

Математические методы верификации схем и программ

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

Блок 4

Дедуктивная верификация программ:
постановка задачи,
логика Хоара

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

Задача дедуктивной верификации программ

Неформальная постановка

Программа **частично корректна** относительно требований, выраженных в виде предусловия φ и постусловия ψ , если для любых входных данных, удовлетворяющих φ , результат любого конечного вычисления программы удовлетворяет ψ

Программа **тотально корректна**, если

- ▶ она частично корректна и
- ▶ любое её вычисление на входных данных, удовлетворяющих предусловию φ , конечно

Задача верификации императивных программ

состоит в проверке тотальной или частичной корректности заданной программы относительно заданных предусловия и постусловия

Задача дедуктивной верификации программ

Формальная постановка

Парой формул логики предикатов φ, ψ в интерпретации \mathcal{I} зададим
отношение $R_{\varphi, \psi}^{\mathcal{I}} = \{(\sigma, \bar{\sigma}) \mid \sigma, \bar{\sigma} \in \Sigma, \mathcal{I} \models \varphi\sigma, \mathcal{I} \models \psi\bar{\sigma}\}$

Для интерпретации \mathcal{I} и формул φ и ψ , называющихся соответственно
предусловием и **постусловием**, говорят, что программа π

- ▶ **частично корректна** в \mathcal{I} относительно φ и ψ , если $R_{\pi}^{\mathcal{I}} \subseteq R_{\varphi, \psi}^{\mathcal{I}}$, и
- ▶ **тотально корректна** в \mathcal{I} относительно φ и ψ , если
 - ▶ она частично корректна в \mathcal{I} относительно φ и ψ и
 - ▶ вычисление π в \mathcal{I} на любой оценке σ , для которой верно $\mathcal{I} \models \varphi\sigma$, конечно

Утверждение. Для любых программы π , интерпретации \mathcal{I} ,
предусловия φ и постусловия ψ верно следующее:

программа π частично корректна в \mathcal{I} относительно φ и $\psi \Leftrightarrow$
для любых состояний данных σ и $\bar{\sigma}$,
таких что $\mathcal{I} \models \varphi\sigma$ и $\langle \pi \mid \sigma \rangle \xrightarrow{\mathcal{I}^*} \langle \emptyset \mid \bar{\sigma} \rangle$, верно $\mathcal{I} \models \psi\bar{\sigma}$

Задача дедуктивной верификации программ

Формальная постановка

Триплет Хоара (или, по-другому, тройка Хоара) — это запись вида $\{\varphi\}\pi\{\psi\}$, где

- ▶ φ и ψ — формулы логики предикатов, называемые соответственно **предусловием** и **постусловием**, и
- ▶ π — программа

Триплет Хоара $\{\varphi\}\pi\{\psi\}$ **истинен** в интерпретации \mathcal{I} ($\mathcal{I} \models \{\varphi\}\pi\{\psi\}$), если программа π частично корректна в \mathcal{I} относительно φ и ψ

Логика Хоара

Для доказательства частичной корректности программ будем использовать систему правил¹ вида:

$$\frac{\Phi}{\Psi_1}, \quad \frac{\Phi}{\varphi}, \quad \frac{\Phi}{\Psi_1, \Psi_2}, \quad \frac{\Phi}{\varphi, \Psi_1, \psi}$$

(φ, ψ — формулы логики предикатов;
 Φ, Ψ_1, Ψ_2 — триплеты Хоара)

Содержательно каждое из правил прочитывается так:

если истинны все триплеты и формулы, записанные под чертой,
то триплет Φ истинен

Правила можно прочитать и немного по-другому:

если **доказана** истинность всех триплетов и формул под чертой,
то **доказана** и истинность триплета Φ

