Математическая логика

Михайлов Максим

26 августа 2021 г.

Оглавление

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, $\lim\limits_{x \to +\infty} \frac{1}{x} = 0 = \lim\limits_{x \to +\infty} \frac{1}{x^2}$, 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 истинностных 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 (М.Р.). Эта новая последовательность — доказательство $\Gamma, \alpha \vdash \beta$

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

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

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

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

   $n + 1$ $\quad \alpha \to \delta_{n+1}$ (M.P. $n + 0.2, n + 0.4$)

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 $\quad \alpha \to \delta_l$

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

   $n + 0.4$ $\quad (\alpha \to \delta_l \to \delta_{n+1}) \to (\delta \to \delta_{n+1})$ (M.P. $n + 2, l$)

   $n + 1$ $\quad \alpha \to \delta_{n+1}$ (M.P. $n + 0.4, k$)

$\square$

$\square$

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

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

Рассмотрим n и пусть $[\![\delta_1]\!] =$ И, $\ldots$ $[\![\delta_n]\!] =$ 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 $\vDash \alpha$. 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.

$$1. \quad \alpha \qquad (\in \Gamma)$$

$$
\begin{array}{lll}
2. & \alpha \to (\neg\beta \to \alpha) & \text{(a. 1)} \\
3. & \neg\beta \to \alpha & \text{(M.P. 1,2)} \\
4. & \neg\alpha & (\in \Gamma) \\
5. & \neg\alpha \to (\neg\beta \to \neg\alpha) & \text{(a. 1)} \\
6. & \neg\beta \to \neg\alpha & \text{(M.P. 4,5)} \\
7. & (\neg\beta \to \alpha) \to (\neg\beta \to \neg\alpha) \to \neg\neg\beta & \text{(a. 9)} \\
8. & (\neg\beta \to \neg\alpha) \to \neg\neg\beta & \text{(M.P. 3,7)} \\
9. & \neg\neg\beta & \text{(M.P. 6,8)} \\
10. & \neg\neg\beta \to \beta & \text{(a. 10)} \\
11. & \beta & \text{(M.P. 9,10)}
\end{array}
$$

□

Доказательство теоремы о полноте. $\vDash \alpha$, 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 ${}_{[x_1]}P_1 \dots {}_{[x_{n-1}]}P_{n-1} \vdash \alpha$

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

□

2 Интуиционистская логика

2.1 BHK-интерпретация (Brouwer–Heyting–Kolmogorov)

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:

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

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. $\dfrac{}{\Gamma \vdash \gamma, \gamma \in \Gamma}$ (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. $$\frac{\Gamma, \varphi \vdash \rho \qquad \Gamma, \psi \vdash \rho \qquad \Gamma \vdash \varphi \vee \psi}{\Gamma \vdash \rho}$$

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

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

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

Пример.

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

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

Лемма 4. В импликативной решетке всегда есть 1.

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

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

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

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. $\varnothing \in \Omega, X \in \Omega$

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, $a + b = a \cup b$, $a \cdot b = a \cap b$, $a \to b = ((X \setminus a) \cup b)^\circ$, $a \leq b \Leftrightarrow a \subseteq b$, тогда $(\Omega, \leq)$ есть алгебра Гейтинга.

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

1. $X^\circ = X$
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. $(X/_{\approx}, \le)$ — **алгебра Линденбаума**, где $X, \approx$ из интуиционистской логики.

Теорема 6. Алгебры Гейтинга — полная модель интуиционистской логики.

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

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 $[\![P_i]\!] \in V$, $f_{\mathcal{P}} : P_i \rightarrow V$

И $[\![P_i]\!] = f_{\mathcal{P}}(P_i)$, $[\![\alpha \star \beta]\!] = f_{\star}([\![\alpha]\!], [\![\beta]\!])$, $[\![\neg\alpha]\!] = f_{\neg}([\![\alpha]\!])$

$\vDash \alpha$ означает, что $[\![\alpha]\!] = T$ 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)* $W_i \Vdash \alpha \mathbin{\&} \beta$
- $W_i \Vdash \alpha$ 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 $W_i \Vdash \alpha \to \beta$
- $W_i \Vdash \neg\alpha$ 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 $\vDash \alpha$

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 $[\![P_i]\!] = \{W_k \mid W_k \Vdash P_j\}$ и аналогично $[\![\alpha]\!] = \{W_k \mid W_k \Vdash \alpha\}$. Корректность этого определения докажем в ДЗ.

