорема 25. f — рекурсивная функция. Тогда f представима в формальной арифметике.

Теорема 26. f представима в формальной арифметике. Тогда f рекурсивна.

Доказательство. Пусть $\vdash \varphi$ и $\delta_1 \dots \delta_n \equiv \varphi$ — доказательство φ в формальной арифметике.

Пусть C — рекурсивная функция, проверяющая доказательство в формальной арифметике, т.е. $C(p, x) = \begin{cases} 0, & \text{доказательство корректно} \\ \neq 0, & \text{доказательство некорректно} \end{cases}$, где x — запись доказательства формулы p .

По теореме 25 получим формулу σ , для которой верно $\vdash \sigma(p, x, 0)$, если p — доказательство формулы x . \square

6.2 Проблема останова

Пусть есть программа $P(p, x) = \begin{cases} 0, & \text{если } p(x) \text{ останавливается} \\ 1, & \text{если } p(x) \text{ не останавливается} \end{cases}$

Рассмотрим программу Q :

```

Q(p)
  if P(p) = 1
    return 0
  else
    while true do;

```

Чему равно $Q(Q)$? Ни 0, ни 1. Это противоречие.

Мы аналогичным образом ломаем наше доказательство — создадим формулу “для меня нет доказательства”.

Теорема 25.А. Примитивы Z, N, S, P представимы в формальной арифметике.

Доказательство.

1. $Z : \xi := x_1 = x_1 \ \& \ x_2 = 0$
2. $N : \nu := x_2 = x'_1$
3. $P_k^l : \pi_k^l := x_1 = x_1 \ \& \ x_2 = x_2 \ \& \ \dots \ \& \ x_l = x_{k+1} \ \& \ \dots \ \& \ x_k = x_k$
4. $S \langle g, f_1 \dots f_k \rangle : g \leftrightarrow \gamma, f_i \leftrightarrow \varphi_i.$

$$\exists r_1. \exists r_2. \dots \exists r_k. \varphi_1(x_1 \dots x_m, r_1) \ \& \ \varphi_2(x_1 \dots x_m, r_2) \ \& \ \dots \ \& \ \varphi_k(x_1 \dots x_m, r_k) \ \& \ \gamma(r_1 \dots r_k, x_{m+1})$$

6. $M \langle f \rangle$

$$\varphi(x_{m+1}, x_1 \dots x_m, \bar{0}) \ \& \ \forall y. y < x_{m+1} \rightarrow \neg \varphi(y, x_1 \dots x_m, \bar{0})$$

5. β -функция Гёделя:

$$\beta(b, c, i) = b \% (1 + c \cdot (i + 1))$$

Теорема 25.В. $a_0 \dots a_n$ — некоторые значения $\in \mathbb{N}$. Тогда найдутся b с такие, что $\beta(b, c, i) = a_i$

Доказательство.

Утверждение. Если $i \neq j$, то $1 + c(i + 1)$ взаимно просто с $1 + c(j + 1)$.

Доказательство. $c := \max(a_0 \dots a_n, n)!$.

Пусть есть некоторый простой p : $1 + c(i + 1) \equiv 0 \pmod p$ и $1 + c(j + 1) \equiv 0 \pmod p$. Тогда $c(i + 1 - j - 1) \equiv 0 \pmod p$ и $c(i - j) \equiv 0 \pmod p$ — противоречие. \square

Утверждение. По китайской теореме об остатках найдётся b с нужными свойствами. \square

β примитивно-рекурсивна и представима в формальной арифметике:

$$B(b, c, i, q) = (\exists p. b = p \cdot (1 + c \cdot (1 + i)) + q) \ \& \ q < b$$

Тогда для $R \langle f, g \rangle$, если $f \leftrightarrow \varphi, g \leftrightarrow \gamma$:

$$\begin{aligned} \exists b. \exists c. \exists f. \varphi(x_1 \dots x_n, f) \ \& \ B(b, c, \bar{0}, f) \ \& \ \forall y. y < x_{n+1} \rightarrow \exists r_{y-1}. B(b, c, y-1, r_{y-1}) \\ \ \& \ \exists r_{y+1}. B(b, c, y+1, r_{y+1}) \ \& \ \varphi(y, r_y, x_1 \dots x_n, r_{y+1}) \\ \ \& \ B(b, c, x_{n+1}, x_{n+2}) \end{aligned}$$

□

Лекция 11

7 мая

7 Гёделева нумерация

Это кодировка для строк.

