Лекции по Математической логике 4 семестр

Ilya Yaroshevskiy

13 мая 2023 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 $(\alpha \to \beta), (\alpha \& \beta), (\alpha \vee \beta), (\neg \alpha)$ — высказывания

1.1.2 Мета и предметные

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

Метавыражение: $\alpha \to \beta$
Предметное выражение: $A \to (A \to A)$ (заменили α на A, β на $(A \to A)$)
Пример. Черным — предметные выражения, Синим — метавыражения

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

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

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

1.1.3 Сокращение записи

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

Пример. Расставление скобок

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

1.1.4 Теория моделей

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

1. $[\![x]\!] : \mathcal{P} \to V$ — 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 $\star \in [\&, \vee, \neg, \to]$

   Пример.

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

   Также можно записать так:

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

   , где $f_\to$ определена так:

a	b	$f_\to$
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. $\neg\neg\alpha \to \alpha$

1.1.6 Правило Modus Ponens и доказательство

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

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

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

Пример. $\vdash A \rightarrow A$

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

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

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

Лекция 2

Обозначение. Γ, Δ, Σ — списки высказываний

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

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

Пример. $\models \alpha$ — α общезначимо

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

Определение. Исчисление полно, если при любом α из $\models \alpha$ 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 $\delta_1, \ldots, \delta_n$, где $\delta_n = \alpha \to \beta$
Построим новое доказательство: $\delta_1, \ldots, \delta_n, \alpha$(гипотеза)$, \beta$(М.Р.)
Эта новая последовательность — доказательство $\Gamma, \alpha \vdash \beta$

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

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

Утвреждение: последовательность $\sigma_1, \ldots, \sigma_n$ 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 $\sigma_0, \ldots, \sigma_n$ — 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. $\delta_k \equiv \delta_l \to \delta_{n+1},\ k, l \leq n$

Докажем каждый из трех вариантов

1.

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

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

3.

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

□

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

Доказательство. Индукция по длине доказательства: каждая $[\![\delta_i]\!] = \text{И}$, если $\delta_1, \ldots, \delta_k$ — доказательство α
Пусть $[\![\delta_1]\!] = \text{И}, \ldots, [\![\delta_n]\!] = \text{И}$. 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 $\alpha \equiv A, \beta \equiv B$
   $[\![\alpha \to \beta \to \alpha]\!]^{[\![\alpha]\!]:=a, [\![\beta]\!]:=b} = \text{И}$

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

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

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

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

□

Теорема 2.0.3 (о полноте)**.** Пусть $\vDash \alpha$, 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: $P_1, \dots, P_n$
Рассмотрим $[\![\alpha]\!]^{P_1:=x_1,\dots P_n:=x_n} = $ И. Докажем, что $\underbrace{[x_1]^{P_1}, \dots, [x_n]^{P_n}}_{\Delta} \vdash [\alpha]^\alpha$.

Индукция по длине формулы (по структуре)
База: $\alpha \equiv P_i$ $[P_i]^{P_i} \vdash [P_i]^{P_i}$
Переход: 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: $\vDash \alpha$, т.е. $[x_1]^{P_1}, \dots, [x_n]^{P_n} \vdash [\alpha]^\alpha$. Но $[\![\alpha]\!] = $ И при любой оценке, т.е. $[x_1]^{P_1}, \dots, [x_n]^{P_n} \vdash \alpha$ при всех x_i

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

□

Лемма 1.

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

Тогда $\Gamma \vdash \zeta$

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

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 нет, то ОК
- Если да, 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 $\rightarrow$

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \rightarrow \psi}$$

- Удаление $\rightarrow$

$$\frac{\Gamma \vdash \varphi \rightarrow \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi}$$

- 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.

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

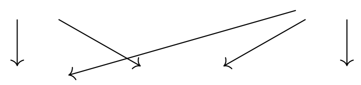
Пример. Докажем $\overline{\vdash A\&B \to B\&A}$

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

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

- $a \le b \vee b \le a$
- **Наименьший элемент** S — такой $k \in S$, что если $x \in S$, то $k \le x$
- **Минимальный элемент** S — такой $k \in S$, что нет $x \in S$, что $x \le k$

Пример.



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

Определение.

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

Определение.

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

Определение. Решетка $= \langle A, \le \rangle$ — 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 $a \cdot (b + c) = a \cdot b + a \cdot c$

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

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

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.

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

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

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

Определение. 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. $\emptyset, X \in \Omega$

Определение.

$$(X)^\circ = \text{наиб.}\{w \big| w \subseteq X, w \text{ — откр.}\}$$

Пример. Дискретная топология: $\Omega = 2^X$ — любое множество открыто. Тогда $\langle \Omega, \leq \rangle$ — булева алгебра

Теорема 3.1.3.

