Математические методы верификации схем и программ

Семинар 1

Логика Хоара, Корректность программ

Упражнение 1

Построить вычисление императивной программы на заданной оценке переменных

```
x ⇐ z;
while x < y do
  if x % 2 then
    x ⇐ 3 * x + 1
  else
    x ⇐ x / 2
  fi
od
```

Оценка переменных:

1. $\{\mathrm{x}/\mathbf{15}, \mathrm{y}/\mathbf{4}, \mathrm{z}/\mathbf{1}\}$
2. $\{\mathrm{x}/\mathbf{3}, \mathrm{y}/\mathbf{1}, \mathrm{z}/\mathbf{0}\}$

Упражнение 2

Является ли программа

- частично корректной
- тотально корректной

относительно заданных триплетом предусловия и постусловия?

$$
\begin{array}{lll}
\mathbf{true} & \{x \Leftarrow 100\} & \mathbf{true} \\
\mathbf{true} & \{x \Leftarrow 100\} & \mathbf{false} \\
\mathbf{false} & \{x \Leftarrow 100\} & \mathbf{false} \\
\mathbf{false} & \{x \Leftarrow 100\} & \mathbf{true} \\
\mathbf{true} & \{x \Leftarrow 100\} & x = 100 \\
x = 50 & \{x \Leftarrow 100\} & x = 50 \\
\mathbf{false} & \{x \Leftarrow 100\} & x = 50 \\
y = 50 & \{x \Leftarrow 100\} & y = 50
\end{array}
$$

Упражнение 2

Является ли программа

- частично корректной
- тотально корректной

относительно заданных триплетом предусловия и постусловия?

$$
\begin{array}{lll}
\mathbf{true} & \{\mathbf{while}\ x > 0\ \mathbf{do}\ x \Leftarrow x - 1\ \mathbf{od}\} & \mathbf{true} \\
\mathbf{true} & \{\mathbf{while}\ x > 0\ \mathbf{do}\ x \Leftarrow x - 1\ \mathbf{od}\} & \mathbf{false} \\
\mathbf{false} & \{\mathbf{while}\ x > 0\ \mathbf{do}\ x \Leftarrow x - 1\ \mathbf{od}\} & \mathbf{false} \\
\mathbf{false} & \{\mathbf{while}\ x > 0\ \mathbf{do}\ x \Leftarrow x - 1\ \mathbf{od}\} & \mathbf{true} \\
x > 3 & \{\mathbf{while}\ x > 0\ \mathbf{do}\ x \Leftarrow x - 1\ \mathbf{od}\} & x = 0 \\
x < 3 & \{\mathbf{while}\ x > 0\ \mathbf{do}\ x \Leftarrow x - 1\ \mathbf{od}\} & x = 0 \\
x < 3 & \{\mathbf{while}\ x > 0\ \mathbf{do}\ x \Leftarrow x - 1\ \mathbf{od}\} & x = 1 \\
x < -3 & \{\mathbf{while}\ x > 0\ \mathbf{do}\ x \Leftarrow x - 1\ \mathbf{od}\} & x = 0 \\
x < -3 & \{\mathbf{while}\ x > 0\ \mathbf{do}\ x \Leftarrow x - 1\ \mathbf{od}\} & x = -7
\end{array}
$$

Упражнение 2

Является ли программа

- частично корректной
- тотально корректной

относительно заданных триплетом предусловия и постусловия?

$$\mathbf{true}\ \{\mathrm{x} \Leftarrow \mathrm{E}\}\ \mathrm{x} = \mathrm{E}$$

(E — произвольное выражение)

Упражнение 3

Записать в виде предусловия и постусловия требование корректности программы, записанное на естественном языке

1. программа записывает в переменную `prod` произведение значений `x` и `y`
2. программа записывает в переменные `quo`, `rem` частное и остаток от деления положительного значения `x` на положительное значение `y`
3. программа меняет местами значения переменных `x`, `y`
4. программа записывает в переменную `N` наибольший общий делитель значений `x`, `y`
5. программа записывает в переменную `m` максимальный элемент непустого массива $\mathtt{s}[\mathbf{0} : \mathtt{n} - \mathbf{1}]$
6. программа разворачивает непустой массив $\mathtt{s}[\mathbf{0} : \mathtt{n} - 1]$ задом наперёд

