Лекции по Математической логике 4 семестр

Ilya Yaroshevskiy

19 марта 2021 г.

Оглавление

Лекция 1

TODO

Лекция 2

TODO

Лекция 3

TODO

Лекция 4

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

~~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 $\Omega = \{w \subseteq W |$если $W_i \in w,\ W_i \preceq W_j,$ 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 $[\![\alpha]\!] = \{W_k | W_k \Vdash \alpha\}$

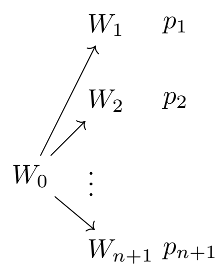
$\square$

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

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

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

$$\nvDash \varphi_n$$

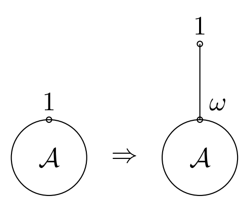
2. $\vDash_V \varphi_n$: по признаку Дирихле найдутся $i \ne j : [\![p_i]\!] = [\![p_j]\!]$
   $[\![p_i \to p_j]\!] =$ И и $[\![\varphi_n]\!] =$ И
   Значит $\vdash \varphi_n$ — противоречие

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 $\mathcal{A}$ — алгебра Гейтинга, тогда:

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



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

Теорема 4.3.1.

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

Определение. Гомоморфизм алгебр Гейтинга

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

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

Определение.

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

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

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

Теорема 4.3.4. ИИВ дизъюнктивно

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

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

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

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 $\varphi([\![\alpha]\!]) \neq 1_{\mathcal{L}}$ и $\varphi([\![\beta]\!]) \neq 1_{\mathcal{L}}$, т.е. $[\![\alpha]\!]_{\mathcal{L}} \neq 1_{\mathcal{L}}$ и $[\![\beta]\!]_{\mathcal{L}} \neq 1_{\mathcal{L}}$, тогда $[\![\alpha]\!]_{\Gamma(\mathcal{L})} \neq 1_{\Gamma(\mathcal{L})}$ и $[\![\beta]\!]_{\Gamma(\mathcal{L})} \neq 1_{\Gamma(\mathcal{L})} \Rightarrow$ Противоречие $\square$

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

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
  - $\&, \vee, \neg, \rightarrow$ — 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 $D^n \rightarrow D$

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.

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

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

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

5.1.3 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

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.

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

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

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.

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

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 1. *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 $\Gamma, \alpha \vdash \beta$

1. **TODO** Доказательсво