Определение ($\ulcorner \urcorner$).

x	$\ulcorner x \urcorner$
(3
)	5
,	7
&	9
\vee	11
\neg	13
\rightarrow	15
\forall	17
\exists	19
.	21
f_n^k	$23 + 6 \cdot 2^n \cdot 3^k$
P_n^k	$25 + 6 \cdot 2^n \cdot 3^k$
x_k	$27 + 6 \cdot 2^k$

Пример. Для формальной арифметики: $(=) = P_0^2$, $(0) = f_0^0$, $(') = f_0^1$, $(+) = f_0^2$, $(\cdot) = f_1^2$

Определение. $\ulcorner a_0 a_1 \dots a_{n-1} \urcorner = 2^{\ulcorner a_0 \urcorner} \cdot 3^{\ulcorner a_1 \urcorner} \dots p_n^{\ulcorner a_{n-1} \urcorner}$, где p_i — i -тое простое число.

Определение. $\ulcorner S_0 \dots S_n \urcorner = 2^{\ulcorner S_0 \urcorner} \dots p_n^{\ulcorner S_{n-1} \urcorner}$, где S_i — некоторая строка.

Несложно заметить, что символы всегда нечетные, а строки всегда чётные, что упрощает жизнь. Это не содержательно и сделано только для удобства вычисления “руками”, т.к. это было сделано до компьютеров.

Таким образом, мы можем взять любую формулу или доказательство и закодировать.

Пример. $\ulcorner a = 0 \urcorner = 2^{27+6} \cdot 3^{25+6 \cdot 4} \cdot 5^{23+6}$

Теорема 27. Рассмотрим функцию

$$Proof(\underbrace{x}_{\ulcorner \chi \urcorner}, p) = \begin{cases} 0, & \text{если } p \text{ — гёделев номер доказательства } \chi \\ 1, & \text{иначе} \end{cases}$$

Proof рекурсивна.

Теорема 28. Если функция представима в формальной арифметике, то она рекурсивна.

Доказательство. Рассмотрим $f : \mathbb{N} \rightarrow \mathbb{N}$, представимую в формальной арифметике. Тогда существует φ с $n + 1$ свободной переменной $(x_1 \dots x_{n+1})$ ¹.

Если $f(k_1 \dots k_n) = k_{n+1}$, то $\vdash \varphi(\overline{k_1} \dots \overline{k_{n+1}})$, т.е. существует доказательство $\delta = \delta_1 \dots \delta_t$.

$$Proof(\ulcorner \varphi(\overline{k_1} \dots \overline{k_{n+1}}) \urcorner, \ulcorner \delta \urcorner) = 0$$

Найдём δ и $\overline{k_{n+1}}$. Переберем y и будем подставлять $\text{plog}_2 y$ вместо $\overline{k_{n+1}}$ и $\text{plog}_3 y$ вместо δ . Таким образом, мы переберем все возможные комбинации:

$$S \langle \text{plog}_2, M \langle S \langle Proof, S \langle Subst_{n+1}, \ulcorner \varphi \urcorner, P_{n+1}^2, P_{n+1}^3 \dots P_{n+1}^{n+1}, S \langle \text{plog}_2, P_{n+1}^1 \rangle \rangle, S \langle \text{plog}_3, P_{n+1}^1 \rangle \rangle \rangle \rangle$$

- $S \langle \text{plog}_2, P_{n+2}^1 \rangle$ — то же самое, что и $\text{plog}_2 y$.
- $Subst_i$ берёт i -тый аргумент x_i и заменяет все вхождения x_i в во всех аргументах, кроме последнего, на значение последнего аргумента.

Объяснение: M найдёт минимальное² y , такое что при вышеуказанной подстановке $Proof = 0$. Т.к. нам нужно получить k_{n+1} , то мы берём plog_2 . \square

7.1 Самоприменение

Определение. $W_1(\ulcorner \chi \urcorner, \ulcorner p \urcorner) = 0$ тогда и только тогда, когда p — доказательство самоприменения χ , т.е. доказательство $\chi[x_0 := \ulcorner \chi \urcorner]$; иначе $W_1 = 1$.