Поскольку любая топология является корректной моделью ИИВ, искомое доказано. □

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

Рассмотрим следующую формулу:

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

1. $\nvdash \varphi_n$. Почему? Рассмотрим последовательность миров, таких что $W_i \Vdash P_i$, состоящую из $n+1$ мира. Тогда $W_i \nVdash (P_i \to P_j) \mathbin{\&} (P_j \to P_i)$, т.к. $W_i \nVdash P_j$, но $W_i \Vdash P_i$, таким образом $\nVdash (P_i \to P_j) \mathbin{\&} (P_j \to P_i)$ и $\nVdash \bigvee (P_i \to P_j) \mathbin{\&} (P_j \to P_i)$, а значит $\nvdash \varphi_n$
2. $\vDash \varphi_n$ в V по принципу Дирихле: $\exists i \neq j : [\![P_i]\!] = [\![P_j]\!]$, а значит $[\![P_i \to P_j]\!] =$ И, и соответственно $[\![\varphi_n]\!] =$ И.

Т.к. $\vDash \varphi_n$, то $\vdash \varphi_n$, но это не так — противоречие. □

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. □

Определение. Гомоморфизм алгебр Гейтинга — отображение $\varphi : \mathcal{A} \to \mathcal{B}$, 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 : ИИВ $\to \mathcal{A}$, g : ИИВ $\to \mathcal{B}$. Тогда φ **согласовано** с f, g, если $\varphi(f(\alpha)) = g(\alpha)$

Теорема 13. Если $\varphi : \mathcal{A} \to \mathcal{B}$ согласована с f, g и $[\![\alpha]\!]_g \neq 1_\mathcal{B}$, то $[\![\alpha]\!]_f \neq 1_\mathcal{A}$

Доказательство теоремы 10. Рассмотрим алгебру Линденбаума $\mathcal{L}$, $\Gamma(\mathcal{L})$ и $\varphi : \Gamma(\mathcal{L}) \to \mathcal{L}$ — 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 $[\![\alpha \vee \beta]\!]_{\Gamma(\mathcal{L})} = 1_{\Gamma(\mathcal{L})}$, но по Гёделевости $\Gamma(\mathcal{L})$ $[\![\alpha]\!] = 1$ или $[\![\beta]\!] = 1$.

Пусть $\nvdash \alpha$ и $\nvdash \beta$. Тогда $\varphi([\![\alpha]\!]) \neq 1_\mathcal{L}$ и $\varphi([\![\beta]\!]) \neq 1_\mathcal{L}$. Тогда $[\![\alpha]\!]_{\Gamma(\mathcal{L})} \neq 1_\mathcal{L}, [\![\beta]\!] \neq 1_\mathcal{L}$ — противоречие. □

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. $p : \alpha \to \beta$

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 -> 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
$\to$	функция
&	упорядоченная пара
$\vee$	алгебраический тип *(тип-сумма)*

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 *(дизъюнктное)* объединение** множеств A, B обозначается $A \sqcup B$ или $A \uplus B$ [1] и равно $\{\langle \text{“}A\text{”}, a\rangle \mid a \in A\} \cup \{\langle \text{“}B\text{”}, b\rangle \mid b \in B\}$.

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 интуиционистской [2] логики и запишем её как правило натурального вывода:

$$\frac{\Gamma \vdash \alpha \to \gamma \qquad \Gamma \vdash \beta \to \gamma \qquad \Gamma \vdash \alpha \vee \beta}{\Gamma \vdash \gamma}$$

[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:

$$\frac{\Gamma \vdash Nil \to string \qquad \Gamma \vdash list \to string \qquad \Gamma \vdash Nil \vee list}{\Gamma \vdash string}$$

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 — метапеременная для термов.