- $a + b = a \cup b$
- $a \cdot b = a \cap b$
- $a \to b = ((X \setminus a) \cup b)^\circ$
- $a \leq b$ 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
- $X/_\approx = \{[\alpha]_\approx \big| \alpha \in X\}$

$\langle X/_\approx, \leq \rangle$ — алгебра Гейтинга

Свойство 1. *$\langle X/_\approx, \leq \rangle$ — алгебра Линденбаума, где $X, \approx$ — из интуиционистской логики*

Теорема 3.1.4. Алгебра Гейтинга — полная модель ИИВ

Лекция 4

4.1 Упорядоченность

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 наименььшего
- $\mathbb{R}$ не имеет наименьшего

4.2 Табличные модели

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

- V — множество истинностных значений
  $f_{\rightarrow}, f_{\&}, f_{V} : V^2 \rightarrow V,\ f_{\neg} : V \rightarrow V$
  Выделенные значения $T \in V$
  $[\![p_i]\!] \in V\ f_{\mathcal{P}} : p_i \rightarrow V$
- $[\![p_i]\!] = f_{\mathcal{P}}(p_i)$
  $[\![\alpha \star \beta]\!] = f_{\star}([\![\alpha]\!], [\![\beta]\!])$
  $[\![\neg\alpha]\!] = f_{\neg}([\![\alpha]\!])$

~~Если $\vdash \alpha$, то~~ $\models \alpha$ означает, что $[\![\alpha]\!] = T$, при любой $f_{\mathcal{P}}$

Определение. Конечная модель: модель где V — конечно

Теорема 4.2.1. У ИИВ не существует полной конечной табличной модели

4.3 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 $W_k \Vdash p$

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 $W_i \Vdash \alpha \rightarrow \beta$
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 4.3.1. 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 4.3.2. 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 $[\![\alpha]\!] = \{W_k | W_k \Vdash \alpha\}$

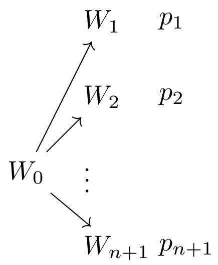
□

4.4 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

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

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

$$\nvdash \varphi_n$$

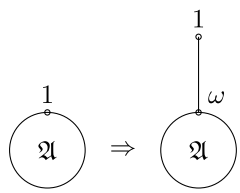
2. $\vDash_V \varphi_n$: по признаку Дирихле найдутся $i \ne j : [\![p_i]\!] = [\![p_j]\!]$
$[\![p_i \to p_j]\!] =$ И и $[\![\varphi_n]\!] =$ И
Значит $\vdash \varphi_n$ — противоречие

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 $1_{\Gamma(\mathfrak{A})}$ переименуем $1_{\mathfrak{A}}$ в ω

Теорема 4.4.1.

- $\Gamma(\mathfrak{A})$ — 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 4.4.2. $a \le b$, 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 согласована с f, g, если $\varphi(f(\alpha)) = g(\alpha)$

Теорема 4.4.3. 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 4.4.4. ИИВ дизъюнктивно

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

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

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

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 □

Лекция 5

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

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 *)
```

5.2 Исчисление предикатов

Определение. Язык исчисления предикатов

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

Θ — метаперменные для термов
Термы:

- Атомы:

  - $a, b, c, d, \dots$ — предметные переменные
  - x, y, z — метапеременные для предметных перменных

- Функциональные Символы
  - f, g, h — Функциональные символы(метаперемнные)
  - $f(\Theta_1, \dots \Theta_n)$ — применение функциональных символов

- Логические выражения:
  Если $n = 0$, будем писать f, g — без скобок
  - P — метаперменные для предикатных символов
  - A, B, C — предикатный символ
  - $P(\Theta_1, \dots, \Theta_n)$ — применение предикатных символов
  - $\&, \vee, \neg, \rightarrow$ — Связки
  - $\forall x.\varphi$ и $\exists x.\varphi$ — кванторы
    “<квантор> <переменная>.<выражение>“

5.2.1 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):

$$\forall a.B(A)\&\forall b.B(b)$$

5.2.2 Теория моделей

Оценка формулы в исчислении предикатов:

1. Фиксируем D — предметное множетво
2. Кажодму $f_i(x_1, \dots, x_n)$ сопоставим функцию $D^n \rightarrow D$
3. Каждому $P_j(x_1, \dots, x_m)$ сопоставим функцию(предикат) $D^2 \rightarrow V$
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.

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

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

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

5.2.3 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

6.1 Исчисление предикатов

6.1.1 Расставление скобок

Кванторы имеют наименьший приоритет

Пример.

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

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

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. $\alpha_1, \dots, \alpha_n$ — доказательство

- если α_i — аксимома
- либо существует $j, k < i$, что $\alpha_k = \alpha_j \to \alpha_i$
- либо существует $\alpha_j :\ \alpha_j = \varphi \to \psi$ 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.

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

1, 2, 3 — свободные, 5 — связанное, по перменённой 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 $x = 0 \to x = 0$

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

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

Пример.

(n) $x = 0 \to y = 0$ — откуда то

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

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

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 в доказательстве $\Gamma, \alpha \vdash \beta$ 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

- $\Gamma \vDash \alpha$ — 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.
<u>Тогда</u> $\Gamma \vdash \alpha$ 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 имеющих 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 $\square$

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

Определение. $\varphi_1, \varphi_2, \varphi_3, \dots$ — 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^* *— непротиворечивое*

Доказательство. Пусть $\Gamma^* \vdash \beta \& \neg\beta$
Конечное доказательство $\gamma_1, \dots \gamma_n$, часть из которых гипотезы: $\gamma_1, \dots, \gamma_k$
$\gamma_i \in \Gamma_{R_i}$. 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"
- $[\![f_k^m(\Theta_1, \dots, \Theta_k)]\!] \Rightarrow$ "f_k^m(" + $[\![\Theta_1]\!]$ + "," + $\dots$ + "," + $[\![\Theta_k]\!]$ + ")"
- $[\![P(\Theta_1, \dots, \Theta_n)]\!] = \begin{cases} \text{И} & P(\Theta_1, \dots, \Theta_n) \in \Gamma \\ \text{Л} & \text{иначе} \end{cases}$
- свободные переменные: $\emptyset$

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

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

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

Определение. Предваренная нормальная форма — формула, где $\forall\exists\forall\dots(\tau)$, 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. $\Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_1 \subseteq \dots \subseteq \Gamma^*$. $\Gamma^* = \bigcup_i \Gamma_i$
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: $d_0^e, d_1^{e'} \dots, d_{i-1}^{e'^{\dots'}}$
3. $\varphi_j \equiv \exists x.\psi$ — добавим $\psi[x := d_i^j]$

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

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

8.1 Исчисление 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^i_j. 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 $d^k_1, \dots, d^k_j$
3. $\gamma_i \equiv \exists x.\varphi$ — добавим одну формулу — $\varphi[x := d^i_{j+1}]$

Утв. 1 Γ_{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 $\Gamma_i \vdash \forall x.\xi$

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

$(\exists x.\xi)$

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

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

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

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

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
Значит у $\Gamma^{\triangle}$ есть модель M

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

1. $\gamma \equiv \forall x.\delta$
$[\![\forall x.\delta]\!]$, если $[\![\delta]\!]^{x:=\kappa} = \text{И}, \kappa \in D$. 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, $[\![\delta[x := k]]\!] = \text{И}$
2. $\gamma \equiv \exists x.\delta$ — аналогично

$\square$

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: $R(\ldots)\&R(\ldots)\&\ldots\&R(\ldots) \to \exists z.\exists.R(z, w, b_\triangle)$ 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

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. <u>База</u> $b = 0$ — свойство
<u>Переход</u> $a + c'' = c'' + a$, 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 $(\forall q.(\exists x.x' = q) \vee q = 0)$

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

Определение.

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

9.1.2 Выразимость отношений и представимость функций в формальной арифметике

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

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

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

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

- $f(k_1, \ldots, k_n) = k_{n+1}$, то $\vdash \varphi(\overline{k_1}, \ldots, \overline{k_{n+1}})$
- $\vdash \exists!x.\varphi(\overline{k_1}, \ldots, \overline{k_n}, x)$

Лекция 10

10.1 Рекурсивные функции

Определение. $f : \mathbb{N}^n \to \mathbb{N}$

1. $Z : \mathbb{N} \to \mathbb{N}$
   $Z(x) = 0$

2. $N : \mathbb{N} \to \mathbb{N}$
   $N(x) = x + 1$

3. $S_k : \mathbb{N}^m \to \mathbb{N}$

   - $f_1, \ldots, f_k : \ \mathbb{N}^m \to \mathbb{N}$
   - $g : \mathbb{N}^k \to \mathbb{N}$

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

   , где $\overline{x} = x_1, \ldots, x_m$

4. $P_k^l : \mathbb{N}^k \to \mathbb{N}$, $l \leq k$

   $$P_k^l(x_1, \ldots, x_k) = x_l$$

5. $R \langle f, g \rangle : \mathbb{N}^{m+1} \to \mathbb{N}$ — **примитивная рекурсия**

   - $f : \mathbb{N}^m \to \mathbb{N}$
   - $g : \mathbb{N}^{m+2} \to \mathbb{N}$

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

Пример.

$$R \langle f, g \rangle (0, x) = f(x)$$

$$R \langle f, g \rangle (1, x) = g(0, f(x), x)$$

$$R \langle f, g \rangle (2, x) = g(1, g(0, f(x), x), x)$$

Определение. $f : \mathbb{N}^m \to \mathbb{N}$ — **примитивно-рекурсивная**, если найдется g – выражение f через примитивы Z, N, S, P, R, т.е. $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$

Пример.

- $1 = S\langle N, Z\rangle$
- $(+2) = S\langle N, N\rangle$

$$S\left\langle \underset{g}{N}, \underset{f}{N}\right\rangle(x) = g(f(x)) = N(N(x)) = x + 2$$

- $(+3) = S\langle N, (+2)\rangle$
- $(\times 2)_a = R\left\langle P_1^1, S\left\langle N, P_3^2\right\rangle\right\rangle$

$$f(a, b) = \begin{cases} b & a = 0 \\ f(a-1, b+1) & a > 0 \end{cases}$$

— это почти определение $+$, т.е. $f(x, x) = x \cdot 2$

$$(\times 2)_a = \begin{cases} P_1^1(a) & y = 0 \\ b + 1 & y > 0 \end{cases} \boxed{\text{Исправить}}$$

, где a — счетчик, b — предыдущее значение, c — x

- $(\times 2) = S\left\langle (\times 2)_a, P_1^1, P_1^1\right\rangle$

Определение.

6. $M\langle f\rangle : \mathbb{N}^m \to \mathbb{N}$ — **минимизация**

   - $f : \mathbb{N}^{m+1} \to \mathbb{N}$

$$M\langle f\rangle(x_1, \ldots, x_m) = y$$

— минимальный y

$$f(y, x_1, \ldots, x_m) = 0$$

Если $f(y, x_1, \ldots, x_m) > 0$ при всех y, то результат не определен

