Математическая логика

Михайлов Максим

4 марта 2021 г.

Оглавление

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, $\lim\limits_{x \to +\infty} \frac{1}{x} = 0 = \lim\limits_{x \to +\infty} \frac{1}{x^2}$, 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 $(\alpha \to \beta), (\alpha \,\&\, \beta), (\alpha \vee \beta), (\neg\alpha)$ — 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. $\alpha \to \beta$ — метавыражение; $A \to (A \to A)$ — предметное выражение.

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

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

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

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

Соглашение. символы логических операций не пишутся в метаязыке.

Пример.

$$(\alpha \to (A \to X))[\alpha := A, X := B] \equiv A \to (A \to B)$$
$$(\alpha \to (A \to X))[\alpha := (A \to P), X := B] \equiv (A \to P) \to (A \to B)$$

1.3. Сокращения записи

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

Примечание. Здесь операторы записаны в порядке их приоритета

Пример. Расставим скобки в следующем выражении:

$$A \to B \,\&\, C \to D$$

$$A \to ((B \,\&\, C) \to D)$$

1.4. Теория моделей

Модель состоит из:

Обозначение.

- P — некоторое множество предметных переменных
- τ — множество высказываний предметного языка
- V — множество истинных значений. Классическое — $\{\text{И}, \text{Л}\}$
- $[\![\ ]\!] : \tau \to V$ — оценка высказывания *(высказывание ставится в скобки).*

1. $[\![x]\!] : P \to V$ — задается при оценке.
2. $[\![\alpha \star \beta]\!] = [\![\alpha]\!] \star [\![\beta]\!]$, где $\star$ есть логическая операция ($\vee, \&, \neg, \to$), а $\star$ определено естественным образом как элемент метаязыка.

1.5. Теория доказательств

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

Пример.

$$(\alpha \to (\beta \to (A \to \alpha)))$$

10 схем аксиом:

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

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 $\exists k, l < i : \alpha_k \equiv \alpha_l \to \alpha_i$ *(правило Modus Ponens)*

Пример. $\vdash A \to A$

1.	$A \to A \to A$	сх. акс. 1
2.	$A \to (A \to A) \to A$	сх. акс. 1
3.	$(A \to (A \to A)) \to (A \to (A \to A) \to A) \to (A \to A)$	сх. акс. 2
4.	$(A \to (A \to A) \to A) \to (A \to A)$	M.P. 1, 3
5.	$A \to A$	M.P. 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 $[\![\gamma_i]\!] =$ И, то $[\![\alpha]\!] =$ И.

Пример. $\models \alpha$ — α 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).

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

Доказательство.

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

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

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

  Но эту последовательность можно дополнить до доказательства, так что каждый σ_i есть аксиома, гипотеза или получается через M.P. 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.

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

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

   $n + 1$ $\quad \alpha \to \delta_{n+1}$ (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 $\alpha \to \alpha$

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

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

   l $\quad \alpha \to \sigma_l$

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

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

   $n + 1$ $\quad \alpha \to \sigma_{n+1}$ (М.Р. $n + 0.4, k$)

□

□

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

Доказательство. Индукция по длине доказательства: каждая $[\![\delta_i]\!] =$ И, если $\delta_1 \dots \delta_n$ — доказательство α

Рассмотрим n и пусть $[\![\delta_1]\!] =$ И, $\dots$ $[\![\delta_n]\!] =$ И.

Тогда рассмотрим основание δ_{n+1}

1. δ_{n+1} — аксиома. Это упражнение.

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

$$\lhd [\![\alpha \to \beta \to \alpha]\!]^{[\![\alpha]\!]:=a, [\![\beta]\!]:=b} = \text{И}$$

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

Аналогично можно доказать для остальных аксиом.

2. δ_{n+1} — М.Р. $\delta_k = \delta_l \to \delta_{n+1}$

   Фиксируем оценку. Тогда $[\![\delta_k]\!] = [\![\delta_l]\!] =$ И. Тогда:

$[\![\delta_k]\!]$	$[\![\delta_{n+1}]\!]$	$[\![\delta_k]\!] = [\![\delta_l \to \delta_{n+1}]\!]$
Л	Л	И
Л	И	И
И	Л	Л
И	И	И

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

□

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

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

Рассмотрим $[\![\alpha]\!]^{P_1 := x_1 \dots P_n := x_n} =$ И

Обозначение. $_{[\beta]}\alpha \equiv \begin{cases} \alpha, & [\![\beta]\!] = \text{И} \\ \neg\alpha, & [\![\beta]\!] = \text{Л} \end{cases}$ 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 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 $[\![\alpha]\!] = \text{И}$ 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 ${}_{[x_1]}P_1 \dots {}_{[x_{n-1}]}P_{n-1} \vdash \alpha$

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

□

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
- $\alpha \to \beta$ — есть способ перестроить α в β
- $\perp$ — конструкция без построения *(bottom)*
- $\neg\alpha \equiv \alpha \to \perp$

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

Теория моделей — теория, в которой $[\![\alpha]\!]$ — открытое множество в Ω — топологическом пространстве.

