

Математические методы верификации схем и программ

mk.cs.msu.ru → Лекционные курсы
→ Математические методы верификации схем и программ

Блок 2

Логика предикатов
(напоминание)

Лектор:
Подымов Владислав Васильевич
E-mail:
valdus@yandex.ru

ВМК МГУ, 2025/2026, осенний семестр

Сигнатура

Сигнатура логики предикатов $\langle Const, Func, Pred \rangle$ состоит из

- ▶ множества констант *Const*
- ▶ множества функциональных символов *Func*
(символов операций)
- ▶ множества предикатных символов *Pred*
(символов отношений)

Каждый функциональный и предикатный символ имеет вид $s^{(n)}$, где $n \in \mathbb{N} = \{1, 2, \dots\}$ — местность символа

Местность часто опускается в записи символа s

Var — счётное множество переменных

Термы и формулы

Форма Бэкуса-Наура (БНФ), задающая синтаксис термов (выражений) и формул (условий, или булевых выражений):

$$\begin{aligned} t &::= x \mid \mathbf{c} \mid \mathbf{f}(t_1, \dots, t_n), \\ \varphi &::= P(t_1, \dots, t_n) \mid (\neg \varphi) \mid (\varphi \& \varphi) \mid (\varphi \vee \varphi) \mid \\ &\quad (\varphi \rightarrow \varphi) \mid (\exists x \varphi) \mid (\forall x \varphi) \mid \mathbf{t} \mid \mathbf{f}, \end{aligned}$$

где φ — **формула**, $t, t_1, \dots, t_n$ — **термы**,
 $x \in \text{Var}$, $\mathbf{c} \in \text{Const}$ и $\mathbf{f}^{(n)} \in \text{Func}$, $P^{(n)} \in \text{Pred}$

Примеры

(сигнатура: $\langle \{\mathbf{3}\}, \{+^{(2)}, \cdot^{(2)}\}, \{=^{(2)}\} \rangle$)

- ▶ $x + \mathbf{3} \cdot y$ — терм в инфиксной записи
- ▶ $+(x, \cdot(\mathbf{3}, y))$ — терм в функциональной записи
- ▶ $x + \mathbf{3} \cdot y = \mathbf{2} + z$ — формула в инфиксной записи
- ▶ $=(+(x, \cdot(\mathbf{3}, y)), +(\mathbf{2}, z))$ — формула в функциональной записи

Term — множество всех термов (заданной сигнатуры)

Термы и формулы

Приоритеты логических операций в порядке убывания:

$\exists$, $\forall$ и $\neg$; затем $\&$; затем $\vee$; затем $\rightarrow$

Ещё немного формул:

$$\forall x \exists y (y = x + 1)$$

$$\exists x \forall y P(x, y) \rightarrow \forall y \exists x P(x, y)$$

Свободные и связанные переменные

Квантор **связывает** ту переменную, которая следует за ним

Область действия внешнего квантора

в формулах вида $\forall x \varphi$ и $\exists x \varphi$ — это подформула φ

Связанное вхождение переменной в формулу — это вхождение переменной в область действия квантора, связывающего эту переменную

Свободное вхождение переменной — это вхождение, не являющееся связанным

Свободная переменная формулы — это переменная, имеющая свободное вхождение в формулу

Пример:

$$\exists y (\forall x \neg P(y, f(x, y)) \rightarrow R(x))$$

Свободные и связанные переменные

Квантор **связывает** ту переменную, которая следует за ним

Область действия внешнего квантора

в формулах вида $\forall x \varphi$ и $\exists x \varphi$ — это подформула φ

Связанное вхождение переменной в формулу — это вхождение переменной в область действия квантора, связывающего эту переменную

Свободное вхождение переменной — это вхождение, не являющееся связанным

Свободная переменная формулы — это переменная, имеющая свободное вхождение в формулу

Пример:

$$\exists y (\forall x \neg P(y, f(x, y)) \rightarrow R(x))$$

Переменная y связана квантором $\exists$

Свободные и связанные переменные

Квантор **связывает** ту переменную, которая следует за ним

Область действия внешнего квантора

в формулах вида $\forall x \varphi$ и $\exists x \varphi$ — это подформула φ

Связанное вхождение переменной в формулу — это вхождение переменной в область действия квантора, связывающего эту переменную

Свободное вхождение переменной — это вхождение, не являющееся связанным

Свободная переменная формулы — это переменная, имеющая свободное вхождение в формулу

Пример:

$$\exists y (\forall x \neg P(y, f(x, y)) \rightarrow R(x))$$

Переменная **x** связана квантором $\forall$



Свободные и связанные переменные

Квантор **связывает** ту переменную, которая следует за ним

Область действия внешнего квантора

в формулах вида $\forall x \varphi$ и $\exists x \varphi$ — это подформула φ

Связанное вхождение переменной в формулу — это вхождение переменной в область действия квантора, связывающего эту переменную