Теорема 10.1.1. $(+), (\cdot), (x^y), (:), (\sqrt{\ }),$ деление с остатком — примитивно-рекурсивные функции

Лемма 6. *$p_1, p_2, \ldots$ — простые числа.*
$p(i) : \mathbb{N} \to \mathbb{N}$, $p(i) - p_i$ — примитивно-рекурсивная функция

Определение. $\operatorname{plog}_n k = \max t : n^t | k$ — примитивно-рекурсивная функция

Пример.

- $\operatorname{plog}_5 120 = 1$
- $\operatorname{plog}_2 120 = 3$

10.1.1 Функция Аккермана

$$A(m,n) = \begin{cases} n+1 & m = 0 \\ A(m-1,1) & m > 0,\ n = 0 \\ A(m-1, A(m,n-1)) & m > 0, n > 0 \end{cases}$$

Лемма 7. $A(m,n)$ — *не примитивно-рекурсивная*

Можно сказать что если есть текст длинны n, которые выводит текст длинны k, то текст длинны $n+1$ не может выводить текст больше чем k^k Исправить

10.2 Связь с формальной арифметикой

Теорема 10.2.1. f — рекурсивная функция, тогда f представима в формальной арифметике

Теорема 10.2.2. Если f представима в формальной арифметике, то она рекурсивна

Примечание.

- $\vdash \varphi$ — доказательство (φ) в ФА
- $\delta_1, \dots, \delta_n \equiv \varphi$ — доказательство
- C — функция(рекурсивная), превращающая доказательство в ФА

$$C(p,x) \begin{matrix} = 0 & \text{если доказательство корректно} \\ \neq 0 & \text{если не доказуемо} \end{matrix}$$

  , где p — запись доказательства, x — формула

- Формула $\delta(p,x,y)$ – доказательство

Доделать

Примечание. Проблема останова

$$P(p,x) = \begin{cases} 0, \text{если } p(x) \text{ останавливается} \\ 1, \text{если не останавливается} \end{cases}$$

$$Q(p,x) = \text{if } P(p,p) = 1 \text{ then } 0 \text{ else while true do;}$$

Теорема 10.2.3. Примитивы Z, N, S, P представимы в ФА

Доказательство. Аргументы: $x_1, \dots, x_n$

1. $Z(x) : \mathbb{N} \to \mathbb{N}$
$$\xi := x_1 = x_1 \& x_2 = 0$$
2. $N(x) : \mathbb{N} \to \mathbb{N}$
$$\nu := x_2 = x_1'$$

3. $P_k^l(x, \dots, x_k) : \mathbb{N}^k \to \mathbb{N}$

$$\pi_k^l \coloneqq x_1 = x_1 \& x_2 = x_2 \& \dots \& x_l = x_{k+1} \& \dots \& x_k = x_k$$

$$\left(\underset{i \neq l}{\&} x_i = x_i \right) \& x_l = x_{k+1}$$

4. $S \left\langle \underset{\gamma}{g}, \underset{\varphi_1}{f_1}, \dots, \underset{\varphi_k}{f_k} \right\rangle$

   - $(x_1, \dots, x_m) = x_{m+1}$

$$\exists r_1 . \exists r_2 . \dots \exists r_k . \varphi_1(x_1, \dots, x_m, r_1) \& \dots \& \varphi_k(x_1, \dots, x_m, r_k) \& \gamma(r_1, \dots, r_k, x_{m+1})$$

□

Определение. β-функция Геделя

$$\beta(b, c, i) = b \bmod (1 + c \cdot (i + 1))$$

Теорема 10.2.4.

- $a_0, a_1, \dots, a_k$ — некоторые значения $\in \mathbb{N}$

Тогда найдутся b и c, что

$$\beta(b, c, i) = a_i$$

Доказательство. Доделать □

Примечание. β-функция Геделя — представима в ФА

$$B(b, c, i, q) = (\exists p . b = p \cdot (q + c \cdot (1 + i)) + q) \& q < b$$

Примечание.

- $M \langle f \rangle$, $f : \mathbb{N}^{m+1} \to \mathbb{N}$

$$\varphi(x_{m+1}, x_1, \dots, x_m, \overline{0}) \& \forall y . y < x_{m+1} \to \neg \varphi(y, x_1, \dots, x_m, \overline{0})$$

  , где $(a < b) = (\exists n . a + n = b) \& \neg a = b$

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

$$\exists b . \exists c . \exists f . \varphi(x_1, \dots, x_n f) \& B(b, c, \overline{0}, f) \&$$

$$\& \forall y . y < x_{n+1} \to \exists r_y . B(b, c, y, r_y) \& \exists r_{y+1} . B(b, c, y + 1, r_{y+1}) \& \gamma(y, r_y, x_1, \dots, x_n, r_{y+1})$$

Лекция 11

11.1 Геделева нумерация

Определение. ($\ulcorner \bullet \urcorner$)

s	$\ulcorner s \urcorner$
(	3
)	5
,	7
&	9
$\vee$	11
$\neg$	13
$\rightarrow$	15
$\forall$	17
$\exists$	19
.	21
f_k^n	$23 + 6 \cdot 2^n \cdot 3^k$
P_k^n	$25 + 6 \cdot 2^n \cdot 3^k$
x_k	$27 + 6 \cdot 2^k$

Тогда известные функции будут:

- $(=) = P_0^2$
- $(0) = f_0^0$
- $(+) = f_0^2$
- $(\cdot) = f_1^2$
- $(') = f_0^1$

Определение. $\ulcorner a_0 a_1 \ldots a_{n-1} \urcorner = 2^{\ulcorner a_0 \urcorner} \cdot 3^{\ulcorner a_1 \urcorner} \cdot \ldots \cdot p_n^{\ulcorner a_{n-1} \urcorner}$

Определение. $S_0\ S_1\ S_2 = 2^{\ulcorner S_0 \urcorner} \cdot 3^{\ulcorner S_1 \urcorner} \cdot \ldots \cdot p_n^{\ulcorner S_n \urcorner}$

Примечание. p_i — i-е простое ($p_1 = 2$)

Пример. $\ulcorner a = 0 \urcorner = 2^{27+6} \cdot 3^{25+6\cdot 4} \cdot 5^{23+6}$

Теорема 11.1.1. Рассмотрим функцию $\mathrm{Proof}(x,p) = \begin{cases} 1 & \text{если } p \text{ — геделев номер доказательства } \chi \\ 0 & \text{иначе} \end{cases}$, Proof — рекурсивна