Термы бывают двух видов:

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

Логические выражения:

- Применение предикатных символов $P(\theta_1, \dots \theta_n)$, где P — метапеременная для предикатных символов, а предикатный символ — $A, B, C \dots$
- Связки $\&, \vee, \neg, \to$ 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. $\forall x.P(x) \mathbin{\&} \forall y.P(y) \equiv \forall x.(P(x) \mathbin{\&} (\forall y.P(y)))$

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 $f_{f_n} : D^n \to D$
3. Каждому $P_j(x_1 \dots x_m)$ сопоставим функцию [5] $f_{p_m} : D^m \to V$
4. Каждой x_i сопоставим $f_{x_i} \in D$

- $[\![x]\!] = f_{x_i}$
- $[\![\alpha \star \beta]\!]$ — так же, как в исчислении высказываний.
- $[\![P_i(\theta_1 \dots \theta_n)]\!] = f_{p_i}([\![\theta_1]\!] \dots [\![\theta_n]\!])$
- $[\![f_j(\theta_1 \dots \theta_n)]\!] = f_{f_j}([\![\theta_1]\!] \dots [\![\theta_m]\!])$
- $[\![\forall x.\varphi]\!] = \begin{cases} \text{И}, & \text{если } [\![\varphi]\!] = \text{И при всех } k \in D \\ \text{Л}, & \text{иначе} \end{cases}$
- $[\![\exists x.\varphi]\!] = \begin{cases} \text{И}, & \text{если } [\![\varphi]\!] = \text{И при некотором } k \in D \\ \text{Л}, & \text{иначе} \end{cases}$

Пример. $\forall x.\forall y.E(x, y)$

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

$[\![\forall x.\forall y.E(x, y)]\!]_{x:=1, y:=2} = \text{Л}$, т.к. $[\![E(x, y)]\!] = \text{Л}$.

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

$$\forall \varepsilon.\varepsilon \to 0\ \exists N.\forall n.(n > N) \to (|a_n - a| < \varepsilon)$$
$$\forall \varepsilon.\varepsilon \to 0\ \exists N.\forall n.(n > N) \to (|a_n - a| < \varepsilon)$$
$$\forall e.G(e, m_0)\ \exists n_0.\forall n.G(n, n_0) \to G(e, m_|(m_-(m_a(n), a)))) < \varepsilon)$$

4.3 Теория доказательств

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

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

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. $\dfrac{\varphi \to \psi}{\varphi \to (\forall x.\psi)}$ (правило $\forall$)
2. $\dfrac{\psi \to \varphi}{(\exists x.\psi) \to \varphi}$ (правило $\exists$)

Лекция 6

19 марта

Пример. $\dfrac{\varphi \to \psi}{\exists x.(\varphi \to \psi)}$ — 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 $\alpha_k = \alpha_j \to \alpha_i$
3. Существует j, такое что $\alpha_j = \varphi \to \psi$ и $\alpha_i = (\exists x.\varphi) \to \psi$, причём x не входит свободно в ψ.
4. Существует j, такое что $\alpha_j = \psi \to \varphi$ и $\alpha_i = \psi \to \forall x.\varphi$, причём x не входит свободно в ψ.

4.4 Вхождение

Рассмотрим некоторую формулу и рассмотрим вхождения x в неё:

$$(P(\underbrace{x}_{1}) \vee Q(\underbrace{x}_{2})) \to (R(\underbrace{x}_{3})\ \&\ (\overbrace{\forall \underbrace{x}_{4}.P_1(\underbrace{x}_{5})}^{\text{Область действия } \forall \text{ по } x}))$$

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

Случай множественного связывания:

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

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.

$$(\forall x.\forall y.\forall x.P(x))[x := y] \equiv \forall x.\forall y.\forall x.P(x)$$

$$P(x) \lor \forall x.P(x)[x := y] \equiv P(y) \lor \forall x.P(x)$$

$$(\forall y.x = y)[x := y] \equiv \forall y.y = y$$

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.