Свободное вхождение переменной — это вхождение, не являющееся связанным

Свободная переменная формулы — это переменная, имеющая свободное вхождение в формулу

Пример:

$$\exists y (\forall x \neg P(y, f(x, y)) \rightarrow R(x))$$

Область действия квантора $\exists$

Свободные и связанные переменные

Квантор **связывает** ту переменную, которая следует за ним

Область действия внешнего квантора

в формулах вида $\forall x \varphi$ и $\exists x \varphi$ — это подформула φ

Связанное вхождение переменной в формулу — это вхождение переменной в область действия квантора, связывающего эту переменную

Свободное вхождение переменной — это вхождение, не являющееся связанным

Свободная переменная формулы — это переменная, имеющая свободное вхождение в формулу

Пример:

$$\exists y (\forall x \neg P(y, f(x, y)) \rightarrow R(x))$$

Область действия квантора $\forall$

Свободные и связанные переменные

Квантор **связывает** ту переменную, которая следует за ним

Область действия внешнего квантора

в формулах вида $\forall x \varphi$ и $\exists x \varphi$ — это подформула φ

Связанное вхождение переменной в формулу — это вхождение переменной в область действия квантора, связывающего эту переменную

Свободное вхождение переменной — это вхождение, не являющееся связанным

Свободная переменная формулы — это переменная, имеющая свободное вхождение в формулу

Пример:

$$\exists y (\forall x \neg P(y, f(x, y)) \rightarrow R(x))$$



Связанные вхождения переменной y

Свободные и связанные переменные

Квантор **связывает** ту переменную, которая следует за ним

Область действия внешнего квантора

в формулах вида $\forall x \varphi$ и $\exists x \varphi$ — это подформула φ

Связанное вхождение переменной в формулу — это вхождение переменной в область действия квантора, связывающего эту переменную

Свободное вхождение переменной — это вхождение, не являющееся связанным

Свободная переменная формулы — это переменная, имеющая свободное вхождение в формулу

Пример:

$$\exists y (\forall x \neg P(y, f(x, y)) \rightarrow R(x))$$

Связанное вхождение переменной x

Свободные и связанные переменные

Квантор **связывает** ту переменную, которая следует за ним

Область действия внешнего квантора

в формулах вида $\forall x \varphi$ и $\exists x \varphi$ — это подформула φ

Связанное вхождение переменной в формулу — это вхождение переменной в область действия квантора, связывающего эту переменную

Свободное вхождение переменной — это вхождение, не являющееся связанным

Свободная переменная формулы — это переменная, имеющая свободное вхождение в формулу

Пример:

$$\exists y (\forall x \neg P(y, f(x, y)) \rightarrow R(x))$$

Свободное вхождение переменной x



Интерпретации, выполнимость, истинность

Интерпретация (сигнатуры $\langle Const, Func, Pred \rangle$) состоит из

- ▶ предметной области D
 - ▶ (это произвольное непустое множество предметов, на котором задана интерпретация)
- ▶ оценки констант
 - ▶ оценка константы c — это предмет $\bar{c} \in D$
- ▶ оценки функциональных символов
 - ▶ оценка функционального символа $f^{(k)}$ — это функция $\bar{f} : D^k \rightarrow D$
- ▶ оценки предикатных символов
 - ▶ оценка предикатного символа $P^{(k)}$ — это предикат $\bar{P} : D^k \rightarrow \{\mathbf{t}, \mathbf{f}\}$

Интерпретации, выполнимость, истинность

Оценка переменных множества V , $V \subseteq \text{Var}$, в интерпретации на D — это отображение вида $\sigma : V \rightarrow D$

Связка оценки переменных — это запись вида x/d , где $x \in \text{Var}$ и $d \in D$

Связка x/d означает, что переменная x **оценивается** предметом d

Оценку σ переменных конечного множества $V = \{x_1, \dots, x_n\}$ можно представить в виде конечного множества связок, в котором вместо фигурных скобок обычно изображаются квадратные:

$$\sigma = [x_1/\sigma(x_1), \dots, x_n/\sigma(x_n)]$$

Записью $\sigma[x \leftarrow d]$, где $x \in \text{Var}$, $d \in D$ и σ — оценка переменных V , будем обозначать оценку переменных $V \cup \{x\}$, отличающуюся от σ только тем, что x оценивается предметом d :

- ▶ $\sigma[x \leftarrow d](x) = d$
- ▶ Для остальных переменных y верно $\sigma[x \leftarrow d](y) = \sigma(y)$

Интерпретации, выполнимость, истинность

Если все переменные терма t принадлежат множеству переменных V , то **значение терма** на оценке σ переменных V ($t\sigma$) в интерпретации $\mathcal{I}$ — это предмет, задающийся так:

- ▶ $c\sigma = \bar{c}$
- ▶ $x\sigma = \sigma(x)$
- ▶ $\mathbf{f}(t_1, \dots, t_n)\sigma = \bar{\mathbf{f}}(t_1\sigma, \dots, t_n\sigma)$

