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, 2023/2024, 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):

$$t \quad ::= \quad \mathrm{x} \;\mid\; \mathbf{c} \;\mid\; \mathbf{f}(t_1, \dots, t_n),$$

$$\varphi \quad ::= \quad \mathrm{P}(t_1, \dots, t_n) \;\mid\; (\neg\varphi) \;\mid\; (\varphi \,\&\, \varphi) \;\mid\; (\varphi \vee \varphi) \;\mid\; (\varphi \rightarrow \varphi) \;\mid\; (\exists \mathrm{x}\varphi) \;\mid\; (\forall \mathrm{x}\varphi) \;\mid\; \mathbb{t} \;\mid\; \mathbb{f},$$

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

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

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

Ещё немного формул:

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

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

Свободные и связанные переменные

Квантор связывает ту переменную, которая следует за ним

Область действия внешнего квантора
в формулах вида $\forall \mathrm{x}\ \varphi$ и $\exists \mathrm{x}\ \varphi$ — 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:

$$\exists \mathrm{y}(\forall \mathrm{x} \neg \mathrm{P}(\mathrm{y}, \mathbf{f}(\mathrm{x}, \mathrm{y})) \rightarrow \mathrm{R}(\mathrm{x}))$$

Свободные и связанные переменные

Квантор связывает ту переменную, которая следует за ним

Область действия внешнего квантора
в формулах вида $\forall \mathrm{x}\, \varphi$ и $\exists \mathrm{x}\, \varphi$ — 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:

$$\exists \mathrm{y}(\forall \mathrm{x} \neg \mathrm{P}(\mathrm{y}, \mathbf{f}(\mathrm{x}, \mathrm{y})) \to \mathrm{R}(\mathrm{x}))$$

Переменная y связана квантором $\exists$

Свободные и связанные переменные

Квантор связывает ту переменную, которая следует за ним

Область действия внешнего квантора
в формулах вида $\forall \mathrm{x}\ \varphi$ и $\exists \mathrm{x}\ \varphi$ — 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:

$$\exists \mathrm{y}(\forall \mathrm{x} \neg \mathrm{P}(\mathrm{y}, \mathbf{f}(\mathrm{x},\mathrm{y})) \to \mathrm{R}(\mathrm{x}))$$

Переменная x связана квантором $\forall$

Свободные и связанные переменные

Квантор связывает ту переменную, которая следует за ним

Область действия внешнего квантора
в формулах вида $\forall \mathrm{x}\, \varphi$ и $\exists \mathrm{x}\, \varphi$ — 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:

$$\exists \mathrm{y} \underbrace{(\forall \mathrm{x} \neg \mathrm{P}(\mathrm{y}, \mathbf{f}(\mathrm{x}, \mathrm{y})) \to \mathrm{R}(\mathrm{x}))}_{\text{Область действия квантора } \exists}$$

Свободные и связанные переменные

Квантор связывает ту переменную, которая следует за ним

Область действия внешнего квантора
в формулах вида $\forall \mathrm{x}\, \varphi$ и $\exists \mathrm{x}\, \varphi$ — 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:

$$\exists \mathrm{y}(\forall \mathrm{x} \underbrace{\neg \mathrm{P}(\mathrm{y}, \mathbf{f}(\mathrm{x}, \mathrm{y}))}_{\text{Область действия квантора } \forall} \to \mathrm{R}(\mathrm{x}))$$

Свободные и связанные переменные

Квантор связывает ту переменную, которая следует за ним

Область действия внешнего квантора
в формулах вида $\forall \mathrm{x}\, \varphi$ и $\exists \mathrm{x}\, \varphi$ — 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:

$$\exists \mathrm{y}(\forall \mathrm{x} \neg \mathrm{P}(\mathrm{y}, \mathbf{f}(\mathrm{x}, \mathrm{y})) \to \mathrm{R}(\mathrm{x}))$$

Связанные вхождения переменной y

Свободные и связанные переменные

Квантор связывает ту переменную, которая следует за ним

Область действия внешнего квантора
в формулах вида $\forall \mathrm{x}\, \varphi$ и $\exists \mathrm{x}\, \varphi$ — 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:

$$\exists \mathrm{y} (\forall \mathrm{x} \neg \mathrm{P}(\mathrm{y}, \mathbf{f}(\mathrm{x}, \mathrm{y})) \to \mathrm{R}(\mathrm{x}))$$

Связанное вхождение переменной x

Свободные и связанные переменные

Квантор связывает ту переменную, которая следует за ним

Область действия внешнего квантора
в формулах вида $\forall \mathrm{x}\ \varphi$ и $\exists \mathrm{x}\ \varphi$ — 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:

$$\exists \mathrm{y}(\forall \mathrm{x} \neg \mathrm{P}(\mathrm{y}, \mathbf{f}(\mathrm{x}, \mathrm{y})) \rightarrow \mathrm{R}(\mathrm{x}))$$

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 $\bar{\mathbf{c}} \in D$
- оценки функциональных символов
  - оценка функционального символа $\mathbf{f}^{(k)}$ — это функция $\bar{\mathbf{f}} : D^k \to D$
- оценки предикатных символов
  - оценка предикатного символа $\mathrm{P}^{(k)}$ — это предикат $\overline{\mathrm{P}} : D^k \to \{\mathbb{t}, \mathbb{f}\}$

Интерпретации, выполнимость, истинность

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

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

Связка $\mathtt{x}/d$ означает, что переменная $\mathtt{x}$ оценивается предметом d

Оценку σ переменных конечного множества $V = \{\mathtt{x}_1, \dots, \mathtt{x}_n\}$ можно представить в виде конечного множества связок, в котором вместо фигурных скобок обычно изображаются квадратные:

$$\sigma = [\mathtt{x}_1/\sigma(\mathtt{x}_1), \dots, \mathtt{x}_n/\sigma(\mathtt{x}_n)]$$

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

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

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:

- $\mathbf{c}\sigma = \overline{\mathbf{c}}$
- $\mathrm{x}\sigma = \sigma(\mathrm{x})$
- $\mathbf{f}(t_1, \ldots, t_n)\sigma = \overline{\mathbf{f}}(t_1\sigma, \ldots, t_n\sigma)$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Подстановки

Подстановка — это отображение $\theta : \mathrm{Var} \to \mathrm{Term}$

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

Связка $\mathtt{x}/t$ означает, что при применении подстановки
на место $\mathtt{x}$ подставляется терм t

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

Подстановка считается конечной, если конечна её область

Конечную подстановку θ с областью $V = \{\mathtt{x}_1, \dots, \mathtt{x}_n\}$
можно представить в виде конечного множества связок:

$$\theta = \{\mathtt{x}_1/\theta(\mathtt{x}_1), \dots, \mathtt{x}_n/\theta(\mathtt{x}_n)\}$$

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

Например,

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

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

$$\mathrm{x}(\theta\eta) = (\mathrm{x}\theta)\eta$$

Например,

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