Упражнение 4

Вычислить слабейшее предусловие для заданных программы и постусловия

$$\{x \Leftarrow x + 10\}\ x = 7$$
$$\{x \Leftarrow x + 10\}\ \mathbf{true}$$
$$\{x \Leftarrow x + 10\}\ \mathbf{false}$$
$$\{x \Leftarrow x + 10\}\ x = x + 10$$
$$\{x \Leftarrow x + 10;\ y \Leftarrow x + y\}\ x = A\ \&\ y = B$$
$$\{\mathbf{if}\ x = y\ \mathbf{then}\ x \Leftarrow 7\ \mathbf{else}\ x \Leftarrow x + y + 2\}$$
$$x = A\ \&\ y = B\ \&\ z = C$$
$$\{a[1] = x\}\ \forall i\ (0 \leq i \leq n \rightarrow a[i] < 7)$$
$$\{a[y] = x\}\ a[3] = 7$$

Упражнение 5

Используя логику Хоара, доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

$$\begin{aligned} \mathrm{x} &\Leftarrow \mathrm{x} + 1; \\ \mathrm{y} &\Leftarrow \mathrm{y} + 1 \end{aligned}$$

Требование: если значения переменных x, y совпадали до выполнения программы, то будут совпадать после выполнения

Упражнение 5

Используя логику Хоара, доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

$$
\begin{aligned}
z &\Leftarrow x\,; \\
x &\Leftarrow y\,; \\
y &\Leftarrow z
\end{aligned}
$$

Требование: значения переменных $\mathtt{x}$, $\mathtt{y}$ меняются местами

Упражнение 5

Используя логику Хоара, доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

$$
\begin{aligned}
&x \Leftarrow 1;\\
&a[1] \Leftarrow 2;\\
&a[x] \Leftarrow x
\end{aligned}
$$

Требование: в первый элемент массива a записывается единица

Упражнение 5

Используя логику Хоара, доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

$$
\begin{array}{l}
x \Leftarrow 0; \\
\textbf{while } a[x] \neq 0 \textbf{ do} \\
\quad x \Leftarrow x + 1 \\
\textbf{od}
\end{array}
$$

Требование: если на вход подаётся массив $a[0:1] = [1, 0]$, то значения нолевого и первого элементов не изменяются, а значение $a[x]$ после выполнения — ноль

Разбираем подробно

$$\{a[0] = 1 \;\&\; a[1] = 0\}$$
$$x \Leftarrow 0;$$

while $a[x] \neq 0$ **do**
$\quad x \Leftarrow x + 1$
od
$$\{a[0] = 1 \;\&\; a[1] = 0 \;\&\; a[x] = 0\}$$

Разбираем подробно

$\{a[0] = 1 \;\&\; a[1] = 0\}$
$x \Leftarrow 0;$
$\{a[0] = 1 \;\&\; a[1] = 0 \;\&\; x = 0\}$ $// = \varphi;$

while $a[x] \neq 0$ **do** $//$ условие $- B$
  $x \Leftarrow x + 1$
od
$\{a[0] = 1 \;\&\; a[1] = 0 \;\&\; a[x] = 0\}$ $// = \psi$

А как искать инвариант цикла?

Это свойство *inv* цикла, которое “показывает, что всё хорошо”:

$$\varphi \to inv, \qquad inv \;\&\; B\{\dots\}inv, \qquad inv \;\&\; \neg B \to \psi$$

И что же хорошего в этом цикле?

Разбираем подробно

$\{a[0] = 1 \;\&\; a[1] = 0\}$
$x \Leftarrow 0;$
$\{a[0] = 1 \;\&\; a[1] = 0 \;\&\; x = 0\}$ // $= \varphi$
$\{inv: \; 0 \leq x \leq 1 \;\&\; a[0] = 1 \;\&\; a[1] = 0\}$
while $a[x] \neq 0$ **do** // условие $- B$
  $x \Leftarrow x + 1$
od
$\{a[0] = 1 \;\&\; a[1] = 0 \;\&\; a[x] = 0\}$ // $= \psi$

Цикл совершает всего один виток, просматривает всего два элемента, и эти элементы остаются неизменными

$$0 \leq x \leq 1 \,\&\, a[0] = 1 \,\&\, a[1] = 0$$

Разбираем подробно

$\{a[0] = 1 \;\&\; a[1] = 0\}$
$x \Leftarrow 0;$
$\{a[0] = 1 \;\&\; a[1] = 0 \;\&\; x = 0\}$ // $= \varphi$
$\{inv: 0 \leq x \leq 1 \;\&\; a[0] = 1 \;\&\; a[1] = 0\}$
while $a[x] \neq 0$ **do** // условие $- B$
  $x \Leftarrow x + 1$
od
$\{a[0] = 1 \;\&\; a[1] = 0 \;\&\; a[x] = 0\}$ // $= \psi$

$\varphi \to inv$:

$$a[0] = 1 \,\&\, a[1] = 0 \,\&\, x = 0$$
$$\to$$
$$0 \leq x \leq 1 \,\&\, a[0] = 1 \,\&\, a[1] = 0,$$

Разбираем подробно

$\{a[0] = 1 \;\&\; a[1] = 0\}$
$x \Leftarrow 0;$
$\{a[0] = 1 \;\&\; a[1] = 0 \;\&\; x = 0\}$ // $= \varphi$
$\{inv: 0 \leq x \leq 1 \;\&\; a[0] = 1 \;\&\; a[1] = 0\}$
while $a[x] \neq 0$ **do** // условие $- B$
  $x \Leftarrow x + 1$
od
$\{a[0] = 1 \;\&\; a[1] = 0 \;\&\; a[x] = 0\}$ // $= \psi$

$inv \;\&\; B\{\ldots\}inv$:

$$a[0] = 1 \;\&\; a[1] = 0 \;\&\; 0 \leq x \leq 1 \;\&\; a[x] \neq 0$$
$$\{x \Leftarrow x + 1\}$$
$$a[0] = 1 \;\&\; a[1] = 0 \;\&\; 0 \leq x \leq 1$$

Разбираем подробно

$\{a[0] = 1 \;\&\; a[1] = 0\}$
$x \Leftarrow 0;$
$\{a[0] = 1 \;\&\; a[1] = 0 \;\&\; x = 0\}$ // $= \varphi$
$\{inv: 0 \leq x \leq 1 \;\&\; a[0] = 1 \;\&\; a[1] = 0\}$
while $a[x] \neq 0$ **do** // условие $- B$
  $x \Leftarrow x + 1$
od
$\{a[0] = 1 \;\&\; a[1] = 0 \;\&\; a[x] = 0\}$ // $= \psi$

$inv \;\&\; \neg B \rightarrow \psi$

$$a[0] = 1 \;\&\; a[1] = 0 \;\&\; 0 \leq x \leq 1 \;\&\; a[x] = 0$$
$$\rightarrow$$
$$a[0] = 1 \;\&\; a[1] = 0 \;\&\; a[x] = 0$$

Разбираем подробно

$\{a[0] = 1 \;\&\; a[1] = 0\}$
$x \Leftarrow 0;$
$\{a[0] = 1 \;\&\; a[1] = 0 \;\&\; x = 0\}$ // $= \varphi$
$\{\mathsf{inv}: 0 \leq x \leq 1 \;\&\; a[0] = 1 \;\&\; a[1] = 0\}$
while $a[x] \neq 0$ **do** // условие $- B$
  $x \Leftarrow x + 1$
od
$\{a[0] = 1 \;\&\; a[1] = 0 \;\&\; a[x] = 0\}$ // $= \psi$

Оказывается, если заменить "$0 \leq x \leq 1$" на "$x \geq 0$" или вообще вычеркнуть из inv, это всё равно останется инвариантом; но в следующих примерах такие "простые" свойства не позволят доказать корректность

Разбираем подробно

$\{a[0] = 1 \;\&\; a[1] = 0\}$
$x \Leftarrow 0;$
$\{a[0] = 1 \;\&\; a[1] = 0 \;\&\; x = 0\}$ // $= \varphi$
$\{\mathsf{inv}: 0 \leq x \leq 1 \;\&\; a[0] = 1 \;\&\; a[1] = 0\}$
while $a[x] \neq 0$ **do** // условие $- B$
  $x \Leftarrow x + 1$
od
$\{a[0] = 1 \;\&\; a[1] = 0 \;\&\; a[x] = 0\}$ // $= \psi$

А как быть с тотальной корректностью?