¹ и т.д., см. определение представимой в формальной арифметике функции

² что нам не нужно, но пусть будет

Представление W_1 в формальной арифметике через $Subst$ очевидно, обозначим его ω_1 .

Формула $\sigma(x) = \forall p. \neg \omega_1(x, p)$ утверждает “самоприменение x недоказуемо”. Доказуемо ли $\sigma(\overline{\sigma})$?

Примечание. Эта тема несколько архаична.

Определение. Теория ω -непротиворечива, если для любой $\varphi(x)$: если $\vdash \varphi(\bar{0}), \vdash \varphi(\bar{1}) \dots$, то $\nvdash \exists x. \neg \varphi(x)$

Теорема 29. Если теория ω -непротиворечива, то она непротиворечива.

Доказательство. Рассмотрим $\varphi(x) := x = x$. Т.к. $\vdash \bar{0} = \bar{0}, \vdash \bar{1} = \bar{1} \dots$, то по ω -непротиворечивости $\nvdash \exists x. \neg(x = x)$. \square

Теорема 30 (Гёделя о неполноте арифметики №1).

1. Если формальная арифметика непротиворечива, то $\nvdash \sigma(\overline{\sigma})$
2. Если формальная арифметика ω -непротиворечива, то $\nvdash \neg \sigma(\overline{\sigma})$

Доказательство.

1. Пусть $\vdash \sigma(\overline{\sigma})$, т.е. существует p — гёделев номер доказательства $\vdash \sigma(\overline{\sigma})$. Тогда $\vdash \forall p. \neg \omega_1(\overline{\sigma}, p)$. С другой стороны, $W_1(\overline{\sigma}, p) = 0$, т.е. $\vdash \omega_1(\overline{\sigma}, \bar{p})$ — противоречие.
2. Пусть $\vdash \neg \sigma(\overline{\sigma})$. Тогда $\vdash \exists p. \omega_1(\overline{\sigma}, p)$, но при этом $\vdash \neg \omega_1(\overline{\sigma}, \bar{0})$ и то же самое для любого числа, т.к. иначе $\vdash \sigma(\overline{\sigma})$ и получается противоречие.

Но по ω -непротиворечивости $\vdash \sigma(\overline{\sigma})$ — противоречие.

\square

Следствие 30.1. Формальная арифметика со стандартной интерпретацией неполна.

Доказательство. По определению $\vdash \omega_1(x, p)$ тогда и только тогда, когда p — доказательство $x(x)$. Ясно, что $\nvdash \omega_1(\overline{\sigma}, p)$ для любого p . Тогда $\llbracket \omega_1(\overline{\sigma}, p) \rrbracket = \text{Л}$, следовательно $\llbracket \forall p. \neg \omega_1(\overline{\sigma}, p) \rrbracket = \text{И}$. Но $\nvdash \sigma(\overline{\sigma})$ — противоречие. \square

Есть формулировка этой теоремы без ω -непротиворечивости.

Теорема 31 (Гёделя о неполноте арифметики №1 в форме Россера).

$$W_2(x, p) = \begin{cases} 0, & p \text{ — доказательство } \neg x(\ulcorner x \urcorner) \\ 1, & \text{иначе} \end{cases}$$

$$\rho(x) = \forall p. \omega_1(x, p) \rightarrow \exists q. q < p \ \& \ \omega_2(x, q)$$

То есть ρ гласит, что если мы найдём доказательство самоприменения x , то мы найдём доказательство отрицания самоприменения x , при этом данное доказательство будет иметь меньший номер.

1. Если формальная арифметика непротиворечива, то $\not\vdash \rho(\overline{\rho})$
2. Если формальная арифметика непротиворечива, то $\not\vdash \neg\rho(\overline{\rho})$

Примечание. Эта теорема формализована на Coq в 18 тысяч строк.

Определение. $Consis \equiv \forall p. \neg \pi(\overline{1 = 0}, p)$, где π есть арифметизированное *Proof*. Неформально *Consis* эквивалентно тому, что арифметика непротиворечива.

Теорема 32 (Гёделя о неполноте арифметики №2). $\vdash Consis \rightarrow \sigma(\overline{\sigma})$

Примечание. Теорема гласит, что если доказать *Consis*, то докажется $\sigma(\overline{\sigma})$, из чего следует противоречивость формальной арифметики. Следовательно, внутри Ф.А. доказать непротиворечивость Ф.А. невозможно.

Доказательство. Полного доказательства не будет, оно убийственное³.

Если вдуматься, то доказывать нечего, т.к. теорема гласит, что если формальная арифметика непротиворечива, то не существует доказательства самоприменения σ , т.е. $\forall p. \neg \omega_1(\overline{\sigma}, p)$. Таким образом, это просто первый пункт теоремы [Гёделя о неполноте арифметики №1](#), но формализованный. \square

³ Это цитата.

Лекция 12

14 мая

8 Теория множеств

Примечание. Обычно фокус в курсе матлогики делается именно на теории множеств, т.к. она более полезна для математики.

Определение. Теория множеств — теория первого порядка с нелогическим предикатом “принадлежность” (\in) и нижеуказанными схемами аксиом.

Определение. $a \subseteq b$, если $\forall x. x \in a \rightarrow x \in b$

Примечание. Моделью для теории множеств является конструкция в стиле алгебры Линденбаума.

Определение (пара).

$$\begin{aligned}\langle a, b \rangle &= \{\{a\}, \{a, b\}\} \\fst \langle a, b \rangle &= \bigcup \left(\bigcap \langle a, b \rangle \right) \\snd \langle a, b \rangle &= \bigcup \left(\bigcup \langle a, b \rangle \setminus \bigcap \langle a, b \rangle \right)\end{aligned}$$

Определение. $B \subseteq X^2$ — бинарное отношение на X .

Что такое равенство?

- Принцип Лейбница (*неразличимость*): $A = B$, если для любого “предиката”¹ P выполнено $P(A) \leftrightarrow P(B)$
- Принцип объёмности: A и B состоит из одинаковых элементов.

Сокращение: $a \leftrightarrow b$, если $(a \rightarrow b) \ \& \ (b \rightarrow a)$

¹ Множество $\{x \mid P(x)\}$

Определение. $a = b$, если $a \subseteq b$ & $b \subseteq a$

Примечание. То есть мы используем принцип объемности. Из него следует принцип Лейбница.

Аксиома 1 (равенства). Равные множества содержатся в одних и тех же множествах.

$$\forall abc. a = b \ \& \ a \in c \rightarrow b \in c$$

Аксиома 2 (пустого множества). Существует $\emptyset : \forall x. \neg x \in \emptyset$

Примечание. Также можно определить пустое множество как константу теории.

Аксиома 3 (пары). Если $a \neq b$, то $\{a, b\}$ — множество.

В формальном виде:

$$\forall a. \forall b. a \neq b \rightarrow \exists p. a \in p \ \& \ b \in p \ \& \ \forall t. t \in p \rightarrow t = a \vee t = b$$

Примечание. Иначе мы можем получать нечто похожее на открытые множества в топологии стрелки, где у нас нет конечного множества, содержащего некоторый элемент.

Аксиома 4 (объединения). Если x — непустое множество, то $y = \bigcup x$ — множество.

В формальном виде:

$$\forall x. \underbrace{\exists (y. y \in x)}_{x \text{ непустое}} \rightarrow \exists p. \forall y. y \in p \leftrightarrow \exists s. y \in s \ \& \ s \in x$$

Аксиома 5 (степени). Для множества x существует $\mathcal{P}(x)$ — множество всех подмножеств.

В формальном виде:

$$\forall x. \exists p. \forall y. y \in p \leftrightarrow y \subseteq x$$

Пример.

$$\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$

Аксиома 6 (схема выделения). Если a — множество, $\varphi(x)$ — формула, в которую не входит свободно b , то $\{x \mid x \in a \ \& \ \varphi(x)\}$ — множество.

В формальном виде:

$$\forall x. \exists b. \forall y. y \in b \leftrightarrow y \in x \ \& \ \varphi(y)$$

Примечание. Это схема аксиомы, т.к. здесь присутствует метаварiable φ .

