Математические методы верификации схем и программ

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

Блок 5

Дедуктивная верификация программ:
аннотированные программы

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

ВМК МГУ, 2025/2026, осенний семестр

Аннотированные программы: определения

Доказательство корректности программ, основанное логике Хоара, можно сделать более наглядным, если “встроить” информацию о применении правил вывода непосредственно в текст программы

Аннотация — это запись вида $\{\varphi\}$, где φ — произвольная формула

Аннотированная программа — это программа, в которой до и после каждой команды могут располагаться последовательности аннотаций

Аннотация может расцениваться как

- предусловие команды, следующей за аннотацией
- постусловие команды, предшествующей аннотации
- составная часть триплета, использующегося в выводе исходного триплета

Аннотированные программы: определения

Аннотированная программа $\widetilde{\pi}$ правильно отвечает триплету $\{\varphi\}\pi\{\psi\}$ в интерпретации $\mathcal{I}$, если выполняются следующие условия:

1. При удалении всех аннотаций из $\widetilde{\pi}$ получается программа π
2. $\widetilde{\pi}$ начинается с аннотации $\{\varphi\}$ и оканчивается аннотацией $\{\psi\}$
3. Перед каждой командой и после каждой команды в $\widetilde{\pi}$ располагается хотя бы одна аннотация
4. Аннотации перед каждой пустой командой и после неё равны:
$$\{\chi\}\emptyset\{\chi\}$$
5. Аннотации перед каждым присваиванием и после него соотносятся так же, как и в правиле $R_{:=}$:
$$\{\chi\{\mathtt{x}/t\}\}\mathtt{x} := t; \{\chi\},$$
где подстановка $\{\mathtt{x}/t\}$ правильна для формулы χ

Аннотированные программы: определения

Аннотированная программа $\widetilde{\pi}$ правильно отвечает триплету $\{\varphi\}\pi\{\psi\}$ в интерпретации $\mathcal{I}$, если выполняются следующие условия:

6. Каждое ветвление в $\widetilde{\pi}$ аннотировано следующим образом:
$$\begin{array}{l} \{\chi_1\} \\ \textbf{if } C \textbf{ then } \{\chi_1 \,\&\, C\}\widetilde{\pi}_1\{\chi_2\} \textbf{ else } \{\chi_1 \,\&\, \neg C\}\widetilde{\pi}_2\{\chi_2\} \textbf{ fi} \\ \{\chi_2\} \end{array}$$

7. каждый цикл в $\widetilde{\pi}$ аннотирован следующим образом:
$$\begin{array}{l} \{\chi\} \\ \textbf{while } C \textbf{ do } \{\chi \,\&\, C\}\widetilde{\pi}'\{\chi\} \textbf{ od} \\ \{\chi \,\&\, \neg C\} \end{array}$$

8. Для любых двух подряд идущих аннотаций $\{\chi_1\}\{\chi_2\}$ в $\widetilde{\pi}$ верно $\mathcal{I} \models \chi_1 \rightarrow \chi_2$

Аннотированные программы: пример

Рассмотрим такую программу π:

$$\textbf{while } \mathrm{x} \neq \mathrm{y} \textbf{ do if } \mathrm{x} > \mathrm{y} \textbf{ then } \mathrm{x} := \mathrm{x} - \mathrm{y}; \textbf{ else } \mathrm{y} := \mathrm{y} - \mathrm{x}; \textbf{ fi od}$$

Докажем, что программа π корректно реализует вычисление наибольшего общего делителя натуральных значений $\mathtt{x}$ и $\mathtt{y}$ с записью результата в $\mathtt{x}$

Для этого достаточно доказать истинность триплета $\{\varphi\}\pi\{\psi\}$ в интерпретации $\mathcal{I}_{ar}$, где:

$$\begin{aligned}
\varphi(\mathrm{x},\mathrm{y},\mathrm{z}):&\quad \mathtt{x} > \mathbf{0} \,\&\, \mathtt{y} > \mathbf{0} \,\&\, \mathrm{gcd}(\mathtt{x},\mathtt{y},\mathtt{z})\\
\psi(\mathrm{x},\mathrm{y},\mathrm{z}):&\quad \mathtt{x} = \mathtt{z}\\
\mathrm{gcd}(\mathrm{x},\mathrm{y},\mathrm{z}):&\quad \exists \mathtt{u}\,(\mathtt{z} \times \mathtt{u} = \mathtt{x}) \,\&\, \exists \mathtt{u}\,(\mathtt{z} \times \mathtt{u} = \mathtt{y}) \,\&\\
&\quad \forall \mathtt{w}\,(\exists \mathtt{u}\,(\mathtt{w} \times \mathtt{u} = \mathtt{x}) \,\&\, \exists \mathtt{u}\,(\mathtt{w} \times \mathtt{u} = \mathtt{y}) \rightarrow (\mathtt{w} \leq \mathtt{z}))
\end{aligned}$$

