Математические методы верификации схем и программ

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

Семинар 1

Дедуктивная верификация императивных программ

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

ВМК МГУ, 2022/2023, осенний семестр

Соглашение по умолчанию

Каждое упражнение сформулировано для **целочисленной арифметической интерпретации** $\mathcal{I}_{ar}$, содержащей:

- константы $0, 1, -1, 2, -2, ...$
- функциональные символы $+$, $-$, $\cdot$, $/$, $\%$, обозначающие обычные арифметические операции
- предикатные символы $=$, $\neq$, $>$, $<$, $\geq$, $\leq$, обозначающие обычные арифметические отношения

Упражнение 1

Построить вычисление заданной программы на заданной оценке

```
x := z;
while x < y do
  if x%2 > 0 then
    x := 3 · x + 1;
  else
    x := x/2;
  fi
od
```

Оценка:

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

Упражнение 2

Является ли программа в тройке Хоара

- частично корректной
- тотально корректной

относительно предусловия и постусловия тройки?

$$\{\mathtt{t}\} \quad \mathtt{x} := \mathbf{100}; \quad \{\mathtt{t}\}$$

$$\{\mathtt{t}\} \quad \mathtt{x} := \mathbf{100}; \quad \{\mathtt{f}\}$$

$$\{\mathtt{f}\} \quad \mathtt{x} := \mathbf{100}; \quad \{\mathtt{t}\}$$

$$\{\mathtt{f}\} \quad \mathtt{x} := \mathbf{100}; \quad \{\mathtt{f}\}$$

$$\{\mathtt{t}\} \quad \mathtt{x} := \mathbf{100}; \quad \{\mathtt{x} = \mathbf{100}\}$$

$$\{\mathtt{x} = \mathbf{50}\} \quad \mathtt{x} := \mathbf{100}; \quad \{\mathtt{x} = \mathbf{50}\}$$

$$\{\mathtt{f}\} \quad \mathtt{x} := \mathbf{100}; \quad \{\mathtt{x} = \mathbf{50}\}$$

$$\{\mathtt{y} = \mathbf{50}\} \quad \mathtt{x} := \mathbf{100}; \quad \{\mathtt{y} = \mathbf{50}\}$$

Упражнение 2

Является ли программа в тройке Хоара

- частично корректной
- тотально корректной

относительно предусловия и постусловия тройки?

$$\{\mathbb{t}\} \quad \textbf{while } \mathrm{x} \neq \mathbf{0} \textbf{ do } \mathrm{x} := \mathrm{x} - \mathbf{1}; \textbf{ od} \quad \{\mathbb{t}\}$$

$$\{\mathbb{t}\} \quad \textbf{while } \mathrm{x} \neq \mathbf{0} \textbf{ do } \mathrm{x} := \mathrm{x} - \mathbf{1}; \textbf{ od} \quad \{\mathbb{f}\}$$

$$\{\mathbb{f}\} \quad \textbf{while } \mathrm{x} \neq \mathbf{0} \textbf{ do } \mathrm{x} := \mathrm{x} - \mathbf{1}; \textbf{ od} \quad \{\mathbb{t}\}$$

$$\{\mathbb{f}\} \quad \textbf{while } \mathrm{x} \neq \mathbf{0} \textbf{ do } \mathrm{x} := \mathrm{x} - \mathbf{1}; \textbf{ od} \quad \{\mathbb{f}\}$$

$$\{\mathrm{x} > \mathbf{3}\} \quad \textbf{while } \mathrm{x} \neq \mathbf{0} \textbf{ do } \mathrm{x} := \mathrm{x} - \mathbf{1}; \textbf{ od} \quad \{\mathrm{x} = \mathbf{0}\}$$

$$\{\mathrm{x} > \mathbf{3}\} \quad \textbf{while } \mathrm{x} \neq \mathbf{0} \textbf{ do } \mathrm{x} := \mathrm{x} - \mathbf{1}; \textbf{ od} \quad \{\mathrm{x} > -\mathbf{5}\}$$

$$\{\mathrm{x} < \mathbf{3}\} \quad \textbf{while } \mathrm{x} \neq \mathbf{0} \textbf{ do } \mathrm{x} := \mathrm{x} - \mathbf{1}; \textbf{ od} \quad \{\mathrm{x} = \mathbf{0}\}$$

$$\{\mathrm{x} < -\mathbf{3}\} \quad \textbf{while } \mathrm{x} \neq \mathbf{0} \textbf{ do } \mathrm{x} := \mathrm{x} - \mathbf{1}; \textbf{ od} \quad \{\mathrm{x} = \mathbf{5}\}$$

