MI-FME Cvičení 10

Tomáš Chvosta

Duben 2020

Uvažujte následující program (všechny proměnné náleží množině přirozených čísel včetně nuly):

$x_0 \leftarrow x$
$i \leftarrow 0$
while $i < n$ **do**
    @ $x = x_0 + \sum_{k=0}^{i-1} a[k]$
    $x \leftarrow x + a[i]$
    $i \leftarrow i + 1$
@ $x = x_0 + \sum_{k=0}^{n-1} a[k]$

Cvičení 10a

Zadání

Napište všechny základní cesty programu uvedeného výše. Dbejte na to, aby cesty začínající v cyklu měly na začátku odpovídající předpoklad.

Řešení

Nejprve si můžeme všimnout, že program obsahuje while cyklus s podmínkou $i < n$, pomocí které můžeme náš program rozdělit na dvě základní cesty s předpoklady, že tato podmínka platí a neplatí. Dále samotný cyklus obsahuje assertaci na svém začátku, která způsobí, že tělo cyklu také můžeme rozdělit na dvě základní cesty. Celkem tedy získáváme následující 4 základní cesty:

Základní cesta 1:

$x_0 \leftarrow x$
$i \leftarrow 0$
assume $\neg(i < n)$
@ $x = x_0 + \sum_{k=0}^{n-1} a[k]$

Zde tedy předpokládáme, že podmínka cyklu není splněna a rovnou přejdeme k assertaci na konci programu.

Základní cesta 2:

$x_0 \leftarrow x$
$i \leftarrow 0$
assume $(i < n)$
@ $x = x_0 + \sum_{k=0}^{i-1} a[k]$

Zde naopak předpokládáme, že podmínka cyklu je splněna a přejdeme na začátek cyklu k assertaci, kterou tato základní cesta končí.

Základní cesta 3:

assume $x = x_0 + \sum_{k=0}^{i-1} a[k]$
$x \leftarrow x + a[i]$
$i \leftarrow i + 1$
assume $(i < n)$
@ $x = x_0 + \sum_{k=0}^{i-1} a[k]$

Zde vidíme, že této části musela předcházet buď základní cesta 2, nebo 3 a tedy musíme na začátek zapsat příslušný předpoklad. V tomto případě se jedná o předpoklad $x = x_0 + \sum_{k=0}^{i-1} a[k]$. Na konci této základní cesty předpokládáme, že hodnota i je pořád menší než hodnota n a tedy přejdeme k assertaci na začátku cyklu, kterou tato základní cesta končí.

Základní cesta 4:

assume $x = x_0 + \sum_{k=0}^{i-1} a[k]$
$x \leftarrow x + a[i]$
$i \leftarrow i + 1$
assume $\neg(i < n)$
@ $x = x_0 + \sum_{k=0}^{n-1} a[k]$

Zde musí být na začátku opět stejný předpoklad jako u předchozí základní cesty. Na konci však předpokládáme, že podmínka cyklu není splněna, tedy hodnota i není menší než hodnota n. Přejdeme tedy k assertaci na konci programu.

Cvičení 10b

Zadání

Pro každou základní cestu vytvořte ověřovací podmínku a případně se ji pokuste dokázat.

Řešení

Všechny základní cesty vytvořené v předchozí sekci byly převedeny do SSA formy a následně byla z této formy vytvořena logická formule. Zde už budu uvádět pouze logické formule.

Základní cesta 1:

$$(\forall x, x_0, i, n, a)([x_0 = x \wedge i = 0 \wedge \neg(i < n)] \Rightarrow x = x_0 + \sum_{k=0}^{n-1} a[k])$$

Máme tedy předpoklady $x_0 = x$, $i = 0$, $\neg(i < n)$ a pokusíme se dokázat $x = x_0 + \sum_{k=0}^{n-1} a[k]$. Předpoklad $\neg(i < n)$ můžeme zapsat jako $i \geq n$. Pomocí předpokladu $i = 0$ můžeme dosazením získat nový předpoklad $n \leq 0$ a díky tomuto předpokladu víme, že horní hranice sumy $\sum_{k=0}^{n-1} a[k]$ bude menší než 0. To však nutně znamená, že $\sum_{k=0}^{n-1} a[k] = 0$ a že potřebujeme dokázat $x = x_0$, což je ale jeden z předpokladů. Ověřovací podmínka pro základní cestu 1 platí.

Základní cesta 2:

$$(\forall x, x_0, i, n, a)([x_0 = x \wedge i = 0 \wedge i < n] \Rightarrow x = x_0 + \sum_{k=0}^{i-1} a[k])$$

Máme tedy předpoklady $x_0 = x$, