Математические методы верификации схем и программ

Лекторы:

Захаров Владимир Анатольевич

Подымов Владислав Васильевич

e-mail рассказчика:

valdus@yandex.ru

Осень 2017

Семинар 1

Логика Хоара

Корректность программ

Соглашение по умолчанию

В условиях всех упражнений неявно подразумевается добавка

“в естественной арифметической интерпретации над целыми числами ($\mathcal{I}_{ar}$)”

Упражнение 1

Построить вычисление императивной программы на заданной оценке переменных

$$
\begin{array}{l}
\mathtt{x} := \mathtt{z}; \\
\textbf{while } \mathtt{x} < \mathtt{z} \textbf{ do} \\
\quad \textbf{if } \mathtt{x}\%\mathbf{2} \textbf{ then} \\
\quad\quad \mathtt{x} := \mathbf{3} * \mathtt{x} + \mathbf{1} \\
\quad \textbf{else} \\
\quad\quad \mathtt{x} := \mathtt{x}/\mathbf{2} \\
\quad \textbf{fi} \\
\textbf{od}
\end{array}
$$

Оценка переменных:

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

Упражнение 2

Является ли программа

- частично корректной
- тотально корректной

относительно заданных триплетом предусловия и постусловия?

$$
\begin{array}{rcl}
\{\mathbf{true}\} & \mathrm{x} := \mathbf{100} & \{\mathbf{true}\} \\
\{\mathbf{true}\} & \mathrm{x} := \mathbf{100} & \{\mathbf{false}\} \\
\{\mathbf{false}\} & \mathrm{x} := \mathbf{100} & \{\mathbf{true}\} \\
\{\mathbf{false}\} & \mathrm{x} := \mathbf{100} & \{\mathbf{false}\} \\
\{\mathbf{true}\} & \mathrm{x} := \mathbf{100} & \{\mathrm{x} = \mathbf{100}\} \\
\{\mathrm{x} = \mathbf{50}\} & \mathrm{x} := \mathbf{100} & \{\mathrm{x} = \mathbf{50}\} \\
\{\mathbf{false}\} & \mathrm{x} := \mathbf{100} & \{\mathrm{x} = \mathbf{50}\} \\
\{\mathrm{y} = \mathbf{50}\} & \mathrm{x} := \mathbf{100} & \{\mathrm{y} = \mathbf{50}\}
\end{array}
$$

Упражнение 2

Является ли программа

- частично корректной
- тотально корректной

относительно заданных триплетом предусловия и постусловия?

$$
\begin{array}{rll}
\{\textbf{true}\} & \textbf{while } \mathtt{x} \neq \mathbf{0} \textbf{ do } \mathtt{x} := \mathtt{x} - \mathbf{1} \textbf{ od} & \{\textbf{true}\} \\
\{\textbf{true}\} & \textbf{while } \mathtt{x} \neq \mathbf{0} \textbf{ do } \mathtt{x} := \mathtt{x} - \mathbf{1} \textbf{ od} & \{\textbf{false}\} \\
\{\textbf{false}\} & \textbf{while } \mathtt{x} \neq \mathbf{0} \textbf{ do } \mathtt{x} := \mathtt{x} - \mathbf{1} \textbf{ od} & \{\textbf{true}\} \\
\{\textbf{false}\} & \textbf{while } \mathtt{x} \neq \mathbf{0} \textbf{ do } \mathtt{x} := \mathtt{x} - \mathbf{1} \textbf{ od} & \{\textbf{false}\} \\
\{\mathtt{x} > \mathbf{3}\} & \textbf{while } \mathtt{x} \neq \mathbf{0} \textbf{ do } \mathtt{x} := \mathtt{x} - \mathbf{1} \textbf{ od} & \{\mathtt{x} = \mathbf{0}\} \\
\{\mathtt{x} > \mathbf{3}\} & \textbf{while } \mathtt{x} \neq \mathbf{0} \textbf{ do } \mathtt{x} := \mathtt{x} - \mathbf{1} \textbf{ od} & \{\mathtt{x} > -\mathbf{5}\} \\
\{\mathtt{x} < \mathbf{3}\} & \textbf{while } \mathtt{x} \neq \mathbf{0} \textbf{ do } \mathtt{x} := \mathtt{x} - \mathbf{1} \textbf{ od} & \{\mathtt{x} = \mathbf{0}\} \\
\{\mathtt{x} < -\mathbf{3}\} & \textbf{while } \mathtt{x} \neq \mathbf{0} \textbf{ do } \mathtt{x} := \mathtt{x} - \mathbf{1} \textbf{ od} & \{\mathtt{x} = \mathbf{5}\}
\end{array}
$$

