# MI-FME Cvičení 11

Tomáš Chvosta

Duben 2020

Uvažujte následující specifikaci programu:

- Input: $x, y \in \mathbb{N}_0, y \geq 1$
- Output: $xy$

$r \leftarrow x$
$i \leftarrow 1$
**while** $i < y$ **do**
    @
    $r \leftarrow r + x$
    $i \leftarrow i + 1$
@ $r = xy$
**return** $r$

## Cvičení 11a

### Zadání

Vytvořte tabulku, která bude ukazovat hodnoty proměnných $r$ a $i$ v místě programu s chybějící assertací ve všech iteracích cyklu pro nějaké netriviální vstupy $x$ a $y$.

### Řešení

Nejprve pojďme zvolit dvě libovolné hodnoty $x$ a $y$ (samozřejmě tak, aby platilo, že $x, y \in \mathbb{N}_0, y \geq 1$). Například $x = 10$ a $y = 5$. Následující tabulka zobrazuje hodnoty proměnných $i$ a $r$ v místě programu s chybějící assertací pro celý běh programu:

| $i$ | $r$ |
|---|---|
| 1 | 10 |
| 2 | 20 |
| 3 | 30 |
| 4 | 40 |

Nyní si pojďme ukázat, jak bude tabulka vypadat pro obecné hodnoty $x, y$ a $n \in \{1, ..., y-1\}$ :

| $i$ | $r$ |
|---|---|
| 1 | $x$ |
| 2 | $2x$ |
| 3 | $3x$ |
| . | . |
| . | . |
| . | . |
| $n$ | $nx$ |
| . | . |
| . | . |
| . | . |
| $y-1$ | $(y-1)x$ |

# Cvičení 11b

## Zadání

Pokuste se odhadnout chybějící assertaci uvnitř cyklu.

## Řešení

Z předchozích tabulek se můžeme pokusit odhadnout, který výraz bychom mohli doplnit do assertace na začátku cyklu. Z tabulky lze vypozorovat následující vlastnosti:

- $r = ix$
- $i < y$

Pojďme tedy tyto dvě vlastnosti doplnit do assertace na začátku cyklu. Doplněním vznikne následující program:

$r \leftarrow x$
$i \leftarrow 1$
**while** $i < y$ **do**
    @ $r = ix \wedge i < y$
    $r \leftarrow r + x$
    $i \leftarrow i + 1$
@ $r = xy$
**return** $r$

# Cvičení 11c

## Zadání

Zapište odpovídající základní cesty programu a zkontrolujte, zda platí jejich ověřovací podmínky.

## Řešení

Z programu v předchozí sekci lze vytvořit následující základní cesty programu.

### Základní cesta 1

$r \leftarrow x$
$i \leftarrow 1$
**assume** $\neg(i < y)$
@ $r = xy$

### SSA forma 1

V tomto případě není třeba zavádět nové názvy proměnných.

### Logická formule 1

$$(\forall x, y, r, i \in \mathbb{N}_0, y \geq 1)([r = x \wedge i = 1 \wedge \neg(i < y)] \Rightarrow r = xy)$$

### Ověřovací podmínka 1

Máme předpoklady $r = x$, $i = 1$, $\neg(i < y)$ a máme dokázat $r = xy$. Z předpokladů $\neg(i < y)$ a $i = 1$ můžeme vytvořit předpoklad $y \leq 1$. Jelikož však zadání definuje, že $y \geq 1$, může $y$ nabývat pouze hodnoty $y = 1$. Použijeme tedy předpoklady $r = x$ a $y = 1$ a dosadíme je do dokazované části formule $r = xy$, čímž dostaneme $x = x$, což je triviálně dokázáno. Ověřovací podmínka pro základní cestu 1 tedy platí.

### Základní cesta 2

$r \leftarrow x$
$i \leftarrow 1$
**assume** $i < y$
@ $r = ix \wedge i < y$

### SSA forma 2

V tomto případě není třeba zavádět nové názvy proměnných.

