Математическая логика и теория алгоритмов

Сергей Григорян

27 ноября 2024 г.

Содержание

1 Лекция 10

1.1 Напоминание

σ - сигнатура, сост. из функц. и пред. символов. и им соотв. валентности.

$$\mu = (M, I_M), I_M \text{ - соотв. символам } \sigma \text{ функций и предикатов}$$

$$\pi\colon Var \to M$$

$$[\phi]_M(\pi) - ?$$

Рекурсия по постр.ϕ:

1)
$$\phi = P(t_1, \ldots, t_n)$$
$$[\phi]_M(\pi) = [P]_M([t_1]_M(\pi), \ldots, [t_n]_M(\pi))$$

2)
$$\phi = (\psi_0 \underset{\wedge,\vee,\to}{(operation)} \psi_1), \phi = \neg\psi \text{ - аналогично.}$$
$$[\phi]_M(\pi) = \underset{OR,IMPL}{AND}([\psi_0]_M(\pi), [\psi_1]_M(\pi))$$

3)
$$\phi = \exists x, \psi$$
$$[\phi]_M(\pi) = 1 \iff \text{ найдётся } a \in M, \text{ т. ч. } [\phi]_M(\pi_{x\to a}) = 1$$
$$[\phi]_M(\pi) = \bigvee_{a \in M} [\phi]_M(\pi_{x \mapsto a})$$
$$\pi_{x\to a}(y) = \begin{cases} \pi(y), y \neq x \\ a, y = x \end{cases}$$

4) Аналогично (3), но с $\bigwedge$ вместо $\bigvee$

<u>**Определение**</u> **1.1. Параметры** терма t:

1)
$$t = x \in Var \Rightarrow Par(t) = \{\, x \,\}$$

2)
$$t = c \text{ - константа из } \sigma \Rightarrow Par(t) = \emptyset$$

3)

$$t = f(t_1, \dots, t_n), f \text{ - функциональный символ вал-ти } n \Rightarrow Par(t) = \bigcup_{i=1}^{n} Par(t_i)$$

<u>**Определение**</u> **1.2.** Параметры формулы ϕ:

1)

$$\phi = P(t_1, \dots, t_n) \Rightarrow Par(\phi) = \bigcup_{i=1}^{n} Par(t_i)$$

2)

$$\phi = \neg\psi \Rightarrow Par(\phi) = Par(\psi)$$

3)

$$\phi = (\psi_0 \underset{\wedge,\vee,\to}{(operation)} \psi_1) \Rightarrow Par(\phi) = Par(\psi_0) \cup Par(\psi_1)$$

4)

$$\phi = (\exists/\forall)x, \psi \Rightarrow Par(\phi) = Par(\psi) \{ x \}$$

<u>**Теорема**</u> **1.1.** *a) Если π, π' — оценки и для любой пер. $x \in Par(t), \pi(x) = \pi'(x)$, то $[t]_M(\pi) = [t]_M(\pi')$*

b) Если π, π' - оценки, т. ч. для $\forall x \in Par(\phi), \pi(x) = \pi'(x)$ то $[\phi]_M(\pi) = [\phi]_M(\pi')$

Доказательство. a) Индукция по пост. t:

1)

$$t = x \Rightarrow [t]_M(\pi) = \pi(x) = \pi'(x) = [t]_M(\pi')$$

2)

$$t = c \Rightarrow [t]_M(\pi) = [c]_M = [t]_M(\pi')$$

3)

$$t = f(t_1, \dots, t_n), f \text{ — функциональный символ вал-ти } n$$

$$Par(t_i) \subset Par(t)$$

$$[t]_M(\pi) = [f]_M([t_1]_M(\pi), \dots, [t_n]_M(\pi)) =$$
$$= [f]_M([t_1]_M(\pi'), \dots, [t_n]_M(\pi')) = [t]_M(\pi')$$

b) Индукция по построению ϕ:

1) $\phi = P(t_1, \dots, t_n) \Rightarrow [\phi]_M(\pi) =$

$= [P]_M([t_1]_M(\pi), \dots, [t_n]_M[\pi]) = [P]_M([t_1]_M(\pi'), \dots, [t_n]_M(\pi')) = [\phi]_M(\pi'))$

2) $\phi = (\psi_0 \wedge \psi_1) \Rightarrow [\phi]_M[\pi] = AND([\psi_0]_M(\pi), [\psi_1]_M(\pi)]) = And([\psi_0]_M(\pi'), [\psi_1]_M(\pi')) = [\phi]_M(\pi')$ Аналогично для других операций и для отрицания.

