Лекции по Математической логике 4 семестр

Ilya Yaroshevskiy

20 апреля 2021 г.

Оглавление

Лекция 1

1.1 Исчесление высказываний

1.1.1 Язык

1. Пропозициональные переменные
   A_i' — большая буква начала латинского алфавита

2. Связки
   $\underbrace{\alpha}_{\text{метапеременная}}, \beta$ — высказывания
   Тогда $(\alpha \rightarrow \beta), (\alpha \& \beta), (\alpha \vee \beta), (\neg \alpha)$ — высказывания

1.1.2 Мета и предметные

- $\alpha, \beta, \gamma, \ldots, \varphi, \psi, \ldots$ — метапеременные для выражений
- X, Y, Z — метапеременные для предметные переменные

Метавыражение: $\alpha \rightarrow \beta$
Предметное выражение: $A \rightarrow (A \rightarrow A)$ (заменили α на A, β на $(A \rightarrow A)$)

Пример. Черным — предметные выражения, Синим — метавыражения

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

$$(\alpha \rightarrow (A \rightarrow X))[\alpha \coloneqq A, X \coloneqq B] \equiv A \rightarrow (A \rightarrow B)$$

$$(\alpha \rightarrow (A \rightarrow X))[\alpha \coloneqq (A \rightarrow P), X \coloneqq B] \equiv (A \rightarrow P) \rightarrow (A \rightarrow B)$$

1.1.3 Сокращение записи

- $\vee, \&, \neg$ — скобки слева направо(лево-ассоциативная)
- $\rightarrow$ — правоассоциативная
- Приоритет по возрастанию: $\rightarrow, \vee, \&, \neg$

Пример. Расставление скобок

$$(A \rightarrow ((B \& C) \rightarrow D))$$

$$(A \rightarrow (B \rightarrow C))$$

1.1.4 Теория моделей

- $\mathcal{P}$ — множество предметных переменных
- $[\![\cdot]\!] : \mathcal{T} \rightarrow$, где $\mathcal{T}$ — множество высказываний, $V = \{\text{И}, \text{Л}\}$ — множество истиностных значений

1. $[\![x]\!] : \mathcal{P} \rightarrow V$ — задается при оценке
   $[\![]\!]^{A:=v_1, B:=v_2}$:
   - $\mathcal{P} = v_1$
   - $\mathcal{P} = v_2$
2. $[\![\alpha \star \beta]\!] = [\![\alpha]\!] \underbrace{\star}_{\substack{\text{определенно} \\ \text{естественным образом}}} [\![\beta]\!]$, где $\star \in [\&, \vee, \neg, \rightarrow]$

   Пример.

   $$[\![A \rightarrow A]\!]^{A:=\text{И}, B:=\text{Л}} = [\![A]\!]^{A:=\text{И}, B:=\text{Л}} \rightarrow [\![A]\!]^{A:=\text{И}, B:=\text{Л}} = \text{И} \rightarrow \text{И} = \text{И}$$

   Также можно записать так:

   $$[\![A \rightarrow A]\!]^{A:=\text{И}, B:=\text{Л}} = f_{\rightarrow}([\![A]\!]^{A:=\text{И}, B:=\text{Л}}, [\![A]\!]^{A:=\text{И}, B:=\text{Л}}) = f_{\rightarrow}(\text{И}, \text{И}) = \text{И}$$

   , где $f_{\rightarrow}$ определена так:

a	b	$f_{\rightarrow}$
И	И	И
И	Л	Л
Л	И	И
Л	Л	И

1.1.5 Теория доказательств

Определение. Схема высказывания — строка соответсвующая определению высказывания, с:

- метапеременными $\alpha, \beta, \ldots$

Определение. Аксиома — высказывания:

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. $\neg\neg\alpha \to \alpha$

   #+begin$_{\text{defintion}}$ org

1.1.6 Правило Modus Ponens и доказательство

Определение. Доказательство (вывод) — последовательность высказываний $\alpha_1, \ldots, \alpha_n$, где α_i:

- аксиома
- существует $k, l < i$, что $\alpha_k = \alpha_l \to \alpha$

$$\frac{A,\ A \to B}{B}$$

Пример. $\vdash A \to A$

1	$A \to A\ \ \to A$	(схема аксиом 1)
2	$A \to (A \to A) \to A$	(схема аксиом 1)
3	$(A \to (A \to A)) \to (A \to (A \to A) \to A) \to (A \to A)$	(схема аксиом 2)
4	$(A \to (A \to A) \to A) \to (A \to A)$	(М.Р. 1 и 3)
5	$A \to A$	(М.Р. 2 и 4)

Определение. Доказательством высказывания β — список высказываний $\alpha_1, \ldots, \alpha_n$

- $\alpha_1, \ldots, \alpha_n$ — доказательство
- $\alpha_n \equiv \beta$

Лекция 2

Обозначение. Γ, Δ, Σ — списки высказываний

Определение. Следование: $\Gamma \vDash \alpha$, если

- $\Gamma = \gamma_1, \dots, \gamma_n$
- Всегда когда все $[\![\gamma_i]\!] = \text{И}$, то $[\![\alpha]\!] = \text{И}$

Пример. $\vDash \alpha$ — α общезначимо

Определение. ~~Теория~~ Исчисление высказываний корректна, если при любом α из $\vdash \alpha$ следует $\vDash \alpha$

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

Теорема 2.0.1 (о дедукции)**.** $\Gamma, \alpha \vdash \beta$ <u>тогда и только тогда, когда</u> $\Gamma \vdash \alpha \to \beta$

Доказательство.

($\Leftarrow$) Пусть $\Gamma \vdash \alpha \to \beta$.
Т.е. существует доказательство $\delta_1, \dots, \delta_n$, где $\delta_n = \alpha \to \beta$
Построим новое доказательство: $\delta_1, \dots, \delta_n, \alpha(\text{гипотеза}), \beta(\text{М.Р.})$
Эта новая последовательность — доказательство $\Gamma, \alpha \vdash \beta$

($\Rightarrow$) Рассмотрим $\delta_1, \dots, \delta_n$ — доказательство $\Gamma, \alpha \vdash \beta$

$$\begin{array}{ll} \sigma_1 & \alpha \to \delta_1 \\ \vdots & \vdots \\ \sigma_n & \alpha \to \delta_n \end{array}$$

Утврeждение: последовательность $\sigma_1, \dots, \sigma_n$ можно дополнить до доказательства, т.е. каждый σ_i — аксиома, гипотеза или получается по М.Р. Докажем по индукции:
<u>База</u>: $n = 0$
<u>Переход</u>: пусть $\sigma_0, \dots, \sigma_n$ — доказательсво. тогда $\sigma_{n+1} = \alpha \to \delta_{n+1}$ по трем вариантам:

1. δ_{n+1} — аксиома или гипотеза $\not\equiv \alpha$
2. $\delta_{n+1} \equiv \alpha$
3. $\delta_k \equiv \delta_l \to \delta_{n+1},\ k, l \le n$

Докажем каждый из трех вариантов

1.

$$\begin{array}{l|ll} (\text{n} + 0.2) & \delta_{n+1} & \text{(аксиома или гипотеза)} \\ (\text{n} + 0.4) & _{n+1} \to \alpha \to \delta_{n+1} & \text{(сх. акс. 1)} \\ (\text{n} + 1) & \alpha \to \delta_{n+1} & (\text{М.Р. } n + 0.2, n + 0.4) \end{array}$$

2. $(n + 0.2, n + 0.4, n + 0.6, n + 0.8, n + 1)$ — доказательтво $\alpha \to \alpha$
3.

$$\begin{array}{lll} (k) & \alpha \to (\sigma_l \to \sigma_{n+1}) & \\ (l) & \alpha \to \sigma_l & \\ (n+0.2) & (\alpha \to \delta_l) \to (\alpha \to (\delta_l \to \delta_{n+1})) \to (\alpha \to \delta_{n+1}) & \text{(сх. 2)} \\ (n+0.4) & (\alpha \to \delta_l \to \delta_{n+1}) \to (\alpha \to \delta_{n+1}) & (\text{М.Р. } n + 0.2, l) \\ (n+1) & \alpha \to \delta_{n+1} & (\text{М.Р. } n + 0.4, k) \end{array}$$

□

Теорема 2.0.2 (о корректности)**.** Пусть $\vdash \alpha$
Тогда $\models \alpha$

Доказательство. Индукция по длине доказательства: каждая $[\![\delta_i]\!] = $ И, если $\delta_1, \dots, \delta_k$ — доказательство α
Пусть $[\![\delta_1]\!] = $ И$, \dots, [\![\delta_n]\!] = $ И. Тогда осн. δ_{n+1}:

1. δ_{n+1} — аксиома

   (a) $\delta_{n+1} \equiv \alpha \to \beta \to \alpha$ (Сущесвуют α, β, что)
   Пусть $\delta_{n+1} = A \to B \to A$. Тогда $\alpha \equiv A, \beta \equiv B$
   $[\![\alpha \to \beta \to \alpha]\!]^{[\![\alpha]\!]:=a, [\![\beta]\!]:=b} = $ 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

2. δ_{n+1} — М.Р. $\delta_k = \delta_l \to \delta_{n+1}$
   Фиксируем оценку $[\![\delta_k]\!] = [\![\delta_l]\!] = $ И, тогда $[\![\delta_l \to \delta_{n+1}]\!] = $ И

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

Т.е. $[\![\delta_{n+1}]\!] = \text{И}$

$\square$

Теорема 2.0.3 (о полноте)**.** Пусть $\models \alpha$, тогда $\vdash \alpha$

Обозначение.

$$[\beta]^\alpha \equiv \begin{cases} \alpha & [\![\beta]\!] = \text{И} \\ \neg\alpha & [\![\beta]\!] = \text{Л} \end{cases}$$

Доказательство. Фиксируем набор перменных из α: $P_1, \ldots, P_n$
Рассмотрим $[\![\alpha]\!]^{P_1 := x_1, \ldots P_n := x_n} = \text{И}$. Докажем, что $\underbrace{[x_1]^{P_1}, \ldots, [x_n]^{P_n}}_{\Delta} \vdash [\alpha]^\alpha$.

<u>Индукция</u> по длине формулы (по структуре)
<u>База</u>: $\alpha \equiv P_i$ $[P_i]^{P_i} \vdash [P_i]^{P_i}$
<u>Переход</u>: пусть η, ζ: $\Delta \vdash [\eta]^\eta, \Delta \vdash [\zeta]^\zeta$. Покажем, что $\Delta \vdash [\eta \star \zeta]^{\eta \star \zeta}$, где $\star$ — все связки
Используя лемму: $\models \alpha$, т.е. $[x_1]^{P_1}, \ldots, [x_n]^{P_n} \vdash [\alpha]^\alpha$. Но $[\![\alpha]\!] = \text{И}$ при любой оценке,
т.е. $[x_1]^{P_1}, \ldots, [x_n]^{P_n} \vdash \alpha$ при всех x_i

$$\left.\begin{array}{r} [x_1]^{P_1}, \ldots, [x_{n-1}]^{P_{n-1}}, P_n \vdash \alpha \\ [x_1]^{P_1}, \ldots, [x_{n-1}]^{P_{n-1}}, \neg P_n \vdash \alpha \end{array}\right| \xRightarrow{\text{лемма}} [x_1]^{P_1}, \ldots, [x_{n-1}]^{P_{n-1}} \vdash \alpha$$

$\square$

Лемма 1.

- $\Gamma, \eta \vdash \zeta$
- $\Gamma, \neg\eta\zeta$

<u>*Тогда*</u> $\Gamma \vdash \zeta$

Лемма 2. $[x_1]^{P_1}, \ldots, [x_n]^{P_n} \vdash \alpha$*, то* $[x_1]^{P_1}, \ldots, [x_{n-1}]^{P_{n-1}} \vdash \alpha$

2.1 Интуиционистская логика

$A \vee B$ — плохо

Пример. Докажем: существует a, b, что $a, b \in \mathbb{R} \setminus \mathbb{Q}$, но $a^b \in \mathbb{Q}$
Пусть $a = b = \sqrt{2}$. Рассмотрим $\sqrt{2}^{\sqrt{2}} \in \mathbb{R} \setminus \mathbb{Q}$

- Если да, то OK
- Если нет, то возьмем $a = \sqrt{2}^{\sqrt{2}}, b = \sqrt{2}$, $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$

ВНК-интерпретация. α, β

- $\alpha \& \beta$ — есть α, 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 $\neg\alpha \equiv \alpha \to \perp$

Лекция 3

3.1 Правила вывода

Сверху посылки, снизу заключения

- Аксиома
$$\frac{}{\Gamma, \varphi \vdash \varphi}$$
- Введение $\to$
$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}$$
- Удаление $\to$
$$\frac{\Gamma \vdash \varphi \to \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi}$$
- Введение &
$$\frac{\Gamma \vdash \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \& \psi}$$
- Удаление &
$$\frac{\Gamma \vdash \varphi \& \psi}{\Gamma \vdash \varphi}$$
$$\frac{\Gamma \vdash \varphi \& \psi}{\Gamma \vdash \psi}$$
- Введение $\vee$
$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}$$
$$\frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}$$
- Удалние $\vee$
$$\frac{\Gamma, \varphi \vdash \rho \quad \Gamma, \psi \vdash \rho \quad \Gamma \vdash \varphi \vee \psi}{\Gamma \vdash \rho}$$

- Удаление $\perp$

$$\frac{\Gamma \vdash \perp}{\Gamma \vdash \varphi}$$

Пример.

$$\dfrac{\dfrac{}{A \vdash A}\text{(акс.)}}{\vdash A \to A}\text{(вв. }\to\text{)}$$

Пример. Докажем $\frac{}{\vdash A\&B \to B\&A}$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A\&B \vdash A\&B}\text{(акс.)}}{A\&B \vdash B}\text{(уд. \&)} \qquad \dfrac{\dfrac{}{A\&B \vdash A\&B}\text{(акс.)}}{A\&B \vdash A}\text{(уд. \&)}}{A\&B \vdash B\&A}\text{(вв. \&)}}{\vdash A\&B \to BA}\text{(вв. }\to\text{)}$$

Определение. Фиксируем A
Частичный порядок — антисимметричное, транзитивное, рефлексивное отношение
Линейный — сравнимы любые 2 элемента

- $a \leq b \vee b \leq a$
- **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 $x \leq k$

Пример.

$$\begin{tikzcd}
{[9,9,9]} \arrow[d] \arrow[dr] & & {[1,2,1]} \arrow[dll] \arrow[dl] \arrow[d] \\
{[1,0,0]} & {[0,1,0]} & {[0,0,1]}
\end{tikzcd}$$

Нет наименьшего, но есть 3 минимальных. Стрелка из a в b обозначает $b \leq a$

Определение.