$$\begin{array}{lcr}
(1) & \gamma_1 & \\
 & \vdots & \\
(n) & \gamma_n & \\
(n+1) & A \,\&\, A \to A & \text{(акс.)} \\
(n+2) & \alpha \to ((A \,\&\, A \to A) \to \alpha) & \text{(акс.)} \\
(n+3) & (A \,\&\, A \to A) \to \alpha & \text{(M.P. } n, n+2\text{)} \\
(n+4) & (A \,\&\, A \to A) \to \forall x.\alpha & \text{(введение } \forall\text{)} \\
(n+5) & \forall x.\alpha & \text{(M.P. } n+1, n+4\text{)}
\end{array}$$

□

Лемма 6. $(\alpha \to \varphi \to \psi) \to \alpha \,\&\, \varphi \to \psi$

Лемма 7. $(\alpha \,\&\, \varphi \to \psi) \to (\alpha \to \varphi \to \psi)$

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

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

Рассмотрим случаи:

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

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

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

□

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 $\gamma \in \Gamma$ $[\![\gamma]\!] = \text{И}$, выполнено $[\![\alpha]\!] = \text{И}$

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 $[\![\alpha[x := \Theta]]\!] = [\![\alpha]\!]^{x:=[\![\Theta]\!]}$

Примечание. Здесь и далее мы предполагаем условие корректности.

4.6 Полнота исчисления предикатов

Определение. Γ — непротиворечивое. если $\Gamma \nvdash \alpha \mathbin{\&} \neg\alpha$ ни при каком α

Пример.

- Непротиворечивое: $\varnothing, A \vee \neg A$
- Противоречивое: $A \mathbin{\&} \neg A$

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

Пример.

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

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

Определение. $(\ldots)$ 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 Γ $(\dots)$ 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.:

$$\Gamma, \alpha \vdash \beta \mathbin{\&} \neg\beta \quad \Gamma, \neg\alpha \vdash \beta \mathbin{\&} \neg\beta$$

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

Т.е. Γ — противоречиво. Это противоречие. □

Теорема 16. Если Γ — $(\dots)$ и в языке счётное количество формул[1], 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.

$\Gamma_0 := \Gamma$

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

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

$\vdots$

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

Пусть $\Gamma^* \vdash \beta \mathbin{\&} \neg\beta$. 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 $\Gamma_{\max(R_i)} \vdash \beta \mathbin{\&} \neg\beta$ — противоречие. □

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

Доказательство. Пусть D — все записи из функциональных символов:

$[\![f_0^n]\!]$[2] $\Rightarrow$ “f_0^n”

[1] В исчислении предикатов это верно.
[2] константа

$[\![f_k^n(\theta_1 \dots \theta_k)]\!] \Rightarrow \text{“}f_k^n(\text{”} + [\![\theta_1]\!]\text{“},\text{”} + \dots + \text{“},\text{”} + [\![\theta_n]\!] + \text{“})\text{”}$

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

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 $\alpha \mathbin{\&} \beta$.

1. Если $[\![\alpha]\!] = \text{И}$ и $[\![\beta]\!] = \text{И}$, то $\alpha \mathbin{\&} \beta \in \Gamma$
2. Если $[\![\alpha]\!] \neq \text{И}$ или $[\![\beta]\!] \neq \text{И}$, то $\alpha \mathbin{\&} \beta \notin \Gamma$

□

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 $\varphi \to \psi$ и $\psi \to \varphi$.

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:

$$\begin{tikzcd} \Gamma \arrow[d, "\text{без кванторов}"'] & M \\ \Gamma^\Delta \arrow[r, "\text{теорема}"] & M^\Delta \arrow[u, "id"] \end{tikzcd}$$

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 $\Gamma_i \to \Gamma_{i+1}$.

