

Математическая логика

Михайлов Максим

22 февраля 2021 г.

Оглавление

Лекция 1	12 февраля	2
0.	Мотивация	2
0.1.	Математикам	2
0.2.	Программистам	3
1.	Исчисление высказываний	3
1.1.	Язык	3
1.2.	Метаязык и предметный язык	3
1.3.	Сокращения записи	4
1.4.	Теория моделей	4
1.5.	Теория доказательств	5
1.6.	Правило Modus Ponens и доказательство	5
Лекция 2	19 февраля	6
2.	Интуиционистская логика	9
2.1.	ВНК-интерпретация	9

Лекция 1

12 февраля

0. Мотивация

0.1. Математикам

Аксиома 1 (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 истинных 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, $\not\equiv \alpha$

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 $\alpha \rightarrow \sigma_l$

$n + 0.2$ $(\alpha \rightarrow \sigma_l) \rightarrow (\alpha \rightarrow (\sigma_l \rightarrow \sigma_{n+1})) \rightarrow (\alpha \rightarrow \sigma_{n+1})$ (аксиома 2)

$n + 0.4$ $(\alpha \rightarrow \sigma_l \rightarrow \sigma_{n+1}) \rightarrow (\sigma \rightarrow \sigma_{n+1})$ (М.Р. $n + 2, l$)

$n + 1$ $\alpha \rightarrow \sigma_{n+1}$ (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:

$\llbracket \delta_k \rrbracket$	$\llbracket \delta_{n+1} \rrbracket$	$\llbracket \delta_k \rrbracket = \llbracket \delta_l \rrbracket \rightarrow \delta_{n+1} \rrbracket$
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 $\Pi \vdash _{[\eta * \zeta]} \eta * \zeta$, где $*$ — все связки

Это упражнение.

□

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

Доказательство. Было в ДЗ.

□

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 $_{[x_1]}P_1 \dots _{[x_n]}P_n \vdash \alpha$, 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

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:

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