Например, если предметная область интерпретации $\mathcal{I}_{ar}$ — все целые числа ($\mathbb{Z}$) и все символы сигнатуры оцениваются естественно (будем называть такую интерпретацию **целочисленной арифметической**), то

$$\overline{2+2} \equiv 4$$

Интерпретации, выполнимость, истинность

Если все свободные переменные формулы φ принадлежат множеству переменных V , то **выполнимость** формулы φ в интерпретации $\mathcal{I}$ на оценке σ переменных V ($\mathcal{I} \models \varphi\sigma$) задаётся так:

- ▶ Обязательно верно $\mathcal{I} \models \mathbb{t}\sigma$ и $\mathcal{I} \not\models \mathbb{f}\sigma$
- ▶ $\mathcal{I} \models P(t_1, \dots, t_k)\sigma \Leftrightarrow \overline{P}(t_1\sigma, \dots, t_k\sigma) = \mathbb{t}$
- ▶ $\mathcal{I} \models (\neg\psi)\sigma \Leftrightarrow \mathcal{I} \not\models \psi\sigma$
- ▶ $\mathcal{I} \models (\psi_1 \& \psi_2)\sigma \Leftrightarrow \mathcal{I} \models \psi_1\sigma$ и $\mathcal{I} \models \psi_2\sigma$
- ▶ $\mathcal{I} \models (\psi_1 \vee \psi_2)\sigma \Leftrightarrow$ верно хотя бы одно из двух: $\mathcal{I} \models \psi_1\sigma$; $\mathcal{I} \models \psi_2\sigma$
- ▶ $\mathcal{I} \models (\psi_1 \rightarrow \psi_2)\sigma \Leftrightarrow \mathcal{I} \models (\neg\psi_1 \vee \psi_2)\sigma$
- ▶ $\mathcal{I} \models (\exists x \psi)\sigma \Leftrightarrow$ существует предмет d , такой что $\mathcal{I} \models \psi\sigma[x \leftarrow d]$
- ▶ $\mathcal{I} \models (\forall x \psi)\sigma \Leftrightarrow$ для любого предмета d верно $\mathcal{I} \models \psi\sigma[x \leftarrow d]$

Формула φ **истинна** в интерпретации $\mathcal{I}$ ($\mathcal{I} \models \varphi$), если для любой оценки σ свободных переменных формулы φ верно $\mathcal{I} \models \varphi\sigma$

Интерпретации, выполнимость, истинность

Примеры

$$\mathcal{I}_{ar} \models (x = x)[x/1]$$

$$\mathcal{I}_{ar} \models (x = x)[x/2, y/5]$$

$$\mathcal{I}_{ar} \models x = x$$

$$\mathcal{I}_{ar} \models (x = \mathbf{1})[x/1]$$

$$\mathcal{I}_{ar} \not\models (x = \mathbf{1})[x/2]$$

$$\mathcal{I}_{ar} \not\models x = \mathbf{1}$$

$$\mathcal{I}_{ar} \models (y = x + \mathbf{1})[x/3, y/4]$$

$$\mathcal{I}_{ar} \models \exists y (y = x + \mathbf{1})$$

$$\mathcal{I}_{ar} \models \forall x \exists y (y = x + \mathbf{1})$$

$$\mathcal{I}_{ar} \not\models \exists y (x = \mathbf{2} * y)$$

Подстановки

Подстановка — это отображение $\theta : \text{Var} \rightarrow \text{Term}$

Связка подстановки — это запись вида x/t , где $x \in \text{Var}$ и $t \in \text{Term}$

Связка x/t означает, что при применении подстановки на место x **подставляется** терм t

Область подстановки θ — это множество всех переменных x , для которых верно неравенство $\theta(x) \neq x$

Подстановка считается **конечной**, если конечна её область

Конечную подстановку θ с областью $V = \{x_1, \dots, x_n\}$ можно представить в виде конечного множества связок:

$$\theta = \{x_1/\theta(x_1), \dots, x_n/\theta(x_n)\}$$

Подстановки

$E\theta$ — это результат применения подстановки θ к выражению E , то есть выражение, получающееся из E заменой

- ▶ каждого вхождения каждой переменной x на соответствующий терм $\theta(x)$, если E — терм
- ▶ каждого свободного вхождения каждой свободной переменной x на соответствующий терм $\theta(x)$, если E — формула

Например,

$$\begin{aligned}(x + x * y * z)\{x/y, y/z + 2\} &\equiv y + y * (z + 2) * z \\(x = y \vee \exists x (x = y))\{x/1, y/2\} &\equiv 1 = 2 \vee \exists x (x = 2)\end{aligned}$$

Композиция подстановок θ и η — это подстановка $\theta\eta$, такая что для любой переменной x верно равенство

$$x(\theta\eta) = (x\theta)\eta$$

Например,

$$\{x/f(x, c), y/g(u), z/y\}\{x/g(y), y/z, u/c\} = \{x/f(g(y), c), y/g(c), u/c\}$$