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 $\Gamma_{i+1} = \Gamma_i \cup \{$все добавленные формулы$\}$. □

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

Доказательство. Пусть $\models \alpha$, но не $\nvdash \alpha$. Значит, $\{\neg\alpha\}$ — непротиворечивое множество замкнутых формул.

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

Значит, у $\neg\alpha$ есть модель M, $[\![\neg\alpha]\!]_M =$ И. Значит, $\nvDash \alpha$ □

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 — замкнутая[1] формула исчисления предикатов, то найдётся ψ — замкнутая формула исчисления предикатов, такая что $\vdash \varphi \to \psi$ и $\psi \to \varphi$, при этом ψ с поверхностными кванторами.

Доказательство. В домашних заданиях. $\square$

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 $\vdash \varphi \to \psi, \vdash \psi \to \varphi$.

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

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

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

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 $d^k_1 \dots d^k_j$.
3. $\varphi_i \equiv \exists x.\varphi$ — добавим $\varphi[x := d^i_{j+1}]$

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

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

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

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

$\Gamma_i \vdash \gamma_1 \to \gamma_2 \to \dots \to \gamma_n \to \beta \mathbin{\&} \neg\beta$

Докажем, что $\Gamma_i \vdash \beta \mathbin{\&} \neg\beta$ по индукции. $\Gamma_i \vdash \gamma \to \varepsilon$[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 $\Gamma_i \vdash \gamma \to \varepsilon$. $\Gamma_i \vdash (\forall x.\xi) \to \underbrace{(\xi[x := \theta])}_{\substack{\gamma \text{ по} \\ \text{построению } \Gamma_{i+1}}}$ — по аксиоме 11. Очевидно, что $(\forall x.\xi) \to \varepsilon$ 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 никак[3].

Рассмотрим $\Gamma_i \vdash \underbrace{\xi[x := d^k_{i+1}]}_{\gamma} \to \varepsilon$. Заметим, что d^k_{i+1} не входит в ε. Заменим все d^k_{i+1} в доказательстве на y — новую переменную. Это будет доказательством $\Gamma \vdash \xi[x := y] \to \varepsilon$. Тогда $\exists y.\xi[x := y] \to \varepsilon$[4]. По ДЗ можно заметить, что $(\exists x.\xi x) \to (\exists y.\xi[x := y])$ и по лемме $(\exists x.\xi) \to \varepsilon$ и у нас есть гипотеза $\exists x.\xi$, поэтому по М.Р. ε.

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

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

Утверждение. Γ^* непротиворечиво.

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

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

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

Утверждение. Если $\gamma \in \Gamma'$, то $[\![\gamma]\!]_M =$ 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.

$[\![\forall x.\delta]\!] =$ И, если $[\![\delta]\!]^{x:=k} =$ И$, k \in D$[5]. Рассмотрим $[\![\delta]\!]^{x:=k}, k \in D$. 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 $[\![\delta[x := k]]\!] =$ 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 ленты[6]. 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 $(s_x, b_s) \to (s_y b_t, a)$, где a — одно из действий “передвинуться влево”, “перевдинуться вправо”, “не двигаться”. x — буква на ленте, s — текущее состояние. То же самое, но в терминах предиката :

1. Не двигаться:
$$\forall z.\forall w.R(c(s_x, z), w, b_s) \to R(c(s_x, z), w, b_t)$$

2. Передвинуться влево:
$$\forall z.\forall w.R(c(s_x, z), w, b_s) \to R(z, c(s_y, w), b_t)$$

[5] все записи из функциональных символов
[6] машины Тьюринга

3. Передвинуться вправо:

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

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: $\varphi \to \exists z.\exists w.R(z, w, b_\Delta)$. 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 первая[1] попытка формализации чисел. Будем говорить, что N соответствует аксиоматике Пеано, если:

1. Задана $(')$: $N \to N$ — иньективная 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: $P(x) \to P(x')$

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

□

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 $a + c' = c' + a$

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

□

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. $a = b \to a' = b'$
2. $a = b \to a = c \to b = c$
3. $a' = b' \to a = b$
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:

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

   Если x входит свободно в ψ

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

Определение. $a \le b$ — сокращение для $\exists n.a + n = b$

Определение.