3) $\phi = \exists x, \psi$

$$Par(\phi) = Par(\psi) \setminus \{ x \}$$

$[\phi]_M(\psi) = \bigvee_{a \in M} [\phi]_M(\pi_{x \mapsto a}) = \bigvee_{a \in M} [\phi]_M(\pi'_{x \mapsto a}) = [\phi]_M(\pi')$

4) $\phi = \forall x, \psi$ - аналогично 3)

□

2 Лекция 11

Определение 2.1. Предварённая нормальная формула :

$$\underbrace{\exists\forall\exists\exists\forall\dots}_{\text{Кванторы}} \underbrace{(\dots)}_{\text{Бескванторная формула}}$$

Теорема 2.1. *У любой ф-лы 1-ого порядка $\exists$ эквив. ей формула в предв. нормальной форме.*

Доказательство. Будем проводить эквив-ные преобразования:

1) $\neg\exists x\phi \sim \forall x\neg\phi$

$$\neg\forall x\phi \sim \exists x\neg\phi$$

2) $(\forall x\phi \wedge \forall x\psi) \sim \forall x(\phi \wedge \psi)$

$$(\exists x\phi \vee \exists x\psi) \sim \exists x(\phi \vee \psi)$$

3)

$$\exists x(\phi \wedge \psi) \to (\exists x\phi \wedge \exists x\psi)$$

Это не эквивалентность! Поэтому нельзя применять

$$(\forall x\phi \vee \forall x\psi) \to \forall x(\phi \vee \psi)$$

Нужно сделать замену переменной.

$$\exists x\phi \sim \exists y\underline{\phi(y/x)}$$

Получили ф-лу ϕ с подстановкой y вместо x.

$$\phi(y/x) \text{ — } \textbf{все свободные вхожд. } x \textbf{ замен-ся на } y$$

! При этом, эти вхождения не должны подпадать под д-ие кванторов по y, и y не входит свободно в ф-лу ϕ.
Рассм. примеры некорректных подстановок:

1) $\exists x\forall yA(x,y) \not\to \exists y\forall yA(y,y)$
2) $\exists xA(x,y) \not\to \exists yA(y,y)$

Иначе, замена на новую переменную корректна.

4) $(\exists x\phi) \wedge \psi \sim \exists x(\phi \wedge \psi)$, причём $x \notin Params(\psi)$

   $(\exists x\phi \wedge \psi) \sim \exists y\phi(y/x) \wedge \psi \sim \exists y(\phi(y/x) \wedge \psi)$, если $x \in Params(\psi)$, y не встречается в ϕ и ψ

   $\exists\phi \vee \psi \sim \exists x(\phi \vee \psi), \forall$ — аналог.

   $(\exists x\phi \to \psi) \sim \forall x(\phi \to \psi)$

   $(\psi \to \exists x\phi) \sim \exists x(\psi \to \phi)$

$\square$

Замечание. *Значение ф-лы зависит только от значения её параметров. $\Rightarrow$ Ф-ла с k пар-рами при фикс. интерпретации задаёт k-местный предикат.*

Определение 2.2. Предикат наз-ся **выразимым** в данной интерпретации, если его можно задать ф-лой 1-ого порядка.

Пример. $(\mathbb{N}, S, =), S(n) = n+1$. *Тогда:*

$$x = 0 \iff \neg\exists y\colon x = S(y)$$

$$x = 1 \iff \exists y\colon (x = S(y) \wedge \underbrace{y = 0}_{\text{Здесь подставляем строчку выше}})$$