Упражнение 2

Является ли программа

- частично корректной
- тотально корректной

относительно заданных триплетом предусловия и постусловия?

$$\{\textbf{true}\} \quad \mathtt{x} := E \quad \{\mathtt{x} = E\}$$

($\mathtt{E}$ — *произвольное выражение*)

Массивы в программах

- $\mathtt{A}[t]$ — терм, обозначающий t-й элемент массива $\mathtt{A}$
- переменные программы делятся на целочисленные и массивные
- каждая массивная переменная $\mathtt{A}$ встречается только в термах вида $\mathtt{A}[t]$
- никакая целочисленная переменная $\mathtt{x}$ не может образовывать терм $\mathtt{x}[t]$
- терм вида $\mathtt{A}[t]$ может быть записан в левой части присваивания
- оценкой переменных программы определяются значения всех целочисленных переменных, а также значения
$$\ldots, \mathtt{A}[-2], \mathtt{A}[-1], \mathtt{A}[0], \mathtt{A}[1], \mathtt{A}[2], \ldots$$
для каждой массивной переменной $\mathtt{A}$
- отношение переходов для присваивания $\mathtt{A}[t] := t'$, определяется естественным образом

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 `m` максимальное из значений $\mathtt{s}[\mathbf{0} : \mathtt{n} - \mathbf{1}]$
5. программа разворачивает задом наперёд совокупность значений $\mathtt{s}[\mathbf{0} : \mathtt{n} - \mathbf{1}]$

Новое обозначение: $\mathtt{s}[t_1, t_2]$ — это совокупность значений

$$(\mathtt{s}[t_1], \mathtt{s}[t_1 + \mathbf{1}], \ldots, \mathtt{s}[t_2])$$

Упражнение 4

Вычислить слабейшее предусловие для заданных программы и постусловия

$$\mathtt{x} := \mathtt{x} + \mathbf{10} \quad \{\mathtt{x} = 7\}$$

$$\mathtt{x} := \mathtt{x} + \mathbf{10} \quad \{\textbf{true}\}$$

$$\mathtt{x} := \mathtt{x} + \mathbf{10} \quad \{\textbf{false}\}$$

$$\mathtt{x} := \mathtt{x} + \mathbf{10} \quad \{\mathtt{x} = \mathtt{x} + 10\}$$

$$\mathtt{x} := \mathtt{x} + \mathbf{10};\ \mathtt{y} := \mathtt{x} + \mathtt{y} \quad \{\mathtt{x} = \mathtt{A} \,\&\, \mathtt{y} = \mathtt{B}\}$$

$$\textbf{if } \mathtt{x} = \mathtt{y} \textbf{ then } \mathtt{x} := \mathbf{7} \textbf{ else } \mathtt{x} := \mathtt{x} + \mathtt{y} + \mathbf{2} \textbf{ fi}$$

$$\{\mathtt{x} = \mathtt{A} \,\&\, \mathtt{y} = \mathtt{B} \,\&\, \mathtt{z} = \mathtt{C}\}$$

$$\mathtt{a}[\mathbf{1}] := \mathtt{x} \quad \{\forall \mathtt{i}\ (\mathbf{0} \leq \mathtt{i} \,\&\, \mathtt{i} \leq n \rightarrow \mathtt{a}[\mathtt{i}] < \mathbf{7})\}$$

$$\mathtt{a}[\mathtt{y}] := \mathtt{x} \quad \{\mathtt{a}[\mathbf{3}] = \mathbf{7}\}$$

Упражнение 5

Доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

Программа:

$$\begin{aligned} &\mathtt{x} := \mathtt{x} + \mathbf{1}; \\ &\mathtt{y} := \mathtt{y} + \mathbf{1} \end{aligned}$$

Требования: если значения переменных $\mathtt{x}$, $\mathtt{y}$ совпадали до выполнения программы, то будут совпадать и после выполнения

