Математические методы верификации схем и программ

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

Блок 3

Дедуктивная верификация программ:
постановка задачи,
логика Хоара

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

ВМК МГУ, 2022/2023, осенний семестр

Задача дедуктивной верификации программ

Неформальная постановка

Программа частично корректна относительно требований, выражаемых предусловием φ и постусловием ψ, если для любых начальных данных, удовлетворяющих φ, результат любого конечного вычисления программы удовлетворяет ψ

Программа тотально корректна, если

- она частично корректна и
- любое её вычисление на начальных 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

Предусловие φ и постусловие ψ — это формулы логики предикатов, а π — императивная программа

Требование корректности π относительно φ, ψ записывается в виде триплета Хоара (или тройки Хоара):

$$\{\varphi\}\pi\{\psi\}$$

Триплет Хоара $\{\varphi\}\pi\{\psi\}$ истинен в интерпретации $\mathcal{I}$ $\quad$ ($\mathcal{I} \models \{\varphi\}\pi\{\psi\}$), если для любых оценок θ, η верно:

$$\text{если } \mathcal{I} \models \varphi\theta \text{ и } \langle \pi \mid \theta \rangle \to^* \langle \emptyset \mid \eta \rangle, \text{ то } \mathcal{I} \models \psi\eta$$

Программа π частично корректна в интерпретации $\mathcal{I}$ относительно предусловия φ и постусловия ψ, если

$$\mathcal{I} \models \{\varphi\}\pi\{\psi\}$$

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:

$$R_{\emptyset}\colon \frac{\{\varphi\}\emptyset\{\varphi\}}{\mathbb{t}}$$

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

(*переменная* $\mathtt{x}$ *свободна для терма* t *в формуле* φ)

$$R_{inf}\colon \frac{\{\varphi\}\pi\{\psi\}}{\varphi \to \varphi', \{\varphi'\}\pi\{\psi'\}, \psi' \to \psi}$$

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

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

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

Переменная $\mathtt{x}$ свободна для терма t в формуле 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}, $R_{\mathbf{if}}$, $R_{\mathbf{while}}$

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

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 $R_{:=}$: $\dfrac{\{\varphi\{\mathrm{x}/t\}\}\mathrm{x} := t; \{\varphi\}}{\not{t}}$

Рассмотрим произвольную оценку θ, такую что $\mathcal{I} \models \varphi\{\mathrm{x}/t\}\theta$, и соотношение $\langle \mathrm{x} := t; \mid \theta\rangle \to_{\mathcal{I}} \langle \pi \mid \eta\rangle$

По операционной семантике программ, $\pi = \emptyset$ и $\eta = \{\mathrm{x}/t\}\theta$

Значит, $\mathcal{I} \models \varphi\eta$ и $\mathcal{I} \models \{\varphi\{\mathrm{x}/t\}\}\mathrm{x} := t; \{\varphi\}$

Корректность остальных правил доказывается 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

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

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