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

ВМК МГУ, 2023/2024, осенний семестр

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 $R^{\mathcal{I}}_{\varphi,\psi} = \{(\sigma, \overline{\sigma}) \mid \sigma, \overline{\sigma} \in \Sigma,\ \mathcal{I} \models \varphi\sigma,\ \mathcal{I} \models \psi\overline{\sigma}\}$

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 $R^{\mathcal{I}}_{\pi} \subseteq R^{\mathcal{I}}_{\varphi,\psi}$, 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 ψ $\Leftrightarrow$
для любых состояний данных σ и $\overline{\sigma}$,
таких что $\mathcal{I} \models \varphi\sigma$ и $\langle \pi \mid \sigma \rangle \xrightarrow{\mathcal{I}}{}^{*} \langle \emptyset \mid \overline{\sigma} \rangle$, верно $\mathcal{I} \models \psi\overline{\sigma}$

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 правил[1] 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:

$$R_{\emptyset}\colon\ \frac{\{\varphi\}\emptyset\{\varphi\}}{\mathbb{t}} \qquad\qquad R_{:=}\colon\ \frac{\{\varphi\{x/t\}\}\mathtt{x} := t;\{\varphi\}}{\mathbb{t}}$$

(*если подстановка* $\{\mathtt{x}/t\}$ *правильна для* φ)

$$R_{inf}\colon\ \frac{\{\varphi\}\pi\{\psi\}}{\varphi \to \varphi', \{\varphi'\}\pi\{\psi'\}, \psi' \to \psi} \qquad R_{seq}\colon\ \frac{\{\varphi\}\pi_1\ \pi_2\{\psi\}}{\{\varphi\}\pi_1\{\chi\}, \{\chi\}\pi_2\{\psi\}}$$

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

$$R_{\mathbf{while}}\colon\ \frac{\{\varphi\}\mathbf{while}\ C\ \mathbf{do}\ \pi\ \mathbf{od}\{\varphi \,\&\, \neg C\}}{\{\varphi \,\&\, C\}\pi\{\varphi\}}$$

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

Формула φ в правиле $R_{\mathbf{while}}$ 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}, $R_{\textbf{if}}$, $R_{\textbf{while}}$

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

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 $R_{:=}$: $\dfrac{\{\varphi\{x/t\}\}\mathtt{x} := t; \{\varphi\}}{\mathbb{t}}$

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

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

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

Корректность остальных правил доказывается $\boxed{\text{аналогично}}$ ▼

Логика Хоара

Зачем нужна теорема о корректности[1]

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

$$\dfrac{\{\varphi\}\pi\{\psi\}}{\begin{array}{c}\dots\\ \dots\end{array} \quad \dfrac{\dots}{\chi} \quad \begin{array}{c}\dots\\ \dots\end{array} \quad \dfrac{\dots}{\chi' \quad \dfrac{\{\varphi'\}\pi'\{\psi'\}}{\dots} \quad \chi''} \quad \begin{array}{c}\dots\\ \dots\end{array}}\ ,$$

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 χ, χ', χ'' на рисунке), истинна в интерпретации $\mathcal{I}$

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