Аннотированные программы: пример

Аннотированная программа, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$, может выглядеть так:

Аннотированные программы: пример

Аннотированная программа, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$, может выглядеть так:

$\{\mathrm{x} > \mathbf{0} \,\&\, \mathrm{y} > \mathbf{0} \,\&\, \mathrm{gcd}(\mathrm{x}, \mathrm{y}, \mathrm{z})\}$
while $\mathrm{x} \neq \mathrm{y}$ **do**

  if $\mathrm{x} > \mathrm{y}$ **then**

    $\mathrm{x} := \mathrm{x} - \mathrm{y};$

  else

    $\mathrm{y} := \mathrm{y} - \mathrm{x};$

  fi

od

$\{\mathrm{x} = \mathrm{z}\}$

Аннотированные программы: пример

Аннотированная программа, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$, может выглядеть так:

$\{x > \mathbf{0} \,\&\, y > \mathbf{0} \,\&\, gcd(x, y, z)\}$
while $x \neq y$ **do**
  $\{x > \mathbf{0} \,\&\, y > \mathbf{0} \,\&\, gcd(x, y, z) \,\&\, x \neq y\}$
  if $x > y$ **then**
    $x := x - y;$
  else
    $y := y - x;$
  fi
  $\{x > \mathbf{0} \,\&\, y > \mathbf{0} \,\&\, gcd(x, y, z)\}$
od
$\{x > \mathbf{0} \,\&\, y > \mathbf{0} \,\&\, gcd(x, y, z) \,\&\, \neg(x \neq y)\}$
$\{x = z\}$

Аннотированные программы: пример

Аннотированная программа, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$, может выглядеть так:

$\{x > \mathbf{0} \,\&\, y > \mathbf{0} \,\&\, gcd(x, y, z)\}$
while $x \neq y$ **do**
  $\{x > \mathbf{0} \,\&\, y > \mathbf{0} \,\&\, gcd(x, y, z) \,\&\, x \neq y\}$
  if $x > y$ **then**
    $\{x > \mathbf{0} \,\&\, y > \mathbf{0} \,\&\, gcd(x, y, z) \,\&\, x \neq y \,\&\, x > y\}$

    $x := x - y;$

  else
    $\{x > \mathbf{0} \,\&\, y > \mathbf{0} \,\&\, gcd(x, y, z) \,\&\, x \neq y \,\&\, \neg(x > y)\}$

    $y := y - x;$

  fi
  $\{x > \mathbf{0} \,\&\, y > \mathbf{0} \,\&\, gcd(x, y, z)\}$
od
$\{x > \mathbf{0} \,\&\, y > \mathbf{0} \,\&\, gcd(x, y, z) \,\&\, \neg(x \neq y)\}$
$\{x = z\}$

Аннотированные программы: пример

Аннотированная программа, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$, может выглядеть так:

$$
\begin{array}{l}
\{x > \mathbf{0} \,\&\, y > \mathbf{0} \,\&\, gcd(x, y, z)\} \\
\quad \textbf{while } x \neq y \textbf{ do} \\
\qquad \{x > \mathbf{0} \,\&\, y > \mathbf{0} \,\&\, gcd(x, y, z) \,\&\, x \neq y\} \\
\qquad \textbf{if } x > y \textbf{ then} \\
\qquad\quad \{x > \mathbf{0} \,\&\, y > \mathbf{0} \,\&\, gcd(x, y, z) \,\&\, x \neq y \,\&\, x > y\} \\
\\
\qquad\qquad x := x - y; \\
\qquad\quad \{x > \mathbf{0} \,\&\, y > \mathbf{0} \,\&\, gcd(x, y, z)\} \\
\qquad \textbf{else} \\
\qquad\quad \{x > \mathbf{0} \,\&\, y > \mathbf{0} \,\&\, gcd(x, y, z) \,\&\, x \neq y \,\&\, \neg(x > y)\} \\
\\
\qquad\qquad y := y - x; \\
\qquad\quad \{x > \mathbf{0} \,\&\, y > \mathbf{0} \,\&\, gcd(x, y, z)\} \\
\qquad \textbf{fi} \\
\qquad \{x > \mathbf{0} \,\&\, y > \mathbf{0} \,\&\, gcd(x, y, z)\} \\
\quad \textbf{od} \\
\{x > \mathbf{0} \,\&\, y > \mathbf{0} \,\&\, gcd(x, y, z) \,\&\, \neg(x \neq y)\} \\
\{x = z\}
\end{array}
$$