### Logická formule 2

$$(\forall x, y, r, i \in \mathbb{N}_0, y \geq 1)([r = x \wedge i = 1 \wedge i < y] \Rightarrow [r = ix \wedge i < y])$$

### Ověřovací podmínka 2

Máme předpoklady $r = x$, $i = 1$, $i < y$ a máme dokázat $r = ix \wedge i < y$, tedy dokázat zvlášť $r = ix$ a $i < y$. Můžeme si všimnout, že $i < y$ je zároveň i předpoklad, tedy tuto část máme triviálně dokázanou. Nyní použijeme předpoklady $r = x$ a $i = 1$ a dosadíme je do dokazované části formule $r = ix$, čímž dostaneme $x = x$, což je triviálně dokázáno. Ověřovací podmínka pro základní cestu 2 tedy platí.

### Základní cesta 3

**assume** $r = ix \wedge i < y$
$\quad r \leftarrow r + x$
$\quad i \leftarrow i + 1$
**assume** $i < y$
@ $r = ix \wedge i < y$

### SSA forma 3

**assume** $r = ix \wedge i < y$
$\quad r_1 \leftarrow r + x$
$\quad i_1 \leftarrow i + 1$
**assume** $i_1 < y$
@ $r_1 = i_1 x \wedge i_1 < y$

### Logická formule 3

$$(\forall x, y, r, i \in \mathbb{N}_0, y \geq 1)$$
$$([r = ix \wedge i < y \wedge r_1 = r + x \wedge i_1 = i + 1 \wedge i_1 < y] \Rightarrow [r_1 = i_1 x \wedge i_1 < y])$$

### Ověřovací podmínka 3

Máme předpoklady $r = ix$, $i < y$, $r_1 = r + x$, $i_1 = i + 1$, $i_1 < y$ a máme dokázat $r_1 = i_1 x \wedge i_1 < y$, tedy dokázat zvlášť $r_1 = i_1 x$ a $i_1 < y$. Můžeme si všimnout, že $i_1 < y$ je zároveň i předpoklad, tedy tuto část máme triviálně dokázanou. Z předpokladů $r = ix$ a $r_1 = r+x$ můžeme vytvořit nový předpoklad $r_1 = (i + 1)x$. Do tohoto předpokladu můžeme dosadit předpoklad $i_1 = i + 1$, čímž vznikne předpoklad $r_1 = i_1 x$, což jsme zároveň měli dokázat. Ověřovací podmínka pro základní cestu 3 tedy platí.

### Základní cesta 4

**assume** $r = ix \wedge i < y$
$\quad r \leftarrow r + x$
$\quad i \leftarrow i + 1$
**assume** $\neg(i < y)$
@ $r = xy$

**SSA forma 4**

**assume** $r = ix \wedge i < y$
$r_1 \leftarrow r + x$
$i_1 \leftarrow i + 1$
**assume** $\neg(i_1 < y)$
@ $r_1 = xy$

**Logická formule 4**

$$(\forall x, y, r, i \in \mathbb{N}_0, y \geq 1)$$
$$([r = ix \wedge i < y \wedge r_1 = r + x \wedge i_1 = i + 1 \wedge \neg(i_1 < y)] \Rightarrow r_1 = xy)$$

**Ověřovací podmínka 4**

Máme předpoklady $r = ix$, $i < y$, $r_1 = r + x$, $i_1 = i + 1$, $\neg(i_1 < y)$ a máme dokázat $r_1 = xy$. Z předpokladů $r = ix$ a $r_1 = r + x$ můžeme vytvořit nový předpoklad $r_1 = (i + 1)x$. Do tohoto předpokladu můžeme dosadit předpoklad $i_1 = i + 1$, čímž vznikne nový předpoklad $r_1 = i_1 x$. Dále můžeme získat z předpokladu $\neg(i_1 < y)$ předpoklad $y \leq i_1$, který můžeme následně spojit s předpokladem $i < y$, čímž získáme předpoklad $i < y \leq i_1$ z čehož zjistíme, že $y = i_1$. Tento nový předpoklad můžeme dosadit do předpokladu $r_1 = i_1 x$ a tím získat $r_1 = xy$, což jsme zároveň měli dokázat. Ověřovací podmínka pro základní cestu 4 tedy platí.

# Cvičení 11d

## Zadání

Pokud jsou všechny základní cesty programu korektní, stejně tak jako celý algoritmus, pak je úkol dokončen. V opačném případě upravte assertaci uvnitř cyklu a pokračujte předchozími dvěma úkoly, dokud nejsou všechny základní cesty korektní.

## Řešení

V předchozí sekci si můžeme všimnout, že všechny základní cesty programu jsou korektní a tím tedy i celý algoritmus.