

# 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, 2025/2026, осенний семестр

# Задача дедуктивной верификации программ

## Неформальная постановка

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

Программа **тотально корректна**, если

- ▶ она частично корректна и
- ▶ любое её вычисление на входных данных, удовлетворяющих предусловию  $\varphi$ , 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**  $\varphi, \psi$  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  $\varphi$  и  $\psi$ , называющихся соответственно **предусловием** и **постусловием**, говорят, что программа  $\pi$

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

**Утверждение.** Для любых программы  $\pi$ , интерпретации  $\mathcal{I}$ , предусловия  $\varphi$  и постусловия  $\psi$  верно следующее:  
программа  $\pi$  частично корректна в  $\mathcal{I}$  относительно  $\varphi$  и  $\psi \Leftrightarrow$   
для любых состояний данных  $\sigma$  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

- ▶  $\varphi$  и  $\psi$  — формулы логики предикатов, называемые соответственно **предусловием** и **постусловием**, и
- ▶  $\pi$  — программа

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

# Логика Хоара

Для доказательства частичной корректности программ будем использовать систему правил<sup>1</sup> вида:

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

( $\varphi, \psi$  — формулы логики предикатов;  
 $\Phi, \Psi_1, \Psi_2$  — триплеты Хоара)

**Содержательно** каждое из правил прочитывается так:

если истинны все триплеты и формулы, записанные под чертой,  
то триплет  $\Phi$  истинен

Правила можно прочесть и немного по-другому:

если **доказана** истинность всех триплетов и формул под чертой,  
то **доказана** и истинность триплета  $\Phi$

---

<sup>1</sup> Hoare C.A.R. An axiomatic basis for computer programming. 1969

# Логика Хоара

Вот эти правила:

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

$$R_{:=}: \frac{\{\varphi\{x/t\}\} x := t; \{\varphi\}}{\uparrow}$$

(если подстановка  $\{x/t\}$   
правильна для  $\varphi$ )

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

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

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

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

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

Формула  $\varphi$  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  $R_{\emptyset}, R_{:=}, R_{inf}, R_{seq}, R_{if}, R_{while}$

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

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  $R_{:=}: \frac{\{\varphi\{x/t\}\}x := t; \{\varphi\}}{\vdash}$

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

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 корректности<sup>1</sup>

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

$$\frac{\{\varphi\}\pi\{\psi\}}{\begin{array}{ccccccc} \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \underline{\quad \chi \quad} & \dots & \underline{\quad \chi' \quad} & \frac{\{\varphi'\}\pi'\{\psi'\}}{\quad} & \underline{\quad \chi'' \quad} & \dots \end{array}},$$

...

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

---

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