Упражнение 2

Является ли программа в тройке Хоара

- частично корректной
- тотально корректной

относительно предусловия и постусловия тройки?

$$\{\Bbbt\} \quad \mathtt{x} := E; \quad \{\mathtt{x} = E\}$$

($\mathtt{E}$ — *произвольный терм*)

Упражнение 3

Предложить предусловие и постусловие, отвечающие требованию корректности программы π (в предположении, что π не содержит переменные $u_1, u_2, \ldots$):

1. выходное значение переменной `prod` — это произведение выходных значений переменных `x` и `y`
2. выходное значение переменной `prod` — это произведение входных значений переменных `x` и `y`
3. π меняет местами значения переменных `x` и `y`
4. входные значения переменных `x` и `y` и выходные значения `quo` и `rem` — это, соответственно, делимое, делитель, частное и остаток от деления
5. если входное значение n переменной `x` неотрицательно, то её выходное значение — это целая часть числа $\sqrt{n}$

Упражнение 4

Построить слабейшее предусловие для следующих программы и постусловия:

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

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

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

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

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

$$\textbf{if } \mathtt{x} = \mathtt{y} \textbf{ then } \mathtt{x} := \mathbf{7}; \textbf{ else } \mathtt{x} := \mathtt{x} + \mathtt{y} + \mathbf{2}; \textbf{ fi} \quad \{\mathtt{x} = \mathtt{A} \,\&\, \mathtt{y} = \mathtt{B} \,\&\, \mathtt{z} = \mathtt{C}\}$$

Упражнение 5

Доказать, что заданная программа частично корректна относительно заданных требований

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

Требования: если входные значения переменных $\mathtt{x}$ и $\mathtt{y}$ равны, то выходные значения также равны

Упражнение 5

Доказать, что заданная программа частично корректна относительно заданных требований

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

Требования: программа меняет местами значения переменных $\mathtt{x}$ и $\mathtt{y}$

Упражнение 5

Доказать, что заданная программа частично корректна относительно заданных требований

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

Требования: выходное значение переменной $\mathtt{pr}$ — это произведение неотрицательных входных значений переменных $\mathtt{x}$ и $\mathtt{y}$

Упражнение 5

Доказать, что заданная программа частично корректна относительно заданных требований

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

Требования: если входные значения переменных $\mathtt{x}$ и $\mathtt{y}$ соответственно положительны, то входные значения переменных $\mathtt{x}$ и $\mathtt{y}$ и выходные значения $\mathtt{quo}$ и $\mathtt{rem}$ — это, соответственно, делимое, делитель, частное и остаток от деления

Упражнение 5

Доказать, что заданная программа частично корректна относительно заданных требований

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

Требования: выходное значение переменной $\mathtt{x}$ — это $\mathtt{n}$-е число Фибоначчи (для неотрицательного входного значения переменной $\mathtt{n}$)

Немного о тотальной корректности

Чтобы доказать, что частично корректная программа тотально корректна, по определению достаточно показать, что для каждого значения входных данных, удовлетворяющего предусловию, число итераций каждого цикла конечно

Популярный и достаточно простой для понимания способ это доказать — это предоставить ограничивающу функцию (bound function) для каждого цикла: выражение (терм) E, такое что:

- множество всевозможных значений E, вычисляющихся при проверке условия цикла, ограничено снизу величиной, зависящей только от значения E непосредственно перед первой итерацией
- значение E строго уменьшается на каждой итерации цикла и не может уменьшаться бесконечно долго

Немного о тотальной корректности

Пример

Рассмотрим цикл

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

и произвольное состояние данных до выполнения этого цикла
Тогда $(-\mathtt{x})$ — ограничивающая функция для этого цикла:

- значение $-\mathtt{x}$ уменьшается на единицу на каждой итерации
- если начальное значение $\mathtt{x}$ отрицательно, то граница снизу — $\mathbf{0}$
- если начальное значение n переменной $\mathtt{x}$ неотрицательно, то граница снизу — $-n$