Аксиома 7 (бесконечности). Существует множество N такое, что:

$$\emptyset \in N \ \& \ \forall x. x \in N \rightarrow x \cup \{x\} \in N$$

Теорема 33. Если x — множество, то $\{x\}$ — множество, т.е. $\exists t. a \in t \leftrightarrow a = x$

Доказательство. Рассмотрим случаи:

1. $x = \emptyset$. Тогда $t = \mathcal{P}(x)$.
2. $x \neq \emptyset$. Тогда $s = \{x, \emptyset\}$ — существует по аксиоме пары, $t = \{z \mid z \in s \ \& \ z \neq \emptyset\}$.

□

Теорема 34. Если a, b — множества, то $a \cup b$ — множество.

Доказательство. Рассмотрим случаи:

1. $a = b$. Тогда $a \cup b = a$
2. $a \neq b$. Тогда $a \cup b = \{a, b\}$ — существует по аксиоме [пары](#)

□

Обозначение. a, b — множества. Тогда $a \cup b$ — такое c , что:

$$a \subseteq c \ \& \ b \subseteq c \ \& \ \forall t. t \in c \rightarrow t \in a \vee t \in b$$

Определение. $a' = a \cup \{a\}$

Обозначение (ординальные числа).

- $\bar{0} = \emptyset$
- $\bar{1} = \emptyset' = \{\emptyset\}$
- $\bar{2} = \emptyset'' = \{\emptyset, \{\emptyset\}\}$
- $\bar{3} = \emptyset''' = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$

Определение. Множество S **транзитивно**, если:

$$\forall a. \forall b. a \in b \ \& \ b \in S \rightarrow a \in S$$

Определение. Множество s **вполне упорядочено** отношением “ \in ”, если:

1. $\forall a. \forall b. a \in s \ \& \ b \in s \rightarrow a \in b \vee b \in a \vee a = b$ — линейность
2. $\forall t. t \subseteq s \rightarrow \exists a. a \in t \ \& \ \forall b. b \in t \rightarrow b = a \vee a \in b$ — в любом подмножестве есть наименьший элемент

Определение. **Ординал** — вполне упорядоченное отношением “ \in ” транзитивное множество.

Определение. Предельный ординал — непустой ординал, не имеющий предшественника:

$$\forall p. p' \neq s$$

Пример.

$$\omega = \{\emptyset, 1, 2, \dots\}$$

Очевидно, что $\omega \subseteq N$

Теорема 35. ω — множество.

Определение.

$$a + b = \begin{cases} a, & b = 0 \\ (a + c)', & b = c' \\ \sup_{c \in b} (a + c), & b - \text{предельный} \end{cases}$$

Определение. $\sup t$ — минимальный ординал, содержащий все элементы t .

Пример. $a = \{0, 1, 3\}$ — не ординал, т.к. транзитивность не выполнена, т.к. $2 \in 3$, но $2 \notin a$.
 $\sup\{0, 1, 3\} = \{0, 1, 2, 3\}$

Пример.

$$1 + \omega = \sup_{c \in \omega} (1 + c) = \sup\{0 + 1, 1 + 1, \dots\} = \sup\{1, 2, \dots\} = \omega$$

Пример.

$$\omega + 1 = \omega' = \{0, 1, 2, \dots, \omega\}$$

Лекция 13

21 мая

8.1 Аксиома выбора

Аксиома 8. Эквивалентны следующие формулировки:

- На любом семействе¹ непустых множеств $\{A_S\}_{S \in \mathbb{S}}$ можно определить функцию $f : \mathbb{S} \rightarrow \bigcup_S A_S$, которая по множеству возвращает его элемент.
- Любое множество можно вполне упорядочить.
- Для любой сюръективной функции $f : A \rightarrow B$ найдётся частично обратная $g : B \rightarrow A$, т.е. $g(f(x)) = x$.

Примечание. Эта аксиома странная, т.к. по третьей формулировке любую хеш-функцию можно сломать. Конечно, они все ломаются перебором, но это не относится к реальному миру.

Примечание. Эта аксиома не конструктивна — сказано, что можно построить функцию/-порядок, но не сказано, как.