Аннотированные программы: пример

Аннотированная программа, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$, может выглядеть так:

$$
\begin{array}{l}
\{\mathrm{x} > \mathbf{0}\,\&\,\mathrm{y} > \mathbf{0}\,\&\,\mathrm{gcd}(\mathrm{x},\mathrm{y},\mathrm{z})\}\\
\ \ \textbf{while}\ \mathrm{x} \neq \mathrm{y}\ \textbf{do}\\
\quad \{\mathrm{x} > \mathbf{0}\,\&\,\mathrm{y} > \mathbf{0}\,\&\,\mathrm{gcd}(\mathrm{x},\mathrm{y},\mathrm{z})\,\&\,\mathrm{x} \neq \mathrm{y}\}\\
\quad\ \ \textbf{if}\ \mathrm{x} > \mathrm{y}\ \textbf{then}\\
\qquad \{\mathrm{x} > \mathbf{0}\,\&\,\mathrm{y} > \mathbf{0}\,\&\,\mathrm{gcd}(\mathrm{x},\mathrm{y},\mathrm{z})\,\&\,\mathrm{x} \neq \mathrm{y}\,\&\,\mathrm{x} > \mathrm{y}\}\\
\qquad \{\mathrm{x} - \mathrm{y} > \mathbf{0}\,\&\,\mathrm{y} > \mathbf{0}\,\&\,\mathrm{gcd}(\mathrm{x} - \mathrm{y},\mathrm{y},\mathrm{z})\}\\
\qquad\ \ \mathrm{x} := \mathrm{x} - \mathrm{y};\\
\qquad \{\mathrm{x} > \mathbf{0}\,\&\,\mathrm{y} > \mathbf{0}\,\&\,\mathrm{gcd}(\mathrm{x},\mathrm{y},\mathrm{z})\}\\
\quad\ \ \textbf{else}\\
\qquad \{\mathrm{x} > \mathbf{0}\,\&\,\mathrm{y} > \mathbf{0}\,\&\,\mathrm{gcd}(\mathrm{x},\mathrm{y},\mathrm{z})\,\&\,\mathrm{x} \neq \mathrm{y}\,\&\,\neg(\mathrm{x} > \mathrm{y})\}\\
\qquad \{\mathrm{x} > \mathbf{0}\,\&\,\mathrm{y} - \mathrm{x} > \mathbf{0}\,\&\,\mathrm{gcd}(\mathrm{x},\mathrm{y} - \mathrm{x},\mathrm{z})\}\\
\qquad\ \ \mathrm{y} := \mathrm{y} - \mathrm{x};\\
\qquad \{\mathrm{x} > \mathbf{0}\,\&\,\mathrm{y} > \mathbf{0}\,\&\,\mathrm{gcd}(\mathrm{x},\mathrm{y},\mathrm{z})\}\\
\quad\ \ \textbf{fi}\\
\quad \{\mathrm{x} > \mathbf{0}\,\&\,\mathrm{y} > \mathbf{0}\,\&\,\mathrm{gcd}(\mathrm{x},\mathrm{y},\mathrm{z})\}\\
\ \ \textbf{od}\\
\{\mathrm{x} > \mathbf{0}\,\&\,\mathrm{y} > \mathbf{0}\,\&\,\mathrm{gcd}(\mathrm{x},\mathrm{y},\mathrm{z})\,\&\,\neg(\mathrm{x} \neq \mathrm{y})\}\\
\{\mathrm{x} = \mathrm{z}\}
\end{array}
$$

Аннотированные программы: пример

Аннотированная программа, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$, может выглядеть так:

