

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, 2023/2024, 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 $\tilde{\pi}$ **правильно отвечает** триплету $\{\varphi\}\pi\{\psi\}$ в интерпретации \mathcal{I} , если выполняются следующие условия:

1. При удалении всех аннотаций из $\tilde{\pi}$ получается программа π
2. $\tilde{\pi}$ начинается с аннотации $\{\varphi\}$ и оканчивается аннотацией $\{\psi\}$
3. Перед каждой командой и после каждой команды в $\tilde{\pi}$ 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 $R_{:=}$:
$$\{\chi\{x/t\}\}x := t; \{\chi\},$$
где подстановка $\{x/t\}$ правильна для формулы χ

Аннотированные программы: определения

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

6. Каждое ветвление в $\tilde{\pi}$ аннотировано следующим образом:

$$\begin{array}{l} \{\chi_1\} \\ \mathbf{if} \ C \ \mathbf{then} \ \{\chi_1 \ \& \ C\} \tilde{\pi}_1 \{\chi_2\} \ \mathbf{else} \ \{\chi_1 \ \& \ \neg C\} \tilde{\pi}_2 \{\chi_2\} \ \mathbf{fi} \\ \{\chi_2\} \end{array}$$

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

$$\begin{array}{l} \{\chi\} \\ \mathbf{while} \ C \ \mathbf{do} \ \{\chi \ \& \ C\} \tilde{\pi}' \{\chi\} \ \mathbf{od} \\ \{\chi \ \& \ \neg C\} \end{array}$$

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

Аннотированные программы: пример

Рассмотрим такую программу π :

while $x \neq y$ **do if** $x > y$ **then** $x := x - y$; **else** $y := y - x$; **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:

$$\varphi(x, y, z): \quad x > \mathbf{0} \ \& \ y > \mathbf{0} \ \& \ \text{gcd}(x, y, z)$$

$$\psi(x, y, z): \quad x = z$$

$$\text{gcd}(x, y, z): \quad \exists u (z \times u = x) \ \& \ \exists u (z \times u = y) \ \& \\ \forall w (\exists u (w \times u = x) \ \& \ \exists u (w \times u = y) \rightarrow (w \leq z))$$

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:

```
{x > 0 & y > 0 & gcd(x, y, z)}
```

```
while x ≠ y do
```

```
  if x > y then
```

```
    x := x - y;
```

```
  else
```

```
    y := y - x;
```

```
  fi
```

```
od
```

```
{x = z}
```

Аннотированные программы: пример

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

```
{x > 0 & y > 0 & gcd(x, y, z)}
while x ≠ y do
  {x > 0 & y > 0 & gcd(x, y, z) & x ≠ y}
  if x > y then

    x := x - y;

  else

    y := y - x;

  fi
  {x > 0 & y > 0 & gcd(x, y, z)}
od
{x > 0 & y > 0 & gcd(x, y, z) & ¬(x ≠ y)}
{x = z}
```


Аннотированные программы: пример

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

```
{x > 0 & y > 0 & gcd(x, y, z)}
while x ≠ y do
  {x > 0 & y > 0 & gcd(x, y, z) & x ≠ y}
  if x > y then
    {x > 0 & y > 0 & gcd(x, y, z) & x ≠ y & x > y}

    x := x - y;

  else
    {x > 0 & y > 0 & gcd(x, y, z) & x ≠ y & ¬(x > y)}

    y := y - x;

  fi
  {x > 0 & y > 0 & gcd(x, y, z)}
od
{x > 0 & y > 0 & gcd(x, y, z) & ¬(x ≠ y)}
{x = z}
```

Аннотированные программы: пример

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

```
{x > 0 & y > 0 & gcd(x, y, z)}
while x ≠ y do
  {x > 0 & y > 0 & gcd(x, y, z) & x ≠ y}
  if x > y then
    {x > 0 & y > 0 & gcd(x, y, z) & x ≠ y & x > y}

    x := x - y;
    {x > 0 & y > 0 & gcd(x, y, z)}
  else
    {x > 0 & y > 0 & gcd(x, y, z) & x ≠ y & ¬(x > y)}

    y := y - x;
    {x > 0 & y > 0 & gcd(x, y, z)}
  fi
  {x > 0 & y > 0 & gcd(x, y, z)}
od
{x > 0 & y > 0 & gcd(x, y, z) & ¬(x ≠ y)}
{x = z}
```