В ней определено следующее:

$$\begin{aligned} [\![\alpha \,\&\, \beta]\!] &= [\![\alpha]\!] \cap [\![\beta]\!] \\ [\![\alpha \vee \beta]\!] &= [\![\alpha]\!] \cup [\![\beta]\!] \\ [\![\alpha \to \beta]\!] &= ((X \setminus [\![\alpha]\!]) \cup [\![\beta]\!])^\circ \\ [\![\perp]\!] &= \varnothing \\ [\![\neg\alpha]\!] &= (X \setminus [\![\alpha]\!])^\circ \end{aligned}$$

Лекция 3

26 февраля

Рассмотрим новый способ записи доказательств — в виде деревьев.

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

У нас используются следующие правила вывода:

1. $\dfrac{}{\Gamma \vdash \gamma, \gamma \in \Gamma}$ (аксиома)
2. $\dfrac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}$ (введение $\to$)
3. $\dfrac{\Gamma \vdash \varphi \qquad \Gamma \vdash \psi}{\Gamma \vdash \varphi \,\&\, \psi}$ (введение &)
4. $\dfrac{\Gamma \vdash \varphi \to \psi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \psi}$ (удаление $\to$)
5. $\dfrac{\Gamma \vdash \varphi \,\&\, \psi}{\Gamma \vdash \varphi}$ (удаление &)
6. $\dfrac{\Gamma \vdash \varphi \,\&\, \psi}{\Gamma \vdash \psi}$ (удаление &)
7. $\dfrac{\Gamma \vdash \varphi}{\Gamma \vdash \psi \vee \varphi}$ (введение $\vee$)
8. $\dfrac{\Gamma \vdash \psi}{\Gamma \vdash \psi \vee \varphi}$ (введение $\vee$)
9. $\dfrac{\Gamma \vdash \perp}{\Gamma \vdash \varphi}$ (удаление $\perp$)
10. $\dfrac{\Gamma, \varphi \vdash \rho \qquad \Gamma, \psi \vdash \rho \qquad \Gamma \vdash \varphi \vee \psi}{\Gamma \vdash \rho}$

Пример. $$\dfrac{\dfrac{}{A \vdash A}\ \text{(акс.)}}{\vdash A \to A}\ \text{(введение \&)}$$

Пример. $$\dfrac{\dfrac{\dfrac{\dfrac{}{A \mathbin{\&} B \vdash A \mathbin{\&} B}\ \text{(акс.)}}{A \mathbin{\&} B \vdash B} \qquad \dfrac{\dfrac{}{A \mathbin{\&} B \vdash A \mathbin{\&} B}\ \text{(акс.)}}{A \mathbin{\&} B \vdash A}}{A \mathbin{\&} B \vdash B \mathbin{\&} A}}{\vdash A \mathbin{\&} B \to B \mathbin{\&} A}\ \text{(введение} \to\text{)}$$

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 $k \le x$
- **Минимальный элемент** S — такой $k \in S$, что нет $x \in S$, что $x \le k$
- **Множество верхних граней** a и $b : \{x \mid a \le x \mathbin{\&} b \le x\}$.
- **Множество нижних граней** a и $b : \{x \mid x \le a \mathbin{\&} x \le b\}$.
- $a+b$ — наименьший элемент множества верхних граней *(может не существовать)*.
- $a \cdot b$ — наибольший элемент множества нижних граней.
- **Решетка** — множество + отношение, где для каждых 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.

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

Пример.

$$\begin{tikzcd} 1 \arrow[r] \arrow[d] & b \arrow[d] \\ a \arrow[r] & 0 \end{tikzcd}$$

$$
\begin{aligned}
a \cdot 0 &= 0 \\
1 \cdot b &= b \\
a \cdot b &= 0 \\
a + 0 &= 1
\end{aligned}
$$

Лемма 4. В импликативной решетке всегда есть 1.

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

$$a \to a = \text{н}\{x \mid a \cdot x \le a\} = \text{н}(A)$$

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

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

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

Теорема 5. Пусть (X, Ω) — топологическое пространство, $a + b = a \cup b, a \cdot b = a \cap b, a \to b = ((X \setminus a) \subset b)^\circ$, $a \le b \Leftrightarrow a \le b$, тогда $(\Omega, \le)$ есть алгебра Гейтинга.

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

1. $X^0 = X$
2. $a \to 0 = (X \setminus a \cup \varnothing) = X \setminus a$

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

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

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

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

Теорема 6. Алгебра Гейтинга — полная модель интуиционистской логики.

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