Теорема 11.1.2. Если функция представима в формальной арифметике, то она рекурсивна

Доказательство. $f : \mathbb{N}^n \to \mathbb{N}$, т.е. существует формула φ с $n+1$ свободными переменными $x_1, \dots, x_{n+1}$. Если $f(k_1, \dots, k_n) = k_{n+1}$
Ожидаем $\vdash \varphi(\overline{k_1}, \dots, \overline{k_n}, \overline{k_{n+1}})$, т.е. существует доказательство δ — последовательность $\delta_1, \dots, \delta_t$

$$\mathrm{Proof}(\ulcorner \varphi \overline{k_1}, \dots, \overline{k_{n+1}} \urcorner, \ulcorner k \urcorner) = 1$$

$$\begin{aligned}
&S\langle \mathrm{plog}_2, \\
&\quad M\langle S\langle \mathrm{Proof}, \\
&\quad\quad S\left\langle \mathrm{Subst}_{n+1}, \ulcorner \varphi \urcorner, P^2_{n+1}, P^3_{n+1}, \dots, P^{n+1}_{n+1}, S\left\langle \mathrm{plog}_2, P^1_{n+2} \right\rangle \right\rangle, \\
&\quad\quad S\left\langle \mathrm{plog}_3, P^1_{n+1} \right\rangle \\
&\quad \rangle \\
&\rangle
\end{aligned}$$

□

Примечание. Subst — функция которая подставляет аргументы в формулу

Примечание. χ — формула формальной арифметики

$$W_1(\ulcorner \chi \urcorner, \ulcorner p \urcorner) = \begin{cases} 0 & \text{если } p \text{ — доказательство } \chi[x_0 := \overline{\ulcorner \chi \urcorner}] \\ 1 & \text{иначе} \end{cases}$$

Реализация W_1 через Subst очевидна, тогда W_1 представима в формальной арифметике формулой ω_1. $\sigma(x) = \forall p. \neg \omega_1(x,p)$ — "самоприменение x недоказуемо"

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

Определение. ω-непротиворечивость. Теория ω-непротиворечива, если для любой формулы $\varphi(x)$:

- если $\vdash \varphi(\overline{0}), \vdash \varphi(\overline{1}), \dots$, то $\nvdash \exists x. \neg \varphi(x)$

Лемма 8. *Если теория ω-непротиворечива, то непротиворечива*

Доказательство. Рассмотрим $\varphi(x) := x = x$

$$\vdash \overline{0} = \overline{0} \quad \vdash \overline{1} = \overline{1} \quad \dots$$

Т.е. $\nvdash \exists x. x \neq x$ □

Теорема 11.1.3 (Геделя 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 — геделев номер доказательства

$$\vdash \sigma(\overline{\ulcorner\sigma\urcorner}) \quad \vdash \forall p.\neg\omega_1(\overline{\ulcorner\sigma\urcorner}, p)$$

   С другой стороны, $W_1(\ulcorner\sigma\urcorner, p) = 0$, т.е. $\vdash \omega_1(\overline{\ulcorner\sigma\urcorner}, p)$

2. Пусть $\vdash \neg\sigma(\overline{\ulcorner\sigma\urcorner})$

$$\vdash \exists p.\omega_1(\overline{\ulcorner\sigma\urcorner}, p)$$

$$\left.\begin{array}{c}\vdash \neg\omega_1(\overline{\ulcorner\sigma\urcorner}, \overline{0})\\ \vdash \neg\omega_1(\overline{\ulcorner\sigma\urcorner}, \overline{1})\\ \vdash \neg\omega_1(\overline{\ulcorner\sigma\urcorner}, \overline{2})\\ \vdots\end{array}\right\} \text{иначе} \vdash \sigma(\overline{\ulcorner\sigma\urcorner})$$

$$\nvdash \exists p.\omega_1(\overline{\ulcorner\sigma\urcorner}, p)$$

□

Следствие 11.1.3.3. Формальная арифметика со стандартной интерпретацией неполна

Доказательство. Доделать □

Теорема 11.1.4 (Геделя о неполноте арифметики №1 в форме Россера)**.**

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

ω_2 — формула соответствующая W_2

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

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

Доделать

Определение.

$$\text{Consis} \equiv \forall p.\neg\pi(\overline{\ulcorner 1 = 0\urcorner}, p)$$

π — формула соответствующая $Proof(x,p)$, т.е. p — доказательство x

Теорема 11.1.5 (Геделя о неполноте арифметики №2)**.**

$$\vdash \text{Consis} \to \sigma(\overline{\ulcorner\sigma\urcorner})$$

Т.е. если докажем, что если формальная арифметика непротиворечива, то автоматически $\sigma(\overline{\ulcorner\sigma\urcorner})$, т.е. ФА противоречива

Схема. Прочтем что написано в теореме: $\sigma(\overline{\ulcorner\sigma\urcorner})$ раскрывается в $\forall p.\neg\omega_1(\overline{\ulcorner\sigma\urcorner}, p)$, т.е. если формальная арифметика непротиворечива, то не существует p, который доказывает $\sigma(\overline{\ulcorner\sigma\urcorner})$, а это в точности утверждение теоремы Геделя о неполноте №1. Т.е. эта теорема — формализация теоремы Геделя о неполноте №1. □

Следствие 11.1.5.4. Никакая теория, содержащая формальную арифметику, не может доказать свою непротиворечивость

Лекция 12

12.1 Теория множеств

Определение. **Теория множеств** — теория первого порядка с нелогическим предикатом ‘принадлежность‘ ($\in$) и следующими аксиомами и схемами аксиом.