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

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

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 $\vdash w[x_1 := \overline{k_1} \dots x_n := \overline{k_n}]$
2. $(k_1 \dots k_n) \notin W$, тогда $\vdash \neg w[x_1 := \overline{k_1} \dots x_n := \overline{k_n}]$

Определение. $f : \mathbb{N}^n \to \mathbb{N}$ **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 $\vdash \varphi(\overline{k_1} \dots \overline{k_{n+1}})$
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. $Z : \mathbb{N} \to \mathbb{N} : Z(x) = 0$
2. $N : \mathbb{N} \to \mathbb{N} : N(x) = x + 1$
3. $S_k : \mathbb{N}^m \to \mathbb{N}$ — подстановка

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

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

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

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

R называется **примитивной рекурсией**.

R можно воспринимать как цикл `for` с переменной цикла y.

Пример.

(a) $R\left<f, g\right> x = f(x)$

(b) $R\left<f, g\right> x = g(0, f(x), x)$

(c) $R\left<f, g\right> x = g(1, g(0, f(x), x), x)$

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

Пример.

1. $1(x) = 1$
$$1 = S\left<N, Z\right>$$

2. $(+2)(x) = x + 2$
$$(+2) = S\left<N, N\right>$$
$$S\left<N, N\right>(x) = g(f(x)) = N(N(x)) = x + 2$$

3.
$$(+3) = S\left<N, S\left<N, N\right>\right>$$

4. $(\times 2)$

   Промежуточная функция:
$$(\times 2_a) = R\left<P^1_1, S\left<N, P^2_3\right>\right>$$
$$(\times 2) = S\left<(\times 2_a), P^1_1, P^1_1\right>$$

Добавим новый примитив “минимизация”:

6. $M\left<f\right> : \mathbb{N}^m \to N$ при $f : \mathbb{N}^{m+1} \to \mathbb{N}$

   $M\left<f\right>(x_1 \dots x_m) = y$ — 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. $(+), (\cdot), (x^y), (:), (\sqrt{}),$ деление с остатком, числа Фибоначчи — примитивно-рекурсивные функции.

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

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

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

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

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 сломаем наше доказательство — создадим формулу “для меня нет доказательства”.

Теорема 25.A. 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. $M \langle f \rangle$
   $$\varphi(x_{m+1}, x_1 \dots x_m, \overline{0}) \,\&\, \forall y.y < x_{m+1} \to \neg\varphi(y, x_1 \dots x_m, \overline{0})$$

5. β-функция Гёделя:
   $$\beta(b, c, i) = b\%(1 + c \cdot (i + 1))$$

   Теорема 25.B. $a_0 \dots a_n$ — некоторые значения $\in \mathbb{N}$. Тогда найдутся b c 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: $1 + c(i + 1) \equiv 0 \mod p$ и $1 + c(j + 1) \equiv 0 \mod p$. Тогда $c(i + 1 - j - 1) \equiv 0 \mod p$ и $c(i - j) \equiv 0 \mod p$ — противоречие. □

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

□

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 $f \leftrightarrow \varphi, g \leftrightarrow \gamma$:

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

□

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

Определение. $\ulcorner S_0 \dots S_n \urcorner = 2^{\ulcorner S_0 \urcorner} \cdots p_n^{\ulcorner S_{n-1} \urcorner}$, 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 $f : \mathbb{N} \to \mathbb{N}$, 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:

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

- $S \left\langle \text{plog}_2, P^1_{n+2} \right\rangle$ — 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 минимальное[2] y, такое что при вышеуказанной подстановке $Proof = 0$. Т.к. нам нужно получить k_{n+1}, то мы берём plog_2. □

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 $W_1 = 1$.

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 $\sigma(\overline{\ulcorner \sigma \urcorner})$?

Примечание. Эта тема несколько архаична.

---

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

[2] что нам не нужно, но пусть будет

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

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

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

Теорема 30 (Гёделя о неполноте арифметики №1).