Упражнение 6

Доказать тотальную корректность каждой программы из упражнения 5

Массивы

$\mathtt{A}[t]$ — это терм, обозначающий t-й элемент массива $\mathtt{A}$

Переменные программы поделены на целочисленные и массивные

Каждая массивная переменная $\mathtt{A}$ используется только в термах вида $\mathtt{A}[t]$

Никакая целочисленная переменная $\mathtt{x}$ не используется в термах вида $\mathtt{x}[t]$

Терм $\mathtt{A}[t]$ может быть записан в левой части присваивания

В оценку переменных программы включены все целочисленные переменные, а также значения переменных

$$\ldots, \mathtt{A}[-2], \mathtt{A}[-1], \mathtt{A}[0], \mathtt{A}[1], \mathtt{A}[2], \ldots$$

для каждой массивной переменной $\mathtt{A}$

Отношение переходов (шаг вычисления программы) естественным образом обобщается на присваивания вида $\mathtt{A}[t] := t'$;

Упражнение 7

Предложить предусловие и постусловие, отвечающие требованию корректности программы π (в предположении, что π не содержит переменные $u_1, u_2, \ldots$):

1. π обнуляет все значения $\mathtt{s}[\mathbf{0} : \mathtt{n} - \mathbf{1}]$ (для заданного входного значения переменной $\mathtt{n}$)

2. π вычисляет в переменной $\mathtt{m}$ максимальное число среди $\mathtt{s}[\mathbf{0} : \mathtt{n} - \mathbf{1}]$ (для заданного входного значения переменной $\mathtt{n}$) и не меняет значение $\mathtt{s}$

3. π зеркально отражает набор $\mathtt{s}[\mathbf{0} : \mathtt{n} - \mathbf{1}]$ (для заданного входного значения переменной $\mathtt{n}$)

Обозначение: $\mathtt{s}[t_1 : t_2]$ — это набор значений

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

Упражнение 8

Доказать частичную корректность заданной программы относительно заданных требований и выяснить, является ли эта программа тотально корректной

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

Требования: выходное значение переменной $\mathtt{a}[\mathbf{1}]$ обязательно равно 1

Упражнение 8

Доказать частичную корректность заданной программы относительно заданных требований и выяснить, является ли эта программа тотально корректной

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

Требования: если входные значения $\mathtt{a}[0:1]$ — это набор $(1, 0)$, то

- выходные значения $\mathtt{a}[0]$ и $\mathtt{a}[1]$ равны входным и
- выходное значение $\mathtt{a}[\mathtt{x}]$ равно 0

Упражнение 8

Доказать частичную корректность заданной программы относительно заданных требований и выяснить, является ли эта программа тотально корректной

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

Требования: если входные значения $\mathtt{a}[0:1]$ — это набор $(1, 0)$, то

- выходные значения $\mathtt{a}[0]$ и $\mathtt{a}[1]$ равны входным и
- выходное значение $\mathtt{a}[\mathtt{x}]$ равно 0

Упражнение 8

Доказать частичную корректность заданной программы относительно заданных требований и выяснить, является ли эта программа тотально корректной

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

Требования: программа вычисляет в переменной $\mathtt{m}$ максимальное число среди $\mathtt{s}[\mathbf{0} : \mathtt{n} - \mathbf{1}]$

Обозначение: **if** C **then** π**fi** — это синоним записи **if** C **then** π **else** $\emptyset$ **fi**

Упражнение 8

Доказать частичную корректность заданной программы относительно заданных требований и выяснить, является ли эта программа тотально корректной

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

Требования: программа вычисляет в переменной $\mathtt{sum}$ сумму значений $\mathtt{s}[\mathbf{0} : \mathtt{n} - \mathbf{1}]$, если входное значение $\mathtt{n}$ положительно

Упражнение 8

Доказать частичную корректность заданной программы относительно заданных требований и выяснить, является ли эта программа тотально корректной

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

Требования: набор значений $\mathtt{s}[\mathbf{0} : \mathtt{n} - \mathbf{1}]$ зеркально отражается программой, если $\mathtt{n} \geq \mathbf{1}$

Challenge

Доказать тотальную корректность следующей программы

```
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
```

Требования: программа сортирует набор значений $\mathtt{s}[\mathbf{0} : \mathtt{n} - \mathbf{1}]$ по неубыванию, если $\mathtt{n} \geq \mathbf{1}$ перед началом выполнения программы