Упражнение 5

Доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

Программа:

$$\begin{aligned} &\mathtt{z} := \mathtt{x}; \\ &\mathtt{x} := \mathtt{y}; \\ &\mathtt{y} := \mathtt{z} \end{aligned}$$

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

Упражнение 5

Доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

Программа:

$$\begin{aligned} &\mathtt{x} := \mathbf{1}; \\ &\mathtt{a}[\mathbf{1}] := \mathbf{2}; \\ &\mathtt{a}[\mathtt{x}] := \mathtt{x} \end{aligned}$$

Требования: в переменную $\mathtt{a}[\mathbf{1}]$ записывается единица

Упражнение 5

Доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

Программа:

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

Требования: если на входе верно $\mathtt{a}[0:1] = (1, 0)$, то после выполнения программы значения $\mathtt{a}[0]$ и $\mathtt{a}[1]$ не изменяются, и кроме того, $\mathtt{a}[\mathtt{x}] = \mathbf{0}$

Упражнение 5

Доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

Программа:

$$
\begin{array}{l}
\mathtt{x} := \mathbf{2}; \\
\textbf{while } \mathtt{a}[\mathtt{x}] \neq \mathbf{0} \textbf{ do} \\
\quad \mathtt{x} := \mathtt{x} + \mathbf{1} \\
\textbf{od}
\end{array}
$$

Требования: если на входе верно $\mathrm{a}[0:1] = (1, 0)$, то после выполнения программы значения $\mathrm{a}[0]$ и $\mathrm{a}[1]$ не изменяются, и кроме того, $\mathrm{a}[\mathtt{x}] = \mathbf{0}$

Упражнение 5

Доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

Программа:

$$
\begin{array}{l}
\mathtt{quo} := \mathbf{0};\ \mathtt{rem} := \mathtt{x}; \\
\textbf{while}\ \mathtt{rem} \geq \mathtt{y}\ \textbf{do} \\
\quad \mathtt{rem} := \mathtt{rem} - \mathtt{y}; \\
\quad \mathtt{quo} := \mathtt{quo} + \mathbf{1} \\
\textbf{od}
\end{array}
$$

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

Упражнение 5

Доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

Программа:

$$
\begin{array}{l}
\mathtt{quo} := \mathbf{0};\ \mathtt{rem} := \mathtt{x}; \\
\textbf{while}\ \mathtt{rem} \geq \mathtt{y}\ \textbf{do} \\
\quad \mathtt{rem} := \mathtt{rem} - \mathtt{y}; \\
\quad \mathtt{quo} := \mathtt{quo} + \mathbf{1} \\
\textbf{od}
\end{array}
$$

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

Немного о тотальной корректности

Для обоснования тотальной корректности частично корректной программы достаточно доказать, что для любой оценки переменных, удовлетворяющей предусловию, число витков каждого цикла при выполнении программы конечно

Для этого достаточно для каждого цикла предоставить ограничивающую функцию (*bound function*), то есть выражение E, удовлетворяющее двум условиям:

- после выполнения одного витка цикла значение выражения E обязательно уменьшается
- значение выражения E перед каждой проверкой условия цикла ограничено снизу константой, зависящей только от оценки переменных перед началом выполнения цикла

Немного о тотальной корректности

Пример

Ограничивающей функцей для цикла

$$\textbf{while } \mathtt{x} < \mathbf{0} \textbf{ do } \mathtt{x} := \mathtt{x} + \mathbf{1} \textbf{ od}$$

и произвольной оценки переменных перед началом выполнения цикла является выражение $-\mathtt{x}$:

- значение $-\mathtt{x}$ уменьшается на единицу после каждого витка цикла
- следующий виток цикла выполняется только при условии $\mathtt{x} < \mathbf{0}$, то есть $-\mathtt{x} > \mathbf{0}$, а значит, значение $-\mathtt{x}$ перед каждой проверкой условия цикла ограничено снизу значением $\max(\mathtt{x}_0, \mathbf{0})$, где $\mathtt{x}_0$ — оценка переменной $\mathtt{x}$ перед началом выполнения цикла