- **Множество верхних граней** a и b: $\{x | a \leq x \& b \leq x\}$
- **Множество нижних граней** a и b: $\{x | x \leq a \& x \leq b\}$

Определение.

- $a + b$ — нименьший элемент множества верхних граней
- $a \cdot b$ — наибольший элемент множества нижних граней

Определение. Решетка $= \langle A, \leq \rangle$ — структура, где для каждых a, b есть как $a + b$, так и $a \cdot b$,
т.е. $a \in A, b \in B \implies a + b \in A$ и $a \cdot b \in A$

Определение. Дистрибутивная решетка если всегда $a \cdot (b+c) = ab + a \cdot c$

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

Определение. Псевдодополнение $a \to b = \text{наиб.}\{c \big| a \cdot c \leq b\}$

Определение. Импликативная решетка — решетка, где для любых a, b есть $a \to b$

Определение. 0 — наименьший элемент решетки, **1** — наибольший элемент решетки

Определение. Псевдобулева алгебра (алгебра Гейтинга) — импликативная решетка с 0

Определение. Булева алгебра — псевдобулева алгебра, такая что $a + (a \to 0) = 1$

Пример.

$$\begin{tikzcd}
& 1 \arrow[dl] \arrow[dr] & \\
a \arrow[dr] & & b \arrow[dl] \\
& 0 &
\end{tikzcd}$$

- $a \cdot 0 = 0$
- $1 \cdot b = b$
- $a \cdot b = 0$
- $a + b = 1$
- $a \to b = \text{наиб.}\{x \big| a \cdot x \leq b\} = b$
  $\{x \big| a \cdot x \leq\} = \{0, b\}$
- $a \to 1 = 1$
- $a \to 0 = 0$

Можем представить в виде пары $\langle x, y \rangle$

- $a = \langle 1, 0 \rangle$
- $b = \langle 0, 1 \rangle$
- $1 = \langle 1, 1 \rangle$
- $0 = \langle 0, 0 \rangle$

Лемма 4. *В импликативной решетке всегда есть* 1.

Теорема 3.1.1. Любая алгебра Гейтинга — модель ИИВ

Теорема 3.1.2. Любая булева алгебра — модель КИВ

Рассмотрим множество X — **носитель**. Рассмотрим $\Omega \subseteq 2^X$ — подмножество подмножеств X — **топология**.

1. $\bigcup X_i \in \Omega$, где $X_i \in \Omega$
2. $X_1 \cap \dots \cap X_n \in \Omega$, если $X_i \in \Omega$
3. $\emptyset, X \in \Omega$

Теорема 3.1.3.

- $a + b = a \cup b$
- $a \cdot b = a \cap b$
- $a \rightarrow b = ((X \setminus a) \cup b)^{\circ}$
- $a \leq b$ тогда и только тогда, когда $a \subseteq b$

Тогда $\langle \Omega, \leq \rangle$ — алгебра Гейтинга

Определение. X — все формулы логики

- $\alpha \leq \beta$ — это $\alpha \vdash \beta$
- $\alpha \approx \beta$, если $\alpha \vdash \beta$ и $\beta \vdash \alpha$
- $[\alpha]_{\approx} = \{\gamma \big| \gamma \approx \alpha\}$ — класс эквивалентности

Свойство 1. *$\langle X/_{\approx}, \leq \rangle$ — алгебра Гейтинга, где $X/_{\approx} = \{[\alpha]_{\approx} \big| \alpha \in X\}$*

Теорема 3.1.4. Алгебра гейтинга — полная модель ИИВ

Лекция 4

5 марта

Определение. **Предпорядок** — транзитивное, рефлексивнре

Определение. **Отношение порядка** (частичный) — антисимметричное, транзитивное, рефлексивное

Определение. **Линейный порядок** — порядок в котором $a \preceq b$ или $b \preceq a$

Определение. **Полный порядок** — линейный, каждое подмножество имеет наименьший элемент.

Пример. $\mathbb{N}$ — вполне упорядоченное множество

Пример. $\mathbb{R}$ — не вполне упорядоченной множество

- $(0, 1)$ не имееи наименьшего
- $\mathbb{R}$ не имеет наименьшего

4.1 Табличные модели

Определение. Назовем модель **табличной** для ИИВ:

- V — множество истинностных значений
  $f_{\to}, f_{\&}, f_V : V^2 \to V,\ f_{\neg} : V \to V$
  Выделенные значения $T \in V$
  $+i\rrbracket \in V\ f_p : p_i \to V$
- $p_i = f_{\mathcal{P}}(p_i)$
  $\llbracket \alpha \star \beta \rrbracket = f_{\star}(\llbracket \alpha \rrbracket, \llbracket \beta \rrbracket)$
  $\llbracket \neg\alpha \rrbracket = f_{\neg}(\llbracket \alpha \rrbracket)$

~~Если $\vdash \alpha$, то~~ $\vDash \alpha$ означает, что $\llbracket \alpha \rrbracket = T$, при любой $f_{\mathcal{P}}$

Определение. Конечная модель: модель где V — конечно

Теорема 4.1.1. У ИИВ не существует полной табличной модели

4.2 Модели Крипке

$$\begin{tikzcd} & \text{все банки лопнут, RSA сломают!!!} \\ P = NP? \arrow[ur, "+"] \arrow[dr, "-"'] & \\ & \text{RSA устоит} \end{tikzcd}$$

1. $W = \{W_i\}$ — множество миров
2. частичный порядок($\succeq$)
3. отношение вынужденности: $W_j \Vdash p_i$
   $(\Vdash) \subseteq W \times \mathcal{P}$
   При этом, если $W_j \Vdash p_i$ и $W_j \preceq W_k$, то $W_j \Vdash p$

Определение.

1. $W_i \Vdash \alpha$ и $W_i \Vdash \beta$, тогда (и только тогда) $W_i \Vdash \alpha \& \beta$
2. $W_i \Vdash \alpha$ или $W_i \Vdash \beta$, то $W_i \Vdash \alpha \vee \beta$
3. Пусть во всех $W_i \preceq W_j$ всегда когда $W_j \Vdash \alpha$ имеет место $W_j \Vdash \beta$
   Тогда $W_i \Vdash \alpha \to \beta$
4. $W_i \Vdash \neg\alpha$ — α не вынуждено нигде, начиная с W_i: $W_i \preceq W_j$, то $W_j \nVdash \alpha$

Теорема 4.2.1. Если $W_i \Vdash \alpha$ и $W_i \preceq W_j$, то $W_j \Vdash \alpha$

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

Теорема 4.2.2. ИИВ корректна в модели Крипке

Доказательство.