Пример. $(\mathbb{N}, \cdot, =)$
$x = 0 \iff \forall y \cdot x = x$
$x = 1 \iff \forall y \cdot x = y$

$$x \vdots y \iff \exists z (x = y \cdot z)$$

$$p \text{ — \textit{простое}} \iff (p \neq 1 \wedge \forall q (p \vdots q \to (q = 1 \vee q = p)))$$
$$d = gcd(x, y) \iff (x \vdots d \wedge y \vdots d \wedge \forall k ((x \vdots k \wedge y \vdots k) \to d \vdots k))$$
$$d = lcm(x, y) \iff (c \vdots x \wedge c \vdots y \wedge \forall k ((k \vdots x \wedge k \vdots y) \to k \vdots c))$$

Пример. $(2^A, \subset)$
$$x = y \iff (x \subset y \wedge y \subset x)$$
$$x = \emptyset \iff \forall y \colon x \subset y$$
$$|x| = 1 \iff (\neg(x = \emptyset) \wedge \forall y (y \subset x \to (y = \emptyset \vee y = x)))$$
$$z = x \cup y \iff (x \subset z \wedge y \subset z \wedge \forall t ((x \subset t \wedge y \subset t) \to (z \subset t)))$$

Пример. *Метрическая геометрия:*

$(\mathbb{R}^2, E), E(x, y)$ — *значит, что* $|x - y| = 1$, *т. е. расстояние от точки* x *до* $y = 1$

$$x = y \iff \forall z (E(x, z) \to E(y, z))$$
$$|x - y| = 2 \iff \exists! z (E(x, z) \wedge E(y, z))$$

Или:
$$\exists z ((E(x, z) \wedge E(y, z)) \wedge \forall t ((E(x, t) \wedge E(y, t)) \to t = z))$$
$$|x - y| = \sqrt{3}$$

Рисуем прямоугольный треугольник с гипотенузой длины $= 2$ *и катетом длины* $= 1$. *Тогда катет от* x *до* y *имеет длину* $\sqrt{3}$

$$\exists z \exists t (E(x, z) \wedge E(z, t) \wedge E(x, t) \wedge E(y, t) \wedge |y - z| = 2)$$

Пример. $(\mathbb{N}, S, =)$
$$y = x + k, k \text{ — \textit{параметр}}$$
$$y = \underbrace{S(S(S(\ldots(S}_{k \text{ раз}}(x)))))$$
$$y = x + k \iff \exists z (y = z + \frac{k}{2} \wedge z = x + \frac{k}{2})$$

$$\iff \exists z \forall u \forall v \left(((u = y \land v = z) \lor (u = z \land v = x)) \to u = v + \frac{k}{2} \right)$$

$$len(k) = len(\frac{k}{2}) + C$$

$$k = 1 - \textit{база индукции}, y = x + 1 \iff y = S(x)$$

Общая длина: $C \log_2 k$

$$k - \textit{нечётно} \Rightarrow y = x + k \iff \exists z (y = S(z) + \frac{k-1}{2} \land z = x + \frac{k-1}{2})$$

3 Лекция 12

$$< \mathbb{Z}, S, = >$$

$$x = 0 \iff x + x = x$$

$$< \mathbb{N}, \cdot, = >$$

3.1 Метод автоморфизма

Аддитивная ф-ция:

$$f(x + y) = f(x) + f(y)$$

Лин. ф-ция:

$$f(\alpha \cdot x + \beta \cdot y) = \alpha f(x) + \beta f(y)$$

Мультипликативная ф-ция:

$$\phi(x \cdot y) = \phi(x) \cdot \phi(y)$$

Монотонная ф-ция:

$$x \leq y \iff f(x) \leq f(y)$$

Задана сигнатура $(P, \ldots, f, \ldots)$. Интерпретации с носит. A и B:

$$[P]_A, \ldots, [f]_A \text{ и } [P]_B, \ldots, [f]_B$$

$$\gamma \colon A \to B \text{ — гомоморфизм, если}$$

1) При всех $x_1, \ldots, x_k \in A$.

$$[P]_A(x_1, \ldots, x_k) \iff [P]_B(\gamma(x_1), \ldots, \gamma(x_k))$$

"Предикаты сохраняются"

2) При всех $x_1, \dots x_k \in A$:

$$\gamma([f]_A(x_1, \dots, x_k)) = [f]_B(\gamma(x_1), \dots, \gamma(x_k))$$

Для конст. симв.:

$$\gamma([c]_A) = [c]_B$$

Определение 3.1. Автоморфизм:

