

Математическая логика

Михайлов Максим

19 марта 2021 г.

Оглавление

Лекция 1	12 февраля	3
0.	Мотивация	3
0.1.	Математикам	3
0.2.	Программистам	4
1.	Исчисление высказываний	4
1.1.	Язык	4
1.2.	Метаязык и предметный язык	4
1.3.	Сокращения записи	5
1.4.	Теория моделей	5
1.5.	Теория доказательств	6
1.6.	Правило Modus Ponens и доказательство	6
Лекция 2	19 февраля	7
2.	Интуиционистская логика	10
2.1.	ВНК-интерпретация	10
Лекция 3	26 февраля	11
2.2.	Естественный (натуральный) вывод	11
2.3.	Теория решеток	12
Лекция 4	5 марта	15
2.4.	Табличные модели	15
2.5.	Модели Крипке	16
Лекция 5	12 марта	18
3.	Изоморфизм Карри-Ховарда	18
3.1.	Алгебраические типы	18
3.2.	Применение восьмой аксиомы интуиционистской логики	19
4.	Исчисление предикатов	20
4.1.	Язык исчисления предикатов	20
4.2.	Теория моделей	21
4.3.	Теория доказательств	22

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

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)

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

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

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

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.

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

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

1. $X^0 = X$
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. Алгебра 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 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 $\llbracket P_i \rrbracket = \{W_k \mid W_k \Vdash P_i\}$ 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 $W_i \not\models (P_i \rightarrow P_j) \ \& \ (P_k \rightarrow P_j)$, таким образом $\not\models (P_i \rightarrow P_j) \ \& \ (P_k \rightarrow P_j)$ и $\not\models \bigvee (P_i \rightarrow P_j) \ \& \ (P_k \rightarrow P_j)$, 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

Определение. 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 10. $\Gamma(\mathcal{A})$ 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 11. 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 12. 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. 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 Гёделеваемости $\Gamma(\mathcal{L})$ $\llbracket \alpha \rrbracket = 1$ 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:

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

¹ или ещё десятком других символов

² и классической

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.

³ По записи кванторов нет общепринятого соглашения.

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, $V = \{И, Л\}$
2. Каждому $f_i(x_1 \dots x_n)$ сопоставим функцию $f_{f_n} : D^n \rightarrow D$
3. Каждому $P_j(x_1 \dots x_n)$ сопоставим функцию⁵ $f_{p_n} : D^n \rightarrow V$
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.
 - $\llbracket P_i(\theta_1 \dots \theta_n) \rrbracket = f_{p_i}(\llbracket \theta_1 \rrbracket \dots \llbracket \theta_n \rrbracket)$
 - $\llbracket f_j(\theta_1 \dots \theta_n) \rrbracket = f_{f_j}(\llbracket \theta_1 \rrbracket \dots \llbracket \theta_n \rrbracket)$
 - $\llbracket \forall x.\varphi \rrbracket = \begin{cases} И, & \text{если } \llbracket \varphi \rrbracket = И \text{ при всех } k \in D \\ Л, & \text{иначе} \end{cases}$
 - $\llbracket \exists x.\varphi \rrbracket = \begin{cases} И, & \text{если } \llbracket \varphi \rrbracket = И \text{ при некотором } k \in D \\ Л, & \text{иначе} \end{cases}$

Пример. $\forall x.\forall y.E(x, y)$

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

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

Вспомним определение предела последовательности из матанализа:

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

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

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

⁵, называемую предикат

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

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:

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

$$2. \varphi[x := \theta] \rightarrow \exists x. \varphi$$

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:

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

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