1. $\langle W, \Omega \rangle$ — топология, где $\Omega = \{w \subseteq W | \text{если } W_i \in w,\ W_i \preceq W_j,\ \text{то } W_j \in w\}$
2. $\{W_k | W_k \Vdash p_j\}$ — открытое множество
   Примем $[\![p_j]\!] = \{W_k | W_k \Vdash p_j\}$
   Аналогично $[\![\alpha]\!] = \{W_k | W_k \Vdash \alpha\}$

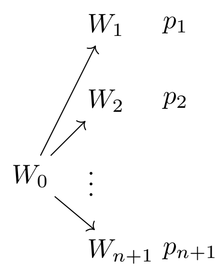
□

4.3 Доказательство нетабличности

Пусть существует конечная табличная модель $|V| = n$

$$\varphi_n = \bigvee_{\substack{1 \le i,j \le n+1 \\ i \ne j}} (p_i \to p_j \& p_j \to p_i)$$

1. $\nvdash \varphi$



$$W_1 \nVdash (p_i \to p_k) \& (p_k \to p_1),\ k \ne 1$$

Значит

$$\nvDash (p_i \to p_j) \& (p_j \to p_i)$$

$$\nvDash \bigvee (p_i \to p_j) \& (p_j \to p_i)$$

$$\nvdash \varphi_n$$

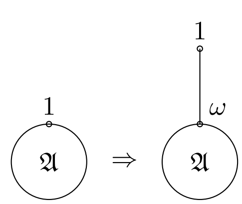
2. $\vDash_V \varphi_n$: по признаку Дирихле найдутся $i \ne j : [\![p_i]\!] = [\![p_j]\!]$
   $[\![p_i \to p_j]\!] = \text{И}$ и $[\![\varphi_n]\!] = \text{И}$
   Значит $\vdash \varphi_n$ — противоречие

Определение. Дизъюнктивность ИИВ: $\vdash \alpha \vee \beta$ влечет $\vdash \alpha$ или $\vdash \beta$

Определение. Гёделева алгебра — алгебра Гейтинга, такая что из $\alpha + \beta = 1$ следует что $\alpha = 1$ или $\beta = 1$

Определение. Пусть $\mathfrak{A}$ — алгебра Гейтинга, тогда:

1. $\Gamma(\mathfrak{A})$



Добавим новый элемент $1_{\Gamma(\mathfrak{A})}$ перенеименуем $1_{\mathfrak{A}}$ в ω

Теорема 4.3.1.

- $\Gamma(\mathfrak{A})$ — алгебра Гейтинга
- $\Gamma(\mathfrak{A})$ — Геделева

Определение. Гомоморфизм алгебр Гейтинга

- $\varphi : \mathfrak{A} \to \mathfrak{B}$
- $\varphi(a \star b) = \varphi(a) \star \varphi(b)$
- $\varphi(1_{\mathfrak{A}}) = 1_{\mathfrak{B}}$
- $\varphi(0_{\mathfrak{A}}) = 0_{\mathfrak{B}}$

Теорема 4.3.2. $a \le b$, то $\varphi(a) \le \varphi(b)$

Определение.

- α — формула ИИВ
- f, g: оценки ИИВ
- f: ИИВ $\to \mathfrak{A}$
- g: ИИВ $\to \mathfrak{B}$

φ согласованы f, g, если $\varphi(f(\alpha)) = g(\alpha)$

Теорема 4.3.3. если $\varphi : \mathfrak{A} \to \mathfrak{B}$ согласована с f, g и оценка $[\![\alpha]\!]_g \ne 1_{\mathfrak{B}}$, то $[\![\alpha]\!]_f \ne 1_{\mathfrak{A}}$

Теорема 4.3.4. ИИВ дизъюнктивно

Доказательство. Рассмторим алгебру Линденбаума: $\mathcal{L}$
Рассмотрим $\Gamma(\mathcal{L})$

- $\varphi : \Gamma(\mathcal{L}) \to \mathcal{L}$

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

φ — гомоморфизм
Пусть $\vdash \alpha \vee \beta$, тогда $[\![\alpha \vee \beta]\!]_{\Gamma(\mathcal{L})} = 1_{\Gamma(\mathcal{L})}$
$[\![\alpha + \beta]\!] = 1$, и т.к. $\Gamma(\mathcal{L})$ — Геделева то $[\![\alpha]\!] = 1$ или $[\![\beta]\!] = 1$
Пусть $\not\vdash \alpha$ и $\not\vdash \beta$, тогда $\varphi([\![\alpha]\!]) \ne 1_{\mathcal{L}}$ и $\varphi([\![\beta]\!]) \ne 1_{\mathcal{L}}$, т.е. $[\![\alpha]\!]_{\mathcal{L}} \ne 1_{\mathcal{L}}$ и $[\![\beta]\!]_{\mathcal{L}} \ne 1_{\mathcal{L}}$, тогда $[\![\alpha]\!]_{\Gamma(\mathcal{L})} \ne 1_{\Gamma(\mathcal{L})}$ и $[\![\beta]\!]_{\Gamma(\mathcal{L})} \ne 1_{\Gamma(\mathcal{L})}$ $\Rightarrow$ Противоречие $\square$

Лекция 5

12 марта

5.1 Программы

программа(функция)

- $P : \alpha \to \beta$ — берет α, возвращает β
- P — доказательство, что из α следует β

  Пример.

  ```
  f a = a
  ```

  $f : A \to A$ — f доказывает что, из A следует A

логическок исчесления	Типизированное λ-исчесление
логическая формула	тип
доказательство	значение
доказуемая формула	обитаемый тип(имеет хотя бы один экземпляр)
$\to$	функция
&	упорядоченная пара
$\vee$	алг. тип(тип-сумма)

Пример. 5 доказывает Int

Пример. Список:

```
Type list = Record
   Nul: boolean;
   case Nul of
     True  : ;
     False : Next: ^list;
end;
```

```
struct list {
        *list next;
};
```

Если `next == NULL` — то конец

Пример. Дерево:

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

Определение. Отмеченное(дизъюнктное) объединение множеств:

- A, B — множества
- $A \sqcup B = \{\langle \text{“}A\text{“}, a\rangle | a \in A\} \cup \{\langle \text{“}B\text{“}, a\rangle | b \in B\}$

Пусть $S \in A \sqcup B$. Мы знаем откуда S

```
data List a = Nil | Cons a (List a)
example = Cons 1 (Cons 2 (Cons 3 Nil)) -- [1; 2; 3]
```

```
union {
        int a;
        char b;
};
```

Пример.

$$\frac{\Gamma \vdash \overset{\text{Nil}}{\alpha} \to \gamma \quad \Gamma \vdash \overset{\text{Cons}}{\beta} \to \gamma \quad \vdash \alpha \vee \beta}{\Gamma \vdash \underset{\text{int}}{\gamma}}$$

```
let rec count l (* α + β *) =
match l with
   | Nil (* α *) -> 0 (* α → int *)
   | Cons(hd, tl) (* β *) -> 1 + count tl (* β → int *)
```