1) $A = B$

2) γ - биекция

Теорема 3.1 (Об автоморфизмах)**.** *Пусть A — интерпр. сигнатуры $(P, \dots, f, \dots)$, α — автоморфизм, Q — выразимый предикат. Тогда при всех $x_1, \dots, x_k \in A$:*

$$Q(x_1, \dots, x_k) \iff Q(\alpha(x_1), \dots, \alpha(x_k)) \qquad (1)$$

Сл-ие, если при некот-ром автоморфизме α эквиваленция (1) неверна, то Q невыразим:

Пример. $(\mathbb{Z}, S, =)$

$$\alpha(x = x + C)$$

$$Q(x) \iff x \vdots 2$$

Пример. $(\mathbb{Z}, +, =)$

$$\alpha(x) = -x$$

$$Q(x, y) \iff x > y$$

Пример.

$$n = 2^a \cdot 3^b \cdot k, k \not\vdots 2, k \not\vdots 3$$

$$\alpha(2^a \cdot 3^b \cdot k) = 2^b \cdot 3^a \cdot k$$

$$\alpha(0) = 0$$

$$Q(x, y) \iff x > y$$

Доказательство теоремы: Докажем индукцией по построению:

1) t — терм $\Rightarrow$ при всех $x_1, \dots, x_k \in A$:

$$[t](\alpha(x_1), \dots, \alpha(x_k)) = \alpha([t](x_1, \dots, x_k))$$

2) ϕ — ф-ла $\Rightarrow$ При всех $x_1, \dots, x_k \in A$:

$$[\phi](\alpha(x_1), \dots, \alpha(x_k)) \iff [\phi](x_1, \dots, x_k)$$

3) Переменная $\alpha(x) = \alpha(x)$, конст. символ $[c] = \alpha([c])$
Конст. символ: $[c] = \alpha([c])$
Сост. терм:

$$[f(t_1, \dots, t_m)](\alpha(x_1), \dots \alpha(x_k)) = [f]([t_1](\alpha(x_1), \dots, \alpha(x_k)), [t_m]) =$$

$$= [f](\alpha([t_1](x_1, \dots, x_k)), \dots, \alpha([t_m](x_1, \dots, x_k))) =$$
$$= \alpha([f]([t_1](x_1, \dots, x_k), [t_m](x_1, \dots, x_k))) =$$
$$= \alpha([f(t_1, \dots, t_m)](x_1, \dots, x_k))$$

Атом. формулы — аналогично термам

$$\bigwedge_y [\phi](\alpha(x_1), \dots, \alpha(x_k), y) = \bigwedge_y [\phi](\alpha(x_1), \dots, \alpha(x_k), \alpha(y)) =$$

$$= \bigwedge_y (x_1, \dots, x_k, y) = [\forall y, \phi](x_1, \dots, x_k)$$

$\square$

Пример.

$$< \mathbb{N}, S, => \text{ — нет автоморфизма, } \leq \text{ — невыраз.}$$

0 — *выразим:* $x = 0 \iff \neg\exists y \colon x = S(y)$

Следствие. *Выразим в* $< \mathbb{N}, S, => \iff$ *выразим в* $< \mathbb{N}, S, 0, =>$

Теорема 3.2 (Об элиминации кванторов). *Любая ф-ла в* $< \mathbb{N}, S, 0, =>$ *равна некот. бесквант. ф-ле*

Следствие. $x \leq y$ *не выраз. в* $< \mathbb{N}, S, =>$

Доказательство. $x \leq y$ выразима в $< \mathbb{N}, S, => \Rightarrow x \leq y$ выразима в $< \mathbb{N}, S, 0, =>$ бескванторной ф-лой, т. е. пропозиц. формулой, в к-рую, вместо переменных подставл. атомарн. формулы.
Ат. формулы:

$$S(S(\dots S(U))) = S(S(\dots S(v)))$$

$$u \text{ — переменная или } 0, v \text{ — тоже}$$

Значит $u = v + d, d \in \mathbb{Z}$ (ф-ла-комбинация кон. числа усл-ий)

$$d_1, \dots, d_n \text{ — все числа из усл.}$$

$$M = max\,\{\,d_1, \dots, d_n\,\} + 1$$

Рассм $x = m, y = 2M$ и $x = 2M, y = M$
Все атом. ф-лы, кроме тожд. истины, будут ложны $\Rightarrow$ комбинация приним. одинаковые значения:
Но $x \leq y$ верно для $x = M, y = 2M$ и неверно для $x = 2M, y = M \Rightarrow$ наша ф-ла не выр-ет $x \leq y$ □

Доказательство теоремы об элиминации. 1) Ат. ф-лы бескв.