¹ Hoare C.A.R. An axiomatic basis for computer programming. 1969

Логика Хоара

Вот эти правила:

$$R_\emptyset: \frac{\{\varphi\} \emptyset \{\varphi\}}{t}$$

$$R_{:=}: \frac{\{\varphi\} x/t \{x := t; \varphi\}}{(если подстановка \{x/t\} правильна для \varphi)}$$

$$R_{inf}: \frac{\{\varphi\} \pi \{\psi\}}{\varphi \rightarrow \varphi', \{\varphi'\} \pi \{\psi'\}, \psi' \rightarrow \psi}$$

$$R_{seq}: \frac{\{\varphi\} \pi_1 \pi_2 \{\psi\}}{\{\varphi\} \pi_1 \{\chi\}, \{\chi\} \pi_2 \{\psi\}}$$

$$R_{if}: \frac{\{\varphi\} \text{if } C \text{ then } \pi_1 \text{ else } \pi_2 \text{ fi } \{\psi\}}{\{\varphi \& C\} \pi_1 \{\psi\}, \{\varphi \& \neg C\} \pi_2 \{\psi\}}$$

$$R_{while}: \frac{\{\varphi\} \text{while } C \text{ do } \pi \text{ od } \{\varphi \& \neg C\}}{\{\varphi \& C\} \pi \{\varphi\}}$$

Подстановка $\{x/t\}$ **правильна** для формулы φ , если
ни одно свободное вхождение x не входит в область действия квантора,
связывающего какую-либо переменную терма t

Формула φ в правиле R_{while} называется **инвариантом цикла**

Логика Хоара

Теорема (о корректности правил вывода логики Хоара)

Для любой интерпретации \mathcal{I}

и любого из правил $R_\emptyset, R_{:=}, R_{inf}, R_{seq}, R_{if}, R_{while}$

$$\left(\frac{\Phi}{\Psi_1}, \frac{\Phi}{\varphi}, \frac{\Phi}{\Psi_1, \Psi_2}, \frac{\Phi}{\varphi, \Psi_1, \psi} \right)$$

верно: если $\mathcal{I} \models \Psi_1, \mathcal{I} \models \Psi_2, \mathcal{I} \models \varphi$ и $\mathcal{I} \models \psi$, то $\mathcal{I} \models \Phi$

Доказательство.

Подробно рассмотрим только правило $R_{:=}$:
$$\frac{\{\varphi\{x/t\}\}x := t; \{\varphi\}}{\dagger}$$

Рассмотрим произвольное состояние данных σ , такое что $\mathcal{I} \models \varphi\{x/t\}\sigma$,
и соотношение $\langle x := t; | \sigma \rangle \xrightarrow{\mathcal{I}} \langle \pi | \bar{\sigma} \rangle$

По **операционной семантике программ**, верно $\pi = \emptyset$ и $\bar{\sigma} = \sigma[x \leftarrow t\sigma]$

Следовательно, верно $\mathcal{I} \models \varphi\bar{\sigma}$ и $\mathcal{I} \models \{\varphi\{x/t\}\}x := t; \{\varphi\}$

Корректность остальных правил доказывается **аналогично** ▼

Логика Хоара

Зачем нужна теорема о корректности¹

Истинность триплета $\{\varphi\}\pi\{\psi\}$ в интерпретации \mathcal{I} доказана, если построен **успешный вывод** этого триплета, то есть конечный вывод вида

$$\frac{\{\varphi\}\pi\{\psi\}}{\dots \frac{\dots}{x} \dots \frac{\dots}{x' \quad \underline{\{\varphi'\}\pi'\{\psi'\}} \quad x''} \dots \dots},$$

где

- ▶ под каждым триплетом Хоара в выводе стоит черта
- ▶ под каждой чертой записаны формулы и триплеты Хоара согласно правилам
- ▶ каждая формула, располагающаяся в выводе вне триплетов (как x , x' , x'' на рисунке), истинна в интерпретации \mathcal{I}

¹ Подробнее о выводе в логике Хоара рассказывается в курсе «Математическая логика и логическое программирование» бакалавриата