5.1.1 Исчесление предикатов

Определение. Язык исчисление предикатов

- логические выражения “предикаты“/“формулы“
- предметные выражния “термы“

Θ — метаперменные для термов
Термы:

- Атомы:
  - $a, b, c, d, \ldots$ — предметные переменные
  - x, y, z — метапеременные для предметных перменных
- Функциональные Символы
  - f, g, h — Функциональные символы(метаперемнные)
  - $f(\Theta_1, \ldots \Theta_n)$ — применение функциональных символов
- Логические выражения:
  Если $n = 0$, будем писать f, g — без скобок
  - P — метаперменные для предикатных символов
  - A, B, C — предикатный символ
  - $P(\Theta_1, \ldots, \Theta_n)$ — применение предикатных символов
  - $\&, \vee, \neg, \to$ — Связки
  - $\forall x.\varphi$ и $\exists x.\varphi$ — кванторы
    “<квантор> <переменная>.<выражение>“

1. Сокращение записи И.В + жадность $\forall, \exists$
   Метавыражение:
   $$\forall x.(P(x)\&(\forall y.P(y)))$$
   Квантор съедает все что дают, т.е. имеет минимальный приоритет.
   Правильный вариант(настоящее выражние):
   $$\forall a.B(A)\&\forall b.B(b)$$

5.1.2 Теория моделей

Оценка формулы в исчислении предикатов:

1. Фиксируем D — предметное множетво
2. Каждому $f_i(x_1, \ldots, x_n)$ сопоставим функцию $D^n \to D$

3. Каждому $P_j(x_1, \dots, x_m)$ сопоставим функцию(предикат) $D^2 \to V$
4. Каждой x_i сопоставим элемент из D

Пример.

$$\forall x. \forall y.\ E(x, y)$$

Чтобы определить формулу сначала определим $D = \mathbb{N}$

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

- $[\![x]\!] = f_{x_i}$
- $[\![\alpha \star \beta]\!]$ — смотри ИИВ
- $[\![P_i(\Theta_1, \dots, \Theta_n)]\!] = f_{P_i}([\![\Theta_1]\!], \dots, [\![\Theta_n]\!])$
- $[\![f_j(\Theta_1, \dots, \Theta_n)]\!] = f_{f_j}([\![\Theta_1]\!], \dots, [\![\Theta_n]\!])$
- $$[\![\forall x. \varphi]\!] = \begin{cases} \text{И} & , \text{если } [\![\varphi]\!]^{f_x = k} = \text{И при всех } k \in D \\ \text{Л} & , \text{иначе} \end{cases}$$
- $$[\![\exists x. \varphi]\!] = \begin{cases} \text{И} & , \text{если } [\![\varphi]\!]^{f_x = k} = \text{И при некотором } k \in D \\ \text{Л} & , \text{иначе} \end{cases}$$

$$[\![\forall x. \forall y. E(x,y)]\!] = \text{Л}$$

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

Пример.

$$\forall \boxed{\varepsilon > \boxed{0}}\ \exists N\ \forall \boxed{\boxed{\text{n}} > \boxed{\text{N}}}\quad \boxed{\boxed{|\text{a}_n - a|} < \boxed{\varepsilon}}$$

Синим отмечены функциональные конструкции(термы), зеленым предикатные

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

Обозначим:

- $(>)(a,b) = G(a,b)$ — предикат
- $|\bullet|(a) = m_|(a)$
- $(-)(a,b) = m_-(a,b)$
- $0() = m_0$
- $a_\bullet(n) = m_a(n)$

$$\forall e. \boxed{\text{G}(\boxed{\text{e}}, \boxed{\text{m}_0})} \to \exists n_0. \forall n. \boxed{\text{G(n, n}_0)} \to \boxed{\text{G}\Big(\text{e}, \boxed{\text{m}_| \Big(m_-\big(m_a(n), a\big)\Big)}\Big)}$$

5.1.3 Теория доказательств

Все аксимомы И.В + М.Р.

(схема 11) $(\forall x.\varphi) \to \varphi[x := \Theta]$

(схема 12) $\varphi[x := \Theta] \to \exists x.\varphi$

Если Θ свободен для подстановки вместо x в φ.

Определение. Свободен для подстановки — никакое свободное вхождение x в Θ не станет связанным

Пример.

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

Заменим `y := x`. Код сломается, т.к. у нас нет свобод для подстановки

(Правило $\forall$)

$$\frac{\varphi \to \psi}{\varphi \to \forall x.\psi}$$

(Правило $\exists$)

$$\frac{\psi \to \varphi}{\exists x.\psi \to \varphi}$$

В обоих правилах x не входит свободно в φ

Пример.

$$\frac{x = 5 \to x^2 = 25}{x = 5 \to \forall x.x^2 = 25}$$

Между x и x^2 была связь, мы ее разрушили. Нарушено ограничение

Пример.

$$\exists y.x = y$$

$$\forall x.\exists y.x = y \to \exists y.y + 1 = y$$

Делаем замену `x := y+1`. Нарушено требование свобод для подстановки. y входит в область действия квантора $\exists$ и поэтому свободная переменная x стала связанная.

Лекция 6

19 марта

6.1 Исчисление предикатов

6.1.1 Расставление скобок

Кванторы имеют наименьший приоритет

Пример.

$$\forall x.A\&B\&y.C\&D \vee \exists z.E$$

$$(\forall x.(A\&B\&\forall y.(C\&D \vee \exists z.(E))))$$

Еще раз про правила только со скобками

1. $$\frac{\varphi \to \psi}{(\exists.\varphi) \to \psi}$$

2. $$\frac{\psi \to \varphi}{\psi \to (\forall x.\varphi)}$$

Пример.

$$\frac{\varphi \to \psi}{\exists x.(\varphi \to \psi)}$$

— можно доказать, но это не правило вывода для $\exists$

Определение. $\alpha_1, \ldots, \alpha_n$ — доказательство

- если α_i — аксимома
- либо существует $j, k < i$, что $\alpha_k = \alpha_j \to \alpha_i$
- либо существует α_j : $\alpha_j = \varphi \to \psi$ и $\alpha_i = (\exists x.\varphi) \to \psi$ причем x не входит свободно в ψ
- либо существует $j : \alpha_j = \psi \to \varphi$ и $\alpha_i = \psi \to \forall x.\varphi$ причем x не входит свободно в ψ

6.1.2 Вхождение

Пример.
$$(P(\underset{1}{x}) \vee Q(\underset{2}{x})) \rightarrow (R(\underset{3}{x})\&(\underbrace{\forall \underset{4}{x}.P_1(\underset{5}{x})}_{\text{область } \forall \text{ по } x}))$$

1, 2, 3 — свободные, 5 — связанное, по пермененной 4

Пример.
$$\underbrace{\forall x.\forall y.\forall x.\forall y.\forall x.P(x)}_{\text{область } \forall \text{ по } x}$$

Здесь x в $P(x)$ связано. x не входит свободно в эту формулу, потому что нет свободных вхождений

Определение. Переменная x входит свободно если существует свободное вхождение

Определение. Вхождение свободно, если не связано

Можно относится к свободно входящим перменным как с перменным из библиотеки, т.е. мы не имеем права их переименовывать

Пример. Некорректная формула

α_1 $x = 0 \rightarrow x = 0$

α_2 $(\exists x.x = 0) \rightarrow (x = 0)$ — не доказано

α_2' $(\exists t.x = 0) \rightarrow (x = 0)$ — (правило $\exists$)

Пример.