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

Доказательство.

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

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

□

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 $\nvdash \omega_1(\ulcorner\sigma\urcorner, p)$ для любого p. Тогда $[\![\omega_1(\overline{\ulcorner\sigma\urcorner}, p)]\!] =$ Л, следовательно $[\![\forall p.\neg\omega_1(\overline{\ulcorner\sigma\urcorner}, p)]\!] =$ И. Но $\nvdash \sigma(\overline{\ulcorner\sigma\urcorner})$ — противоречие. □

Есть формулировка этой теоремы без ω-непротиворечивости.

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

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

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

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 $\nvdash \rho(\overline{\ulcorner\rho\urcorner})$
2. Если формальная арифметика непротиворечива, то $\nvdash \neg\rho(\overline{\ulcorner\rho\urcorner})$

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

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

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

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

Доказательство. Полного доказательства не будет, оно убийственное[3].

Если вдуматься, то доказывать нечего, т.к. теорема гласит, что если формальная арифметика непротиворечива, то не существует доказательства самоприменения σ, т.е. $\forall p.\neg\omega_1(\overline{\ulcorner \sigma \urcorner}, p)$. 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 $\forall x.x \in a \to x \in b$

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

Определение (пара).

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

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 $(a \to b)$ & $(b \to a)$

[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.

$$\forall abc.a = b \,\&\, a \in c \to b \in c$$

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

Примечание. Также можно определить пустое множество как константу теории.

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

В формальном виде:

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

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:

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

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.

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

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 метапеременная φ.

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

$$\varnothing \in N \,\&\, \forall x.x \in N \to x \cup \{x\} \in N$$

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

Доказательство. Рассмотрим случаи:

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

□

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:

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

Определение. $a' = a \cup \{a\}$

Обозначение (ординальные числа).

- $\overline{0} = \varnothing$
- $\overline{1} = \varnothing' = \{\varnothing\}$
- $\overline{2} = \varnothing'' = \{\varnothing, \{\varnothing\}\}$
- $\overline{3} = \varnothing''' = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$

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

$$\forall a.\forall b.a \in b \,\&\, b \in S \to a \in S$$

Определение. Множество s **вполне упорядоченно** отношением "$\in$", если:

1. $\forall a.\forall b.a \in s \,\&\, b \in s \to a \in b \vee b \in a \vee a = b$ — линейность
2. $\forall t.t \subseteq s \to \exists a.a \in t \,\&\, \forall b.b \in t \to b = a \vee a \in b$ — 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.

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

Очевидно, что $\omega \subseteq N$

Теорема 35. ω — множество.

Определение.

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

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 семействе[1] непустых множеств $\{A_S\}_{S \in \mathbb{S}}$ можно определить функцию $f : \mathbb{S} \to \bigcup_S A_S$, которая мо множеству возвращает его элемент.
- Любое множество можно вполне упорядочить.
- Для любой сюрьективной функции $f : A \to B$ найдётся частично обратная $g : B \to A$, 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 **ZF**[2], а с аксиомой выбора обозначается **ZFC**[3].

Определение. **Дизъюнктное семейство множеств** — семейство непересекающихся подмножеств.[4]

$$D(y) : \forall p.\forall q.p \in y \,\&\, q \in y \to p \cap q = \varnothing$$

[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).

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

Формулировка аксиомы выбора, которую мы будем использовать:

Аксиома (выбора). Если $D(y) \,\&\, \forall t.t \in y \to t \neq \varnothing$, то $\bigtimes y \neq \varnothing$

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

Теорема 36 (Диаконеску). Рассмотрим ZF поверх ИИП[5]. Если добавить аксиому выбора, то $\vdash \alpha \vee \neg\alpha$.

Аксиома 9 (фундирования).

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

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 $a \to b$ 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 $f : a \to b$ — инъективно, но нет биекции.

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

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

[5] а не КИП

- $\vdots$

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

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, $f : a \to b$ и $g : b \to a$ инъективны, то существует биекция $a \to b$.