$\{\mathrm{x} > \mathbf{0} \,\&\, \mathrm{y} > \mathbf{0} \,\&\, \mathrm{gcd}(\mathrm{x}, \mathrm{y}, \mathrm{z})\}$
while $\mathrm{x} \neq \mathrm{y}$ **do**
$\{\mathrm{x} > \mathbf{0} \,\&\, \mathrm{y} > \mathbf{0} \,\&\, \mathrm{gcd}(\mathrm{x}, \mathrm{y}, \mathrm{z}) \,\&\, \mathrm{x} \neq \mathrm{y}\}$
if $\mathrm{x} > \mathrm{y}$ **then**
$\{\mathrm{x} > \mathbf{0} \,\&\, \mathrm{y} > \mathbf{0} \,\&\, \mathrm{gcd}(\mathrm{x}, \mathrm{y}, \mathrm{z}) \,\&\, \mathrm{x} \neq \mathrm{y} \,\&\, \mathrm{x} > \mathrm{y}\}$
$\{\mathrm{x} - \mathrm{y} > \mathbf{0} \,\&\, \mathrm{y} > \mathbf{0} \,\&\, \mathrm{gcd}(\mathrm{x} - \mathrm{y}, \mathrm{y}, \mathrm{z})\}$
$\mathrm{x} := \mathrm{x} - \mathrm{y};$
$\{\mathrm{x} > \mathbf{0} \,\&\, \mathrm{y} > \mathbf{0} \,\&\, \mathrm{gcd}(\mathrm{x}, \mathrm{y}, \mathrm{z})\}$
else
$\{\mathrm{x} > \mathbf{0} \,\&\, \mathrm{y} > \mathbf{0} \,\&\, \mathrm{gcd}(\mathrm{x}, \mathrm{y}, \mathrm{z}) \,\&\, \mathrm{x} \neq \mathrm{y} \,\&\, \neg(\mathrm{x} > \mathrm{y})\}$
$\{\mathrm{x} > \mathbf{0} \,\&\, \mathrm{y} - \mathrm{x} > \mathbf{0} \,\&\, \mathrm{gcd}(\mathrm{x}, \mathrm{y} - \mathrm{x}, \mathrm{z})\}$
$\mathrm{y} := \mathrm{y} - \mathrm{x};$
$\{\mathrm{x} > \mathbf{0} \,\&\, \mathrm{y} > \mathbf{0} \,\&\, \mathrm{gcd}(\mathrm{x}, \mathrm{y}, \mathrm{z})\}$
fi
$\{\mathrm{x} > \mathbf{0} \,\&\, \mathrm{y} > \mathbf{0} \,\&\, \mathrm{gcd}(\mathrm{x}, \mathrm{y}, \mathrm{z})\}$
od
$\{\mathrm{x} > \mathbf{0} \,\&\, \mathrm{y} > \mathbf{0} \,\&\, \mathrm{gcd}(\mathrm{x}, \mathrm{y}, \mathrm{z}) \,\&\, \neg(\mathrm{x} \neq \mathrm{y})\}$
$\{\mathrm{x} = \mathrm{z}\}$

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)
Если существует аннотированная программа $\widetilde{\pi}$, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$ в интерпретации $\mathcal{I}$, то $\mathcal{I} \models \{\varphi\}\pi\{\psi\}$

Доказательство.

Достаточно показать, как по аннотированной программе $\widetilde{\pi}$ можно построить успешный вывод триплета $\{\varphi\}\pi\{\psi\}$:

Фрагмент программы $\widetilde{\pi}$ вида

$$\{\chi\}\boldsymbol{\emptyset}\{\chi\}$$

соответствует фрагменту вывода

$$R_{\boldsymbol{\emptyset}}\colon\ \frac{\{\chi\}\boldsymbol{\emptyset}\{\chi\}}{\mathbb{t}}$$

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)
Если существует аннотированная программа $\widetilde{\pi}$, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$ в интерпретации $\mathcal{I}$, то $\mathcal{I} \models \{\varphi\}\pi\{\psi\}$

Доказательство.