(n) $x = 0 \rightarrow y = 0$ — откуда то

$(n + 1)$ $(\exists x.x = 0) \rightarrow (y = 0)$ — (правило $\exists$)

6.1.3 Свободные подстановки

Определение. Θ свободен для подстановки вместо x в φ, если никакая свободная перменная в Θ не станет связанной в $\varphi[x := \Theta]$

Определение. $\varphi[x := \Theta]$ — "Заменить все свободные вхождения x в φ на Θ"

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

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

Пример.

$$(\forall y.x = y)\ [x := \underbrace{y}_{\equiv\Theta}] \equiv \forall y.\underset{1}{y} = y$$

$FV(\Theta) = \{y\}$ — свободные перменные в Θ. Вхождение y с номером 1 стало связанным

Пример.

$$P(x)\&\forall y.x = y\ [x := y + z] \equiv P(y + z)\&\forall y.\underset{1}{y} + z = y$$

Здесь при подстановке вхождение y с номером 1 стало связанным. x — библиотечная функция, переименовали x во что-то другое.

6.1.4 Пример доказательства

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

Доказательство.

1. Т.к. $\vdash \alpha$, то существует $\gamma_1, \dots, \gamma_2 : \gamma_n = \alpha$

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

□

6.1.5 Теорема о дедукции

Теорема 6.1.1. Пусть задана Γ, α, β

1. Если $\Gamma, \alpha \vdash \beta$, то $\Gamma \vdash \alpha \to \beta$, при условии, если b в доказательстве $\Gamma, \alpha \to \beta$ не применялись правила для $\forall, \exists$ по перменным, входяшим свободно в α

2. Если $\Gamma \vdash \alpha \to \beta$, то $\Gamma, \alpha \vdash \beta$

Лекция 7

2 апреля

- $\Gamma \vDash \alpha$ — α следует из Γ при всех оценках, что все $\gamma \in \Gamma \quad [\![\gamma]\!] =$ И, выполнено $[\![\alpha]\!] =$ И
- $x = 0 \vdash \forall x.x = 0$
- $x = 0 \nvDash \forall x.x = 0$

Определение (Условие для корректности)**.** Правила для кванторов по свободным перменным из Γ запрещены.
Тогда $\Gamma \vdash \alpha$ влечет $\Gamma \vDash \alpha$

7.1 Полнота исчесления предикатов

Определение. Γ — **непротиворечивое** множество формул, если $\Gamma \nvdash \alpha \& \neg\alpha$ ни при каком α

Пример. Непротиворечивые:

- $\emptyset$
- $A \vee \neg A$

Противоречивые:

- $A \& \neg A$

Примечание. Непротиворечивое множество замкнутых(не имеющая сводных перменных) бескванторных формул

Пример. $\{A\}, \{0 = 0\}$

Определение. Моделью для непротиворечивого множества замкнутых бескванторных формул Γ — такая модель, что каждая формула из Γ оценивается в И

Определение. Полное непротиворечивое замкнутых бескванторных формул — такое, что для каждой замкнутой бескванторной формулы α: либо $\alpha \in \Gamma$, либо $\neg\alpha \in \Gamma$

Обозначение. **з.б.** — замкнутая бескванторная. **непр. мн** — непротиворечивое множество

Теорема 7.1.1. Если Γ — непротиворечивое множество з.б. фомул и α — з.б. формула.
То либо $\Gamma \cup \{\alpha\}$, либо $\Gamma \cup \{\neg\alpha\}$ — непр. мн. з.б. формул

Доказательство. Пусть и $\Gamma \cup \{\alpha\}$ и $\Gamma \cup \{\neg\alpha\}$ Доделать □

Теорема 7.1.2. Если Γ — непр. мн. з.б. фомул, то можно построить Δ — полное непр. мн. з.б. формул. $\Gamma \subseteq \Delta$ и в языке — счетное количество формул

$\varphi_1, \varphi_2, \varphi_3, \ldots$ — формулы з.б.

- $\Gamma_0 = \Gamma$
- $\Gamma_1 = \Gamma_0 \cup \{\varphi_1\}$ либо $\Gamma_0 \cup \{\neg\varphi_1\}$ — смотря что непротиворечивое
- $\Gamma_2 = \Gamma_1 \cup \{\varphi_2\}$ либо $\Gamma_1 \cup \{\neg\varphi_2\}$

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

Свойство 2. Γ^* *— полное*

Свойство 3. Γ^* *— непрерывное*

Доказательство. Пусть $\Gamma^* \vdash \beta \& \neg\beta$
Конечное доказательство $\gamma_1, \ldots \gamma_n$, часть из которых гипотезы: $\gamma_1, \ldots, \gamma_k$
$\gamma_i \in \Gamma_{R_i}$. Возьмем $\Gamma_{\max R_i}$. Правда ли $\Gamma_{\max R_i} \vdash B \& \neg B$ □

Теорема 7.1.3. Любое полное непротиворечивое множество замкнутых бескванторных формул Γ имеет модель, т.е. существует оценка $[\![]\!]$: если $\gamma \in \Gamma$, то $[\![\gamma]\!] = \text{И}$

Доказательство. D — все записи из функциональных символов.

- $[\![f_0^n]\!]$ — константа $\Rightarrow$ "f_0^n"
- $[\![f_k^m(\Theta_1, \ldots, \Theta_k)]\!] \Rightarrow$ "f_k^m(" $+ [\![\Theta_1]\!] +$ "," $+ \cdots +$ "," $+ [\![\Theta_k]\!] +$ ")"
- $[\![P(\Theta_1, \ldots, \Theta_n)]\!] = \begin{cases} \text{И} & P(\Theta_1, \ldots, \Theta_n) \in \Gamma \\ \text{Л} & \text{иначе} \end{cases}$
- свободные переменные: $\emptyset$

Так построенные модель — модель для Γ. Индукция по количеству связок.
База очев.
Переход $\alpha\&\beta$. При этом

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

Аналогично для других операций □

Теорема 7.1.4 (Геделя о полноте)**.** Если Γ — полное неротиворечивое множество замкнутых(не бескванторных) фомул, то оно имеет модель

Следствие 7.1.4.1. Пусть $\vDash \alpha$, тогда $\vdash \alpha$

Доказательство. Пусть $\vDash \alpha$, но $\nvdash \alpha$. Значит $\{\neg\alpha\}$ — непротиворечивое множество замкнутых формул. Тогда $\{\alpha\}$ или $\{\neg\alpha\}$ — непр. мн. з. ф. Пусть $\{\alpha\}$ — непр. мн. з.ф., а $\{\neg\alpha\}$ — противоречивое. При этом $\neg\alpha \vdash \beta\&\neg\beta$, $\neg\alpha \vdash \alpha$, $\beta\&\neg\beta \vDash \alpha$. $\neg\alpha \vdash \alpha$, $\alpha \vdash \alpha$. Значит $\vdash \alpha$ □