Упражнение 5

Доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

Программа:

$$
\begin{array}{l}
\mathtt{pr} := \mathbf{0};\ \mathtt{cou} := \mathtt{y}; \\
\textbf{while}\ \mathtt{cou} > \mathbf{0}\ \textbf{do} \\
\quad \mathtt{pr} := \mathtt{pr} + \mathtt{x}; \\
\quad \mathtt{cou} := \mathtt{cou} - \mathbf{1} \\
\textbf{od}
\end{array}
$$

Требования: в переменную $\mathtt{pr}$ записывается произведение неотрицательных значений $\mathtt{x}$, $\mathtt{y}$

Упражнение 5

Доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

Программа:

$$
\begin{array}{l}
\mathtt{x} := \mathbf{0};\ \mathtt{y} := \mathbf{1};\ \mathtt{cou} := \mathtt{n}; \\
\textbf{while}\ \mathtt{cou} > \mathbf{0}\ \textbf{do} \\
\quad \mathtt{h} := \mathtt{y}; \\
\quad \mathtt{y} := \mathtt{x} + \mathtt{y}; \\
\quad \mathtt{x} := \mathtt{h}; \\
\quad \mathtt{cou} := \mathtt{cou} - \mathbf{1} \\
\textbf{od}
\end{array}
$$

Требования: в переменную $\mathtt{x}$ записывается $\mathtt{n}$-е число Фибоначчи, $\mathtt{n} \geq \mathbf{0}$

Упражнение 5

Доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

Программа:

$$
\begin{array}{l}
\mathtt{i} := \mathbf{1};\ \mathtt{m} := \mathtt{s}[\mathbf{0}]; \\
\textbf{while}\ \mathtt{i} < \mathtt{n}\ \textbf{do} \\
\quad \textbf{if}\ \mathtt{s}[\mathtt{i}] < \mathtt{m}\ \textbf{then} \\
\qquad \mathtt{m} := \mathtt{s}[\mathtt{i}] \\
\quad \textbf{fi}; \\
\quad \mathtt{i} := \mathtt{i} + \mathbf{1} \\
\textbf{od}
\end{array}
$$

Требования: в переменную $\mathtt{m}$ записывается максимальное из значений $\mathtt{s}[0 : \mathtt{n} - 1]$, $\mathtt{n} \geq \mathbf{1}$

Новое обозначение: **if** C **then** π **fi** — это сокращение для **if** C **then** π **else** $\emptyset$ **fi**

Упражнение 5

Доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

Программа:

$$
\begin{array}{l}
\mathtt{sum} := \mathbf{0};\ \mathtt{i} := \mathbf{0}; \\
\textbf{while}\ \mathtt{i} < \mathtt{n}\ \textbf{do} \\
\quad \mathtt{sum} := \mathtt{sum} + \mathtt{s}[\mathtt{i}]; \\
\quad \mathtt{i} := \mathtt{i} + \mathbf{1} \\
\textbf{od}
\end{array}
$$

Требования: в переменную $\mathtt{sum}$ записывается сумма значений $\mathtt{s}[0 : \mathtt{n} - 1]$, $\mathtt{n} \geq \mathbf{1}$

Упражнение 5

Доказать частичную корректность и проверить тотальную корректность программы относительно заданных требований

Программа:

$$
\begin{array}{l}
\mathtt{i} := \mathbf{0}; \\
\textbf{while } \mathbf{2} * \mathtt{i} < \mathtt{n} - \mathbf{1} \textbf{ do} \\
\quad \mathtt{y} := \mathtt{s}[\mathtt{i}]; \\
\quad \mathtt{s}[\mathtt{i}] := \mathtt{s}[\mathtt{n} - \mathtt{i} - \mathbf{1}]; \\
\quad \mathtt{s}[\mathtt{n} - \mathtt{i} - \mathbf{1}] := \mathtt{y}; \\
\quad \mathtt{i} := \mathtt{i} + \mathbf{1} \\
\textbf{od}
\end{array}
$$

Требования: массив $\mathtt{s}[0 : \mathtt{n} - 1]$ разворачивается задом наперёд, $\mathtt{n} \geq \mathbf{1}$

Challenge

Доказать тотальную корректность программы, правильная работа которой — это сортировка совокупности значений $\mathtt{s}[\mathbf{0} : \mathtt{n} - \mathbf{1}]$, $\mathtt{n} \geq \mathbf{1}$, по неубыванию

Программа:

```
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
```