Достаточно показать, как по аннотированной программе $\widetilde{\pi}$ можно построить успешный вывод триплета $\{\varphi\}\pi\{\psi\}$:

Фрагмент программы $\widetilde{\pi}$ вида

$$\{\chi\{x/t\}\}\mathtt{x} := t; \{\chi\}$$

соответствует фрагменту вывода

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

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)
Если существует аннотированная программа $\widetilde{\pi}$, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$ в интерпретации $\mathcal{I}$, то $\mathcal{I} \models \{\varphi\}\pi\{\psi\}$

Доказательство.

Достаточно показать, как по аннотированной программе $\widetilde{\pi}$ можно построить успешный вывод триплета $\{\varphi\}\pi\{\psi\}$:

Фрагмент программы $\widetilde{\pi}$ вида

$$\{\chi\}\{\chi'\}\widetilde{\pi}'\{\chi''\}$$

соответствует фрагменту вывода

$$R_{inf}: \frac{\{\chi\}\pi'\{\chi''\}}{\chi \to \chi', \{\chi'\}\pi'\{\chi''\}, \chi'' \to \chi''}$$

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)
Если существует аннотированная программа $\widetilde{\pi}$, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$ в интерпретации $\mathcal{I}$, то $\mathcal{I} \models \{\varphi\}\pi\{\psi\}$

Доказательство.

Достаточно показать, как по аннотированной программе $\widetilde{\pi}$ можно построить успешный вывод триплета $\{\varphi\}\pi\{\psi\}$:

Фрагмент программы $\widetilde{\pi}$ вида

$$\{\chi\}\widetilde{\pi}'\{\chi'\}\{\chi''\}$$

соответствует фрагменту вывода

$$R_{inf}: \frac{\{\chi\}\pi'\{\chi''\}}{\chi \to \chi, \{\chi\}\pi'\{\chi'\}, \chi' \to \chi''}$$

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)
Если существует аннотированная программа $\widetilde{\pi}$, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$ в интерпретации $\mathcal{I}$, то $\mathcal{I} \models \{\varphi\}\pi\{\psi\}$

Доказательство.

Достаточно показать, как по аннотированной программе $\widetilde{\pi}$ можно построить успешный вывод триплета $\{\varphi\}\pi\{\psi\}$:

Фрагмент программы $\widetilde{\pi}$ вида

$$\{\chi\}\widetilde{\pi}_1\{\chi'\}\ \widetilde{\pi}_2\{\chi''\}$$

соответствует фрагменту вывода

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

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)
Если существует аннотированная программа $\widetilde{\pi}$, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$ в интерпретации $\mathcal{I}$, то $\mathcal{I} \models \{\varphi\}\pi\{\psi\}$

Доказательство.

Достаточно показать, как по аннотированной программе $\widetilde{\pi}$ можно построить успешный вывод триплета $\{\varphi\}\pi\{\psi\}$:

Фрагмент программы $\widetilde{\pi}$ вида

$$\{\chi\}\textbf{if } C \textbf{ then } \{\chi \,\&\, C\}\widetilde{\pi}_1\{\chi'\} \textbf{ else } \{\chi \,\&\, \neg C\}\widetilde{\pi}_2\{\chi'\} \textbf{ fi}\{\chi'\}$$

соответствует фрагменту вывода

$$R_{\textbf{if}}\colon\ \frac{\{\chi\}\textbf{if } C \textbf{ then } \pi_1 \textbf{ else } \pi_2 \textbf{ fi}\{\chi'\}}{\{\chi \,\&\, C\}\pi_1\{\chi'\},\ \{\chi \,\&\, \neg C\}\pi_2\{\chi'\}}$$

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)
Если существует аннотированная программа $\widetilde{\pi}$, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$ в интерпретации $\mathcal{I}$, то $\mathcal{I} \models \{\varphi\}\pi\{\psi\}$

Доказательство.

Достаточно показать, как по аннотированной программе $\widetilde{\pi}$ можно построить успешный вывод триплета $\{\varphi\}\pi\{\psi\}$:

Фрагмент программы $\widetilde{\pi}$ вида

$$\{\chi\}\textbf{while } C \textbf{ do } \{\chi \,\&\, C\}\widetilde{\pi}'\{\chi\} \textbf{ od}\{\chi \,\&\, \neg C\}$$

соответствует фрагменту вывода

$$R_{\textbf{while}}\colon \frac{\{\chi\}\textbf{while } C \textbf{ do } \pi' \textbf{ od}\{\chi \,\&\, \neg C\}}{\{\chi \,\&\, C\}\pi'\{\chi\}}$$