Чтобы доказать, что цикл всегда завершает работу, достаточно предоставить выражение E над целыми числами (*ограничивающую функцию*), которое уменьшается с каждым витком цикла и при этом ограничено снизу

Например, выражение $(1-x)$ постоянно уменьшается и ограничено снизу значением 0, а значит, программа **тотально корректна**

Упражнение 5

Используя логику Хоара, доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

$$
\begin{array}{l}
\mathrm{x} \Leftarrow 2; \\
\textbf{while } \mathrm{a}[\mathrm{x}] \neq 0 \textbf{ do} \\
\quad \mathrm{x} \Leftarrow \mathrm{x} + 1 \\
\textbf{od}
\end{array}
$$

Требование: если на вход подаётся массив $\mathrm{a}[0:1] = [1, 0]$, то значения нолевого и первого элементов не изменяются, а значение $\mathrm{a}[\mathrm{x}]$ после выполнения — ноль

Упражнение 5

Используя логику Хоара, доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

```
quo ⇐ 0; rem ⇐ x;
while rem ≥ y do
  rem ⇐ rem − y;
  quo ⇐ quo + 1
od
```

Требование: в переменную `quo` записывается частное, а в переменную `rem` — остаток от деления неотрицательного значения `x` на неотрицательное значение `y`

Ответ

$$
\begin{array}{l}
\{x \geq 0 \;\&\; y \geq 0\} \\
quo \Leftarrow 0;\; rem \Leftarrow x; \\
\{x \geq 0 \;\&\; y \geq 0 \;\&\; quo = 0 \;\&\; rem = x\} \\
\{inv:\; x = quo * y + rem \;\&\; rem \geq 0\} \\
\textbf{while}\ rem \geq y\ \textbf{do} \\
\quad rem \Leftarrow rem - y; \\
\quad quo \Leftarrow quo + 1 \\
\textbf{od} \\
\{x = quo * y + rem \;\&\; 0 \leq rem < y\}
\end{array}
$$

Программа не является тотально корректной: если $y = 0$, то цикл не завершит работу

А если $y > 0$, то ограничивающая функция — rem

Упражнение 5

Используя логику Хоара, доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

```
quo ⇐ 0; rem ⇐ x;
while rem ≥ y do
  rem ⇐ rem − y;
  quo ⇐ quo + 1
od
```

Требование: в переменную `quo` записывается частное, а в переменную `rem` — остаток от деления неотрицательного значения `x` на *положительное* значение `y`

Упражнение 5

Используя логику Хоара, доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

```
pr ⇐ 0; cou ⇐ y;
while cou > 0 do
  pr ⇐ pr + x;
  cou ⇐ cou − 1
od
```

Требование: в переменную `pr` записывается произведение неотрицательных значений `x`, `y`

Упражнение 5

Используя логику Хоара, доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

```
x ⇐ 0; y ⇐ 1; cou ⇐ n;
while cou > 0 do
  h ⇐ y;
  y ⇐ x + y;
  x ⇐ h;
  cou ⇐ cou − 1;
od
```

Требование: в переменную x записывается n-е число Фибоначчи

Ничто не запрещает ввести функцию $fib(n)$, *если мы работаем с ней "логично":* $\forall n(n \geq 0 \rightarrow fib(n+2) = fib(n+1) + fib(n))$

Упражнение 5

Используя логику Хоара, доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

```
i ⇐ 1; m ⇐ s[0];
while i < n do
  if s[i] < m then
    m ⇐ s[i]
  fi;
  i ⇐ i + 1
od
```

Требование: в переменную $\mathtt{m}$ записывается максимальный элемент непустого массива $\mathtt{s}[0 : \mathtt{n} - 1]$

Упражнение 5

Используя логику Хоара, доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

```
sum ⇐ 0; i ⇐ 0;
while i < n do
    sum ⇐ sum + s[i]
od
```

Требование: в переменную $\mathtt{sum}$ записывается сумма элементов непустого массива $\mathtt{s}[0 : \mathtt{n} - 1]$

Упражнение 5

Используя логику Хоара, доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

```
i ⇐ 0;
while 2 * i < n − 1 do
    y ⇐ s[i];
    s[i] ⇐ s[n−i−1];
    s[n−i−1] ⇐ y;
    i ⇐ i + 1;
od
```

Требование: в результате работы программы массив $s[0 : n-1]$ разворачивается задом наперёд

Домашнее задание

Используя логику Хоара, доказать тотальную корректность программы, сортирующей непустой массив целых чисел $s[0 : n - 1]$ по неубыванию

```
i ⇐ n − 1;
while i > 0 do
  k ⇐ i; j ⇐ i − 1;
  while j ≥ 0 do
    if s[j] > s[k] then
      k ⇐ j
    fi;
    j ⇐ j − 1
  od;
  y ⇐ s[k]; s[k] ⇐ s[i]; s[i] ⇐ y;
  i ⇐ i − 1;
od
```

(см. подсказку про новые символы для чисел Фибоначчи)