Определение. B – **бинарное отношение** на X: $B \subseteq X^2$

$$\langle a, b\rangle = \{\{a\}, \{a, b\}\}$$

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

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

Определение. $a \subseteq b$, если $\forall x.x \in a \to x \in b$

Примечание. Что такое равенство?

- Duck typing: принцип Лейбница (неразличимость) — $A = B$, если для любого $P \quad P(A) \leftrightarrow P(B)$
  $a \leftrightarrow b$, если $(a \to b)\&(b \to a)$
- Определение равенства как структур в C (принцип объемности) — A и B состоят из одинаковых элементов

Определение. $a = b$, если $a \subseteq b \& b \subseteq a$

Примечание. Пустое множество имеет тип 0, множество с одним элементов имеет тип 1 и т.д. Запретим запросы ‘принадлежит‘ на одинаковых типах

Определение. “Предикат“ $P(x)$ — множество $\{x \big| P(x)\}$

Аксиома 1 (равенства)**.** *Равные множества содержатся в одних и тех же множествах*

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

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

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

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

Аксиома 4 (объединения)**.** *Если x — непустое множество, то $\bigcup x$ — множество*

$$\forall x.(\exists y.y \in x) \to \exists p.\forall y.y \in p \leftrightarrow \exists s.y \in s \& s \in x$$

Пример.

$$\bigcup\{1, \{2, 3\}, \{\{4\}\}\} = 1 \cup \{2, 3, \{4\}\}$$

Почему $2 \in p$, потому что $2 \in \underbrace{\{2, 3\}}_{s}$, $\{2, 3\} \in x$

Аксиома 5 (Степени)**.** *Для множества x, существует $\mathcal{P}(x)$ — множество всех подмножеств*

$$\forall x.\exists p.\forall y.y \in p \leftrightarrow y \subseteq x$$

Пример.

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

$$\mathcal{P}(\{\{4\}\}) = \{\varnothing, \{\{4\}\}\}$$

Аксиома 6 (Схема аксиом выделения)**.** *Если a — множество, $\varphi(x)$ — формула, в которую не входит свободно b, то $\{x \big| x \in a \& \varphi(x)\}$ — множество*

$$\forall x.\exists b.\forall y.y \in b \leftrightarrow y \in x \& \varphi(y)$$

Аксиома 7 (Аксиома бесконечности)**.** *Существуют множества N, такие, что*

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

Теорема 12.1.1. Если x — множество, то $\{x\}$ — множество

$$\exists t.a \in t \leftrightarrow a = x$$

Доказательство.

- $x = \varnothing$, тогда $t \coloneqq \mathcal{P}(x)$, $\mathcal{P}(\varnothing) = \varnothing$
- $x \neq \varnothing$, тогда $s \coloneqq \{x, \varnothing\}$ — аксиома пары, $t \coloneqq \{z \big| z \in s \& z \neq \varnothing\}$

□

Теорема 12.1.2. a, b — множества, то $a \cup b$ — множество

Доказательство.

- $a = b$, тогда $a \cup b = a$ по теореме
- $a \neq b$, тогда $a \cup b = \bigcup\{a, b\}$ по аксиоме

$\square$

Обозначение. a, b — множества, $a \cup b =$ такое c

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

Определение. $a' = a \cup \{a\}$

Определение. **Ординальные числа**

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

Определение. Множество S **транзитивно**, если

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

Определение. Множество S **вполне упорядочено** отношением $\in$, если

1. $\forall a.\forall b.a \neq b \& a \in S \& b \in S \to a \in b \vee b \in a$ — линейный
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** (Ординальное число) — вполне упорядоченное отношением $\in$, транзитивное множество

Определение. **Предельный ординал** $s \neq \varnothing$ — ординал, не имеющий предшественника

$$\forall p.p' \neq s$$

Пример.

$$\omega = \{\varnothing, 1, 2, 3, 4, \dots\}$$

Очевидно, что $\omega \subseteq N$ (из аксиомы бесконечности)

Теорема 12.1.3. ω — множество

Определение.

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

Определение. $\sup t$ — минимальный ординал, содержащий все элементы из t

Пример. $\{0, 1, 3\}$ — ординал?

- упорядоченный
- <u>не транзитивный</u>

$\sup\{0, 1, 3\} = \{0, 1, 2, 3\}$

Пример.

$$1 + \omega = \sup_{c \in \omega}(1 + c) = \sup\{0 + 1, 1 + 1, 2 + 1, \dots\}$$

$$\sup\{1, 2, 3, 4, 5, \dots\} = \omega$$

Пример.

$$\omega + 1 = \omega' = \omega \cup \{\omega\} = \{0, 1, 2, 3, \dots, \omega\}$$

Лекция 13

13.1 Аксиома выбора

Аксиома 8.

- На любом семействе непустых множеств $\{A_S\}_{S\in\mathbb{S}}$ можно определить функцию $f : \mathbb{S} \to \bigcup_S A_S$, которая по множеству возвращает его элемент
