Математические методы верификации схем и программ

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

Блок 4

Дедуктивная верификация программ:
аннотированные программы

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

ВМК МГУ, 2022/2023, 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 инструкции могут располагаться последовательности аннотаций

Аннотация может расцениваться как

- предусловие инструкции, следующей за аннотацией
- постусловие инструкции, предшествующей аннотации
- составная часть триплета, располагающегося в выводе для исходного триплета

Аннотированные программы: определения

Аннотированная программа $\widetilde{\pi}$ обосновывает истинность триплета $\{\varphi\}\pi\{\psi\}$ 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 инструкцией и после каждой инструкции в $\widetilde{\pi}$ располагается хотя бы одна аннотация
4. Аннотации перед каждой пустой инструкцией
   и после неё равны:
   $$\{\chi\}\emptyset\{\chi\}$$

Аннотированные программы: определения

Аннотированная программа $\widetilde{\pi}$ обосновывает истинность триплета $\{\varphi\}\pi\{\psi\}$ в интерпретации $\mathcal{I}$, если выполняются следующие условия:

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 переменная $\mathtt{x}$ свободна для терма t в формуле χ

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

Аннотированные программы: определения

Аннотированная программа $\widetilde{\pi}$ обосновывает истинность триплета $\{\varphi\}\pi\{\psi\}$ в интерпретации $\mathcal{I}$, если выполняются следующие условия:

7. каждый цикл в $\widetilde{\pi}$ аннотирован следующим образом:

$$\begin{array}{l} \{\chi\} \\ \text{while } C \text{ do} \\ \quad \{\chi \,\&\, C\}\widetilde{\pi}'\{\chi\} \\ \text{od} \\ \{\chi \,\&\, \neg C\} \end{array}$$

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

Аннотированные программы: пример

Рассмотрим такую программу π:

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

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

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

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

Аннотированные программы: пример

Аннотированная программа, обосновывающая истинность триплета $\{\varphi\}\pi\{\psi\}$, может выглядеть так:

Аннотированные программы: пример

Аннотированная программа, обосновывающая истинность триплета $\{\varphi\}\pi\{\psi\}$, может выглядеть так:

$\{\mathtt{x} > 0 \,\&\, \mathtt{y} > 0 \,\&\, \mathrm{gcd}(\mathtt{x}, \mathtt{y}, \mathtt{z})\}$

while $\mathtt{x} \neq \mathtt{y}$ do

if $\mathtt{x} > \mathtt{y}$ then

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

else

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

fi

mod

$\{\mathtt{x} = \mathtt{z}\}$

Аннотированные программы: пример

Аннотированная программа, обосновывающая истинность триплета $\{\varphi\}\pi\{\psi\}$, может выглядеть так:

$\{x > 0 \,\&\, y > 0 \,\&\, \mathrm{gcd}(x, y, z)\}$

while $x \neq y$ do

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

if $x > y$ then

$x := x - y;$

else

$y := y - x;$

fi

$\{x > 0 \,\&\, y > 0 \,\&\, \mathrm{gcd}(x, y, z)\}$

mod

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

$\{x = z\}$

Аннотированные программы: пример

Аннотированная программа, обосновывающая истинность триплета $\{\varphi\}\pi\{\psi\}$, может выглядеть так:

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

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

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

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

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

Аннотированные программы: пример

Аннотированная программа, обосновывающая истинность триплета $\{\varphi\}\pi\{\psi\}$, может выглядеть так:

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

    $x := x - y;$
    $\{x > 0 \,\&\, y > 0 \,\&\, gcd(x, y, z)\}$
  else
    $\{x > 0 \,\&\, y > 0 \,\&\, gcd(x, y, z) \,\&\, x \neq y \,\&\, \neg(x > y)\}$

    $y := y - x;$
    $\{x > 0 \,\&\, y > 0 \,\&\, gcd(x, y, z)\}$
  fi
  $\{x > 0 \,\&\, y > 0 \,\&\, gcd(x, y, z)\}$
  mod
$\{x > 0 \,\&\, y > 0 \,\&\, gcd(x, y, z) \,\&\, \neg(x \neq y)\}$
$\{x = z\}$

Аннотированные программы: пример

Аннотированная программа, обосновывающая истинность триплета $\{\varphi\}\pi\{\psi\}$, может выглядеть так:

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

Аннотированные программы: пример

Аннотированная программа, обосновывающая истинность триплета $\{\varphi\}\pi\{\psi\}$, может выглядеть так:

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

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)
Если существует аннотированная программа $\widetilde{\pi}$, обосновывающая истинность триплета $\{\varphi\}\pi\{\psi\}$ 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

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

соответствует фрагменту вывода

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

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)
Если существует аннотированная программа $\widetilde{\pi}$, обосновывающая истинность триплета $\{\varphi\}\pi\{\psi\}$ 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

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

соответствует фрагменту вывода

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

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)

Если существует аннотированная программа $\widetilde{\pi}$, обосновывающая истинность триплета $\{\varphi\}\pi\{\psi\}$ 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

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

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)
Если существует аннотированная программа $\widetilde{\pi}$, обосновывающая истинность триплета $\{\varphi\}\pi\{\psi\}$ 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

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

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)
Если существует аннотированная программа $\widetilde{\pi}$, обосновывающая истинность триплета $\{\varphi\}\pi\{\psi\}$ 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

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

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)
Если существует аннотированная программа $\widetilde{\pi}$, обосновывающая истинность триплета $\{\varphi\}\pi\{\psi\}$ 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

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

соответствует фрагменту вывода

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

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)
Если существует аннотированная программа $\widetilde{\pi}$, обосновывающая истинность триплета $\{\varphi\}\pi\{\psi\}$ 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

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

соответствует фрагменту вывода

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