2) $\phi \wedge \phi' \Rightarrow \neg\phi \wedge \neg\phi'$, аналог. для $\wedge, \vee, \rightarrow$

3) $\forall x \phi \sim \neg\exists x \neg\phi$

4) $\exists x \phi \sim \exists x \underset{\text{бескванторный}}{\phi'}$
Атомарные ф-лы, зависящие от x: $T, \perp, x = t_i$

□

4 Лекция 13

4.1 Элиминация кванторов

$< N, S, O, =>$, S - successor

Теорема 4.1. *Любая ф-ла в сигнатуре $(S, O, =)$ эквив-на в вышеуказанной интерпретации нек-рой бескванторной ф-ле.*
(Т. е. булевой комбинации атомарных формул.)

Доказательство. Инд-ция по построению ф-лы.

1) База: атомарная ф-лы — бескванторная

2) Переход:

   - $\phi = \neg\psi \Rightarrow$ по предположению индукции, $\psi \sim \psi', \psi'$ — бескванторная $\Rightarrow \phi \sim \neg\psi'$ — бесквант.
   - $\phi = (\psi \wedge \eta) \Rightarrow \psi \sim \psi', \eta \sim \eta', \phi \sim (\psi' \wedge \eta')$ — аналогично, $\vee, \rightarrow$
   -
   $$\forall x\phi \sim \neg\exists x\neg\phi$$

   В случае с $\exists x\phi$ нужны содержательные рассуждения, т. е. цель:

   $$\exists \mapsto \text{ конечная дизъюнкция}$$

   $$\exists x\phi \sim \exists x\phi', \phi' \text{ — бесквант.}$$

   Рассмотрим атомарные формулы:

   $$S(S(\ldots(S(u)))) = S(S(S(\ldots(S(v)))))$$

   u, v — либо переменные, либо 0

   $$u = v = x \Rightarrow \text{ф-ла } \perp \text{ или } T$$

   Рассм., что может быть в ϕ:

   $$S(S(\ldots(S(0)))) = x \text{ — задано значение } x$$

   $$S(S(\ldots(S(x)))) = 0 \text{ — тождественная ложь, т. к. } \mathbb{N}$$

   $$S(S(\ldots(S(y)))) = x, x = y + c$$

   $$S(S(\ldots(S(x)))) = y$$

   Итог: $\exists x\phi, \phi$ — бул. комбинация $\perp, T$ и равенств вида $x = d, x = y + c, x = y - c$, а также некот. кол-во $t_1, \ldots, t_k$ — все правые части. Опять же, рассм несколько случаев:

   I) $x \notin \{ t_1, \ldots, t_k \} \Rightarrow$ все рав-ва $x = t_i$ ложны $\Rightarrow \phi(x)$ не зависит от конкретного значения x.

   II) Иначе:

   $$\exists x\phi \sim \phi|_{\text{все } x = t_i \text{ ложны}} \vee \bigvee_i \phi[t_i/x]$$

Замечание. *Выражения с вычет. преобразуются, в сложение с другой части.*

□

Определение 4.1. Две интерпретации одной сигнатуры элемент. эквив., если в них верны один и те же ф-лы 1-ого порядка.