- Любое множество можно вполне упорядочить
- Для любой сюрьективной функции $f : A \to B$, найдется частично обратная $g : B \to A$, $g(f(x)) = x$

Определение. Дизъюнктное семейство множество — семейство непересекающихся множеств

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

Определение. Прямое произведение дизъюнктного множества

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

Аксиома 8. Если $D(y) \& \forall t.t \in y \to t \neq \varnothing$, то $\bigtimes y \neq \varnothing$

Теорема 13.1.1 (Диаконеску)**.** Рассморим ZF(аксиоматика Цермело-Френкеля) поверх ИИП. Если добавим аксиому выбора то $\vdash \alpha \vee \neg\alpha$

13.2 Аксиома фундирования

Аксиома 9.

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

В каждом непустом множестве есть элемент, не пересекающийся с ним

13.3 Схема аксиом подстановки

ZFC — Zemelo-Frenkel Choice
Аксиома 10. S — множество, f — функция, то $f(S)$ — множество, т.е. существует формула $\varphi(x, y)$:

$$\forall x \in S.\exists! y.\varphi(x, y)$$

Пример.

$$f(x) = \begin{cases} x & p(x) \\ \varnothing & \neg p(x) \end{cases}$$

$$\{x \in S | p(x)\} = \cup f(S)$$

13.4 Мощность множества

Определение. Равномощность $|a| = |b|$, если существует биекция $a \to b$

Определение. Строго большая мощность $|a| > |b|$, если существует $f : b \to a$ — инъекция, но не биекция

Определение. Кардинальное число t — ординал x: для всех $y \in x$: $|y| \neq |x|$

Определение. Мощность множества $|x|$ — такое кардинальное число t, что $|t| = |x|$

Лемма 9. *a, b — кардиналы и $|a| = |b|$, то $a = b$*

Примечание.

- $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \dots$ — конечные кардиналы
- $\aleph_0 = |\omega|$
- $\aleph_1$ — следующий кардинал за $\aleph_0$

Теорема 13.4.1 (Кантора)**.** Рассмотрим S — множетво, $\mathcal{P}(S)$ — множество всех подмножеств
Тогда $|\mathcal{P}(S)| > |S|$

Теорема 13.4.2 (Кантора-Бернштейна)**.** Если a, b — множества, $f : a \to b$, $g : b \to a$ — инъективны
Тогда существует биекция $a \to b$

Лекция 14

14.1 Теорема Левенгейма-Сголема

Определение. Мощность модели

- D — предметное множество

Тогда $|D|$ — мощность модели

Определение. Пусть есть две модели M, M'. M' — **элементарная подмодель** M, если

- предметное множество $M' \subseteq$ предметное множество M
- пусть $\vDash_M \varphi$, тогда $\vDash_{M'} \varphi$
- Все функции и предикаты M' — сужение соответствующих функций и предикатов из M

Теорема 14.1.1. Пусть задана теория и модель M. Все ее формулы образуют множество T
Тогда для нее существует элементарная подмодель M'

$$|M'| = \max(|T|, \aleph_0)$$

Доказательство. $D_0 \subseteq D_1 \subseteq D_2 \subseteq \dots$ — предметные множества. $D_i \subseteq D$
$D' = \bigcup D_i$ — ?? предметное множество
Рассмотрим все формулы из T
Определим операцию преобразования D:

$$\varphi \in T \quad [\![\varphi(y, x_1, \dots x_k)]\!]_{y, x_i \in D_n} = \text{И}$$

Доделать ∎

Примечание. **"Парадокс" Сколема**
Известно, что:

1. вещественные числа + матан — счетно-аксиоматизированны
2. $|\mathbb{R}| > \aleph_0$ — внутри теории, на предметном языке
3. У вещественных чисел есть счетная модель $|\mathbb{R}| = \aleph_0$ — по теореме — вне теории, на метаязыке

14.2 Про ω

Определение.

$$a \cdot b = \begin{cases} 0 & b = 0 \\ a \cdot c + a & b = c' \\ \sup_{c \le b}\{a \cdot c\} & b \text{ — предельный} \end{cases}$$

Примечание.

$$\sup \omega = \omega$$
$$\cup\{\omega\} = \omega + 1$$

Пример. $\omega \cdot 1 < \omega \cdot 2$

$$\omega + \omega = \sup\{\omega + 0, \omega + 1, \omega + 2, \dots\}$$

Пример. $(a, b) > (c, d)$, если

1. $a > c$
2. $a = c, b > d$

$(a, b) \to \omega \cdot a + b$

1. $a > c \implies \omega \cdot a + b > \omega \cdot c + d$
2. $a = c, b > d \implies \omega \cdot a + b > \omega \cdot c + d$ Исправить

Пример.

$$\omega \cdot \omega = \sup\{\omega \cdot 0, \omega \cdot 1, \omega \cdot 2, \omega \cdot 3, \dots\}$$

Пример.

$$\omega^\omega = \sup\{\omega, \omega \cdot \omega, \omega \cdot \omega \cdot \omega, \dots\}$$

Пример. $\omega + 1$

```
record:
       i: integer,
       case i of
         0 : a: boolean;
         1 : b: integer
       end
end
```

Исправить

Пример. $\omega + \omega + 2$

```
record:
       i: integer,
       case i of
         0 : a: integer;
         1 : b: integer;
         2 : c: boolean;
       end
end
```