Аннотированные программы: пример

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

```
{x > 0 & y > 0 & gcd(x, y, z)}
while x ≠ y do
  {x > 0 & y > 0 & gcd(x, y, z) & x ≠ y}
  if x > y then
    {x > 0 & y > 0 & gcd(x, y, z) & x ≠ y & x > y}
    {x - y > 0 & y > 0 & gcd(x - y, y, z)}
    x := x - y;
    {x > 0 & y > 0 & gcd(x, y, z)}
  else
    {x > 0 & y > 0 & gcd(x, y, z) & x ≠ y & ¬(x > y)}
    {x > 0 & y - x > 0 & gcd(x, y - x, z)}
    y := y - x;
    {x > 0 & y > 0 & gcd(x, y, z)}
  fi
  {x > 0 & y > 0 & gcd(x, y, z)}
od
{x > 0 & y > 0 & gcd(x, y, z) & ¬(x ≠ y)}
{x = z}
```

Аннотированные программы: пример

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

```
{x > 0 & y > 0 & gcd(x, y, z)}
while x ≠ y do
  {x > 0 & y > 0 & gcd(x, y, z) & x ≠ y}
  if x > y then
    {x > 0 & y > 0 & gcd(x, y, z) & x ≠ y & x > y}
    {x - y > 0 & y > 0 & gcd(x - y, y, z)}
    x := x - y;
    {x > 0 & y > 0 & gcd(x, y, z)}
  else
    {x > 0 & y > 0 & gcd(x, y, z) & x ≠ y & ¬(x > y)}
    {x > 0 & y - x > 0 & gcd(x, y - x, z)}
    y := y - x;
    {x > 0 & y > 0 & gcd(x, y, z)}
  fi
  {x > 0 & y > 0 & gcd(x, y, z)}
od
{x > 0 & y > 0 & gcd(x, y, z) & ¬(x ≠ y)}
{x = z}
```

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)

Если существует аннотированная программа $\tilde{\pi}$, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$ в интерпретации \mathcal{I} , то $\mathcal{I} \models \{\varphi\}\pi\{\psi\}$

Доказательство.

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

Фрагмент программы $\tilde{\pi}$ вида

$$\{x\}\emptyset\{x\}$$

соответствует фрагменту вывода

$$R_{\emptyset}: \frac{\{x\}\emptyset\{x\}}{\top}$$

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)

Если существует аннотированная программа $\tilde{\pi}$, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$ в интерпретации \mathcal{I} , то $\mathcal{I} \models \{\varphi\}\pi\{\psi\}$

Доказательство.

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

Фрагмент программы $\tilde{\pi}$ вида

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

соответствует фрагменту вывода

$$R_{:=} : \frac{\{\chi\{x/t\}\}x := t; \{\chi\}}{\text{т}}$$

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)

Если существует аннотированная программа $\tilde{\pi}$, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$ в интерпретации \mathcal{I} , то $\mathcal{I} \models \{\varphi\}\pi\{\psi\}$

Доказательство.

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

Фрагмент программы $\tilde{\pi}$ вида

$$\{x\}\{x'\}\tilde{\pi}'\{x''\}$$

соответствует фрагменту вывода

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

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)

Если существует аннотированная программа $\tilde{\pi}$, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$ в интерпретации \mathcal{I} , то $\mathcal{I} \models \{\varphi\}\pi\{\psi\}$

Доказательство.

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

Фрагмент программы $\tilde{\pi}$ вида

$$\{x\}\tilde{\pi}'\{x'\}\{x''\}$$

соответствует фрагменту вывода

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

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)

Если существует аннотированная программа $\tilde{\pi}$, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$ в интерпретации \mathcal{I} , то $\mathcal{I} \models \{\varphi\}\pi\{\psi\}$

Доказательство.

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

Фрагмент программы $\tilde{\pi}$ вида

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

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 $\tilde{\pi}$, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$ в интерпретации \mathcal{I} , то $\mathcal{I} \models \{\varphi\}\pi\{\psi\}$

Доказательство.

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

Фрагмент программы $\tilde{\pi}$ вида

$$\{x\}\mathbf{if} C \mathbf{then} \{x \ \& \ C\}\tilde{\pi}_1\{x'\} \mathbf{else} \{x \ \& \ \neg C\}\tilde{\pi}_2\{x'\} \mathbf{fi}\{x'\}$$

соответствует фрагменту вывода

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

Аннотированные программы и логика Хоара

Теорема (о корректности аннотации программ)

Если существует аннотированная программа $\tilde{\pi}$, правильно отвечающая триплету $\{\varphi\}\pi\{\psi\}$ в интерпретации \mathcal{I} , то $\mathcal{I} \models \{\varphi\}\pi\{\psi\}$

Доказательство.

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

Фрагмент программы $\tilde{\pi}$ вида

$$\{\chi\}\mathbf{while} C \mathbf{do} \{\chi \ \& \ C\}\tilde{\pi}'\{\chi\} \mathbf{od}\{\chi \ \& \ \neg C\}$$

соответствует фрагменту вывода

$$R_{\mathbf{while}}: \frac{\{\chi\}\mathbf{while} C \mathbf{do} \pi' \mathbf{od}\{\chi \ \& \ \neg C\}}{\{\chi \ \& \ C\}\pi'\{\chi\}}$$