- Γ — п.м.з.ф.
- перестроим Γ в $\Gamma^\triangle$ — п.н.м. **б.** з. ф.
- по теореме о существование модели: $M^\triangle$ — модель для $F^\triangle$
- покажем, что $M^\triangle$ — модель для $\Gamma - M$

$\Gamma_0 = \Gamma$, где все формулы — в предварительной нормальной форме

Определение. ПНФ — формула, где $\forall\exists\forall\ldots(\tau)$, τ — формула без кванторов

Теорема 7.1.5. Если φ — формула, то существует ψ — в п.ф., то $\varphi \to \psi$ и $\psi \to \varphi$

Доказательство. $\Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_1 \subseteq \cdots \subseteq \Gamma^*$. $\Gamma^* = \bigcup_i \Gamma_i$
Переход: $\Gamma_i \to \Gamma_{i+1}$
Рассмторим: $\varphi_j \in \Gamma_i$
Построим семейство ф.с. d_i^j — новые перменные

1. φ_j без кванторов — не трогаем
2. $\varphi_j \equiv \forall x.\psi$ — добавим все формулы вида $\psi[x := \Theta]$, где Θ – терм, состоящий из f: $d_0^e, d_1^{e'} \ldots, d_{i-1}^{e'\cdots'}$
3. $\varphi_j \equiv \exists x.\psi$ — добавим $\psi[x := d_i^j]$

$\Gamma_{i+1} = \Gamma_i \cup \{$все добавленные формулы$\}$ — счетное количество □

Теорема 7.1.6. Если Γ_i — непротиворечиво, то Γ_{i+1} — непротиворечиво

Теорема 7.1.7. $\Gamma*$ — непротиворечиво

Следствие 7.1.7.2. $\Gamma^\triangle = \Gamma*$ без формул с $\forall, \exists$

Лекция 8

9 апреля

8.1 Исчесление предиктов

Теорема 8.1.1 (Геделя о полноте ИП)**.** У любого н.м.з.ф. (непротиворечивого множества замкнутых формул) ИП существует модель

Теорема 8.1.2. Если формула ϕ — замкнутая формула ИП
Тогда найдется ψ — замкнутая формула ИП, что $\vdash \varphi \to \psi$ и $\psi \to \varphi$. ψ — с поверхностными кванторами

Доказательство. См. ДЗ □

Примечание. Рассмотрим Γ — н.м.з.ф. — рассмотрим Γ' — полное расширение Γ. Пусть φ — фомула из Γ', тогда найдется $\psi in \Gamma'$, что ψ — с поверхностными кванторами и $\vdash \varphi \to \psi, \vdash \psi \to \varphi$

Доказательство теоремы Геделя о полноте ИП. Рассмотрим множество констант(нуль местных функциональных символов) — d_j^i. Построим $\{\Gamma_j\}$:

$$\Gamma' = \Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma 2 \subseteq \dots \subseteq \Gamma_j \subseteq \dots$$

Переход $\Gamma_j \Rightarrow \Gamma_{j+1}$: рассмторим все формулы из Γ_j: $\{\gamma_1, \gamma_2, \gamma_3, \dots\}$

1. γ_i — формула без кванторов — оставим на месте
2. $\gamma_i \equiv \forall x.\varphi$ — добваим к Γ_{j+1} все формулы вида $\varphi[x := \Theta]$, где Θ — составлен из всех ф.с. ИП и констант вида $d_1^k, \dots, d_j^k$
3. $\gamma_i \equiv \exists x.\varphi$ — добавим одну формулу — $\varphi[x := d_{j+1}^i]$

Утв. 1 $Gamma_{i+1}$ непр., если Γ_i — непр.
Докажем от противного. $\Gamma_{i+1} \vdash \beta \& \neg\beta$

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

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

γ_i — замкнутое $\implies$ т. о дедукции. Докажем что $\Gamma_i \vdash \beta\&\neg\beta$ по индукции.

$$\Gamma_i \vdash \gamma \to \varepsilon$$

Покажем $\Gamma_i \vdash \varepsilon$, т.е. γ получен из $\forall x.\xi$ или $\forall x.\xi \in \Gamma_i$

($\forall x.\xi$) Заметим, что $\Gamma_i \vdash \forall x.\xi$

$$\begin{array}{ll}
\vdots & \text{по условию} \\
\gamma \to \varepsilon & \text{по построению } \Gamma_{i+1} \\
\forall x.\xi \to (\underbrace{\xi[x := \Theta]}_{\gamma}) & \text{(акс. 11)} \\
(\forall x.\xi) \to \varepsilon & \left|\begin{array}{l} \eta \to \xi \\ \xi \to \kappa \end{array}\right. \implies \eta \to \kappa \\
\forall x.\xi & \\
\varepsilon & \text{(M.P.)}
\end{array}$$

($\exists x.\xi$)

$$\Gamma_i \vdash \overbrace{\xi[x := d^k_{i+1}]}^{\gamma} \to \varepsilon$$

Заметим, что d^k_{i+1} не входит в ε. Заменим все d^k_{i+1} в доказательстве на y — новая перменная

$$\Gamma_i \vdash \xi[x := y] \to \varepsilon$$

$$\begin{array}{l}
\exists y.\xi[x := y] \to \varepsilon \\
(\exists x.\xi x) \to (\exists t.\xi[x := y]) \\
(\exists x.\xi) \to \varepsilon \\
\exists x.\xi
\end{array}$$

$\boxed{\text{Исправить}}$

Утв. 2 Γ^* — непр. $\Gamma_0 \vdash \gamma_1 \to \dots \to \gamma_n \to \beta\&\neg\beta$

$$\Gamma_{\max_i(0..n)} \vdash \beta\&\neg\beta$$

Значит $\Gamma_{\max}$ — противоречиво, $\Gamma^\triangle = \Gamma^*$ без кванторов
<u>Значит</u> у $\Gamma^\triangle$ есть модель M

Утв. 3 $\gamma \in \Gamma'$, то $[\![\gamma]\!]_M = $ И
Индукция по количеству кванторов в γ. Рассмторим:

1. $\gamma \equiv \forall x.\delta$
   $[\![\forall x.\delta]\!]$, если $[\![\delta]\!]^{x:=\kappa} =$ И$, \kappa \in D$. Рассмотри $[\![\delta]\!]^{x:=\kappa}$, $k \in D$. κ содержит константы и ф-с, κ осмысленно Γ_p. δ добавлена на шаге q. Рассмотрим шаг $\Gamma_{\max(p,q)}$ $\forall x.\delta : \Gamma_{\max(p,q)+1}$ добавлена $\delta[x := \kappa]$. $\delta[x := \kappa]$ — меньше на 1 квантор, $[\![\delta[x := k]]\!] =$ И

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

□

Теорема 8.1.3. ИП неразрешимо

Определение. Язык — множество слов. Язык $\mathcal{L}$ разрешим, если существует A — алгоритм, что по слову w:
$A(w)$ — останавливается в '1', если $w \in \mathcal{L}$ и '0', если $w \notin \mathcal{L}$

Примечание. Проблема останова: не существует алгоритма, который по программе для машина Тьюринга ответит, остановится она или нет.
Пусть $\mathcal{L}'$ — язык всех останов программы для машины Тьюринга. $\mathcal{L}'$ неразрешим