Примечание. Аксиома выбора не даёт парадоксов.

Примечание. Можно рассматривать теорию множеств без этой аксиомы, она тоже часто используется и обозначается \mathbf{ZF}^2 , а с аксиомой выбора обозначается \mathbf{ZFC}^3 .

Определение. Дизъюнктное семейство множеств — семейство непересекающихся подмножеств.⁴

$$D(y) : \forall p. \forall q. p \in y \ \& \ q \in y \rightarrow p \cap q = \emptyset$$

¹ Это синоним слову “множество”.

² Zermelo–Fraenkel

³ Zermelo–Fraenkel–Choice

⁴ Кажется, в формализации ошибка, т.к. если $p = q$, то всё ломается. Нужно в конец добавить $\vee p = q$.

Определение (прямое произведение дизъюнктного множества).

$$\times S = \{t \mid \forall p. p \in S \leftrightarrow \exists! c. c \in p \ \& \ c \in t\}$$

Формулировка аксиомы выбора, которую мы будем использовать:

Аксиома (выбора). Если $D(y) \ \& \ \forall t. t \in y \rightarrow t \neq \emptyset$, то $\times y \neq \emptyset$

Примечание. В матанализе аксиома выбора используется для эквивалентности предела по Коши и по Гейне.

Теорема 36 (Диаконеску). Рассмотрим ZF поверх ИИП⁵. Если добавить аксиому выбора, то $\vdash \alpha \vee \neg \alpha$.

Аксиома 9 (фундирования).

$$\forall x. x = \emptyset \vee \exists y. y \in x \ \& \ y \cap x = \emptyset$$

Иными словами, в каждом непустом множестве есть элемент, не пересекающийся с ним.

Примечание. Эта аксиома запрещает самосодержащие множества.

Примечание. Без аксиомы **фундирования** нельзя определить $\{a, \{a, b\}\}$ как пару, но можно $\{\{a\}, \{a, b\}\}$.

Аксиома 10 (схема подстановки, Френкеля). Если S — множество, f — функция, т.е. существует формула $\varphi(x, y) : \forall x \in S. \exists! y. \varphi(x, y)$, то $f(S)$ — множество.

8.2 Мощность множеств

Определение. Множества a и b **равномощны**, если существует биекция $a \rightarrow b$ и обозначается $|a| = |b|$.

Определение. Кардинальное число t — ординал x , такой что для всех $y \in x$ $|y| \neq |x|$

Определение. **Мощность** $|x|$ — такое кардинальное число t , что $|t| = |x|$.

Определение (строго большая мощность). $|a| < |b|$, если существует $f : a \rightarrow b$ — инъективно, но нет биекции.

Утверждение. Если a, b — кардиналы и $|a| = |b|$, то $a = b$.

- $\bar{0}, \bar{1}, \dots$ — конечные кардиналы.
- $\aleph_0 = |\omega|$
- \aleph_1 — следующий кардинал за \aleph_0 .
- \vdots

⁵ а не КИП

Пример. $|\omega| = |\omega + 1|$, следовательно $|\omega + 1|$ не кардинал, т.к. $\omega \in \omega + 1$.

Теорема 37 (Кантора). Рассмотрим множество S и $\mathcal{P}(S)$. Тогда $|\mathcal{P}(S)| > |S|$

Доказательство. Пусть $f : S \rightarrow \mathcal{P}(S)$ — биекция. Построим $x \in \mathcal{P}(S)$, не имеющий прообраза. Это можно сделать диагональным методом: $t = \{s_k \in S \mid s_k \notin f(s_k)\}$. \square

Напоминание: \aleph_1 — наименьший кардинал такой, что $\aleph_1 > \aleph_0$. Существует ли он? Да, т.к. $|\mathcal{P}(\aleph_0)| > \aleph_0$ по теореме Кантора.

Является ли $\aleph_1 = \mathcal{P}(\aleph_0)$? Это континуум-гипотеза, и её отрицание нельзя доказать.

Теорема 38 (Кантора-Бернштейна). Если a, b — множества, $f : a \rightarrow b$ и $g : b \rightarrow a$ инъективны, то существует биекция $a \rightarrow b$.