Теорема 4.2. $<\mathbb{R}, \leq>, <\mathbb{Q}, \leq>$ — *элементарно эквив-ны.*

Доказательство. В обеих интерпретациях верна теорема об элиминации кванторов, причём она происходит одинаково.
Отличие предыдущих в формуле $\exists x \phi$. Заменим ϕ на эквив. ДНФ.

$$x = y \iff (x \leq y \land y \leq x)$$

$$x < y \iff (x \leq y \land \neg(y \leq x))$$

$$\phi = C_1 \lor \ldots \lor C_k$$

где C_i — конъюнкция $x_j \leq y_j$ или $\neg(x_j \leq y_j)$:

$$(x_j \leq y_j) \mapsto (x_j < y_j) \lor (x_j = y_j)$$

$$\neg(x_j \leq y_j) \mapsto y_j < x_j$$

Рассмотрим по дистриб. $\Rightarrow \phi = C'_1 \lor \ldots \lor C'_m$
C'_i — конъюнкция ф-ул вида $x_j = y_j$ или $x_j < y_j$

$$\exists x \phi \sim \exists x (C'_1 \lor \ldots \lor C'_m) \sim \exists x C'_1 \lor \ldots \lor \exists x C'_m$$

$$\exists x((x > a_1) \land \ldots \land (x > a_o) \land (x < b_1) \land \ldots \land (x < b_q)) \land$$
$$\land (x = c_1) \land \ldots \land (x = c_r) \land (\text{возможно.}) \land x = x \land x < x \land y < z$$

Пример.

$$\exists x (x > a \land x > b \land x < c \land x < d) \iff a < c \land a < d \land b < c \land b < d$$

□

4.1.1 Игра Эренфойхтаsа

Теорема 4.3. *Интерпретации. элем. эквив-ны* $\Longleftrightarrow$

В некот-рой игре есть выигр. страт. у нек-рого игрока.

Правила: заданы 2 интерпретации A *и* B*, сигнат. которых сост. только из предикатных символов.* $(P_1, \ldots, P_n)$

2 игрока: новатор и консерватор

Цель новатора (Н): показать, что A *и* B *отличаются*

Цель консерватора (К): показать, что $A = b$

Подготовка: (Н) фиксир. число ходов m

На i*-ой стадии: отмечено* $a_1, \ldots, a_{i-1} \in A$*,* $b_1, \ldots, b_{i-1} \in B$

Н выбирает $a_i \in A$ *или* $b_i \in B$*,* K *отмечает. наоборот,* $b_i \in B$ *или* $a_i \in A$ *соотв.*

Итог игры:

P_j *— предикат вал-сти* l

$$P_j(a_{i_1}, \ldots a_{i_l}) \neq P_j(b_{i_1}, \ldots b_{i_l}) \Rightarrow \text{ выиграл } H$$

Пример. $< \mathbb{N}, \leq >, < \mathbb{Z}, \leq >$

$$\exists x \forall y, x \leq y \text{ — верно в } \mathbb{N}, \text{ но не в } \mathbb{Z}$$

Н выигравает за 2 хода:

1) $H : 0 \in \mathbb{N}, K : b \in \mathbb{Z}$

2) $H : (b-1) \in \mathbb{Z}, K : a \in \mathbb{N}$

Но $a \geq 0$ *— верно, а* $b - 1 \geq b$ *— ложно.*

Пример. $<\mathbb{Z}, \leq>, <\mathbb{Q}, \leq>$

$$\forall y \forall z (y < z \to \exists v (y < v < z))$$

Н выигрывает за 3 хода:

1) $H: 0 \in \mathbb{Z}, K: b_0 \in \mathbb{Q}$

2) $H: 1 \in \mathbb{Z}, K: b_1 \in \mathbb{Q}$

$$b_0 \geq b_1 \Rightarrow H \text{ — выиграл}$$

$$b_0 < b_1 \Rightarrow H: \frac{b_0 - b_1}{2}, K: a \in \mathbb{Z}, \text{ причём: } a \leq 0 \vee a \geq 1 \Rightarrow H \text{ — выиграл}$$

Пример. $<\mathbb{Q}, \leq>$ *и* $<\mathbb{R}, \leq>$
Выигрывает K, даже если не фиксировать число ходов.
Н ставит точку, либо совпадающую с уже выбранной, либо больше всех, либо меньше всех, либо внутри интервала.

Пример. $\mathbb{Z}$ *и* $\mathbb{Z} + \mathbb{Z}$
Заметим, что в $\mathbb{Z} + \mathbb{Z}$ есть есть беск. интервалы.
Поэтому выигр. K, если кол-во ходов фикс.
Разделим все интервалы на большие (бесконечные или кон. $\geq 2^l$, где l - число ходов до конца игры) и малые ($< 2^l$)
Новатор не может поделить большой интервал на два маленьких