Примечание. `[a, b, c, d, e] = cons(a, cons(b, cons(c, cons(d, cons(e, nil)))))`
A — алфавит ленты

$$\left.\begin{array}{l} S_x,\ x \in A \\ e - \text{nil} \end{array}\right\} - \text{0-местные функциональные символы}$$

$$C(a, b) - \text{2-местные функциональные символы}$$

$b_s, s \in \mathcal{S}$ — множество всех состояний, b_0 — начальное состояние.

$$C(s_c, C(s_b, C(s_a, e))) \quad C(s_d, C(s_e, e))$$

Заведем предикат, которых отвечает было ли состояние в процессе. Начальное состояние — машина Тьюринга запущена на строке α:

$$R(\alpha, e, b_0)$$

Переход:

$$(s_x, b_s) \to (s_y, b_t, \leftrightarrow)$$
$$(s_x, b_s) \to (s_y, b_t, \leftarrow)$$

Если пермещение законно, то можем построить для каждого такие правила:

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

$$\ldots R(z, C(s_y, w), b_t)$$

Сделаем коньюнкцию вех эти правил: $R(\ldots)\&R(\ldots)\&\ldots\&R(\ldots) \to \exists z.\exists.R(z, w, b_\triangle)$

$\boxed{\text{Исправить}}$

Пример.

1. $R(C(s_k, e), e, b_0)$ — доказуемо(мы так сказали) Двинем голвку вправо:

$$\forall x.\forall y.R(C(s_k, x), y, b_0) \to R(x, C(s_k, y), b_1)$$

Лекция 9

16 апреля

9.1 Теория первого порядка

Определение. **Теория I порядка** — Исчесление предикатов + нелогические функции + предикатные символы + нелогические (математические) аксиомы.

Определение. Будем говорить, что N соответсвует **аксиоматике Пеано** если:

- задан $(')$: $N \to N$ — инъективная функция (для разных элементов, разные значения)
- задан $0 \in N$: нет $a \in N$, что $a' = 0$
- если $P(x)$ — некоторое утверждение, зависящее от $x \in N$, такое, что $P(0)$ и всегда, когда $P(x)$, также и $P(x')$. Тогда $P(x)$

Свойство 1. 0 *единственный*

Доказательство. $P(x) = x = 0$ либо существует $t: \ t' = x$

- $P(0) : 0 = 0$
- $P(x) \to P(x')$. Заметим, что x' — не ‘ноль‘

$P(x)$ выполнено при всех $x \in N$ □

Определение.

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

Можем определить это опираясь на доказательтво

Определение. • $1 = 0'$

- $2 = 0''$
- $3 = 0'''$
- $4 = 0''''$
- ...

Задача 1. $2 + 2 = 4$

Решение.

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

Определение.

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

Определение.

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

Свойство 1. $a + 0 = 0 + a$

Доказательство. $P(a) = (a + 0 = 0 + a)$
<u>База</u> $P(0) : 0 + 0 = 0 + 0$
<u>Переход</u> $P(x) \to P(x')$

$$x + 0 = 0 + x$$

$$x' + 0 \stackrel{?}{=} 0 + x'$$

$$0 + x' = (0 + x)' \quad \text{определение} +$$

$$(0 + x)' = (x + 0)' \quad \text{предположение}$$

$$(x + 0)' = x' \quad \text{определение} +$$

$$x' = x' + 0 \quad \text{определение} +$$

□

Свойство 2. $a + b' = a' + b$

Доказательство.

$b = 0$ $a + 0' = a' + 0$

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

$b = c'$ Есть: $a + c' = a' + c$. Покажем: $a + c'' = a' + c'$

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

□

Свойство 3. $a + b = b + a$

Доказательство. База $b = 0$ — свойство
Переход $a + c'' = c'' + a$, если $a + c' = c' + a$

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

□

9.1.1 Формальная арифметика

Определение. Исчесление предикатов:

- Функциональные символы:
  - 0 — 0-местный
  - $(')$ — 1-местный
  - $(\cdot)$ — 2-местный
  - $(+)$ — 2-местный
- $(=)$ — 2-местный предикатный символ

Аксимомы:

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 аксиом индукции:

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

x входит свободно в ψ

Свойство 1.
$$((a + 0 = a) \to (a + 0 = a) \to (a = a))$$

Доказательство.

$$\forall a.\forall b.\forall c.a = b \to a = c \to b = c$$

$$(\forall a.\forall b.\forall c.a = b \to a = c \to b = c) \to \forall b.\forall c.(a + 0 = b \to a + 0 = c \to b = c)$$

$$\forall b.\forall c.a + 0 = b \to a + 0 = c \to b = c$$

$$(\forall b.\forall c.a + 0 = b \to a + 0 = c \to b = c) \to \forall c.(a + 0 = a \to a + 0 = c \to a = c)$$

$$\forall c.a + 0 = a \to a + 0 = c \to a = c$$

$$(\forall c.a + 0 = a \to a + 0 = c \to a = c) \to a + 0 = a \to a + 0 = a \to a = a$$

$$a + 0 = a \to a + 0 = a \to a = a$$

$$a + 0 = a$$

$$a + 0 = a \to a = a$$

$$a = a$$

$$\forall b.\forall c.a = b \to a = c \to b = c$$

$$(0 = 0 \to 0 = 0 \to 0 = 0)$$

$$(\forall b.\forall c.a = b \to a = c\ tob = c) \to (0 = 0 \to 0 = 0 \to 0 = 0) \to \phi$$

Исправить ☐

Определение. $\exists!x.\varphi(x) \equiv (\exists x.\varphi(x))\&\forall p.\forall q.\varphi(p)\&\varphi(q) \to p = q$
Можно также записать $\exists!x.\neg\exists s.s' = x$ или $(\forall q.(\exists x.x' = q) \lor q = 0)$

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

Определение.

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

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

Определение. $W \subseteq \mathbb{N}_0^n$. W — выразимое в формальной арифметике. отношение, если существует формула ω со свободными переменными $x_1, \dots, x_n$. Пусть $k_1, \dots, k_n \in \mathbb{N}$

- $(k_1, \dots, k_n) \in W$, тогда $\vdash \omega[x_1 := \overline{k_1}, \dots, x_n := \overline{k_n}]$
- $(k_1, \dots, k_n) \notin W$, тогда $\vdash \neg\omega[x_1 := \overline{k_1}, \dots, x_n := \overline{k_n}]$

$$\omega[x_1 := \Theta_1, \dots, x_n := \Theta_n] \equiv \omega(\Theta_1, \dots, \Theta_n)$$

Определение. $f : \mathbb{N}^n \to \mathbb{N}$ — представим в формальной арифметике, если найдется φ — фомула с $n + 1$ свободными переменными $k_1, \dots, k_{n+1} \in \mathbb{N}$

- $f(k_1, \dots, k_n) = k_{n+1}$, то $\vdash \varphi(\overline{k_1}, \dots, \overline{k_{n+1}})$

- $\vdash \exists!x.\varphi(\overline{k_1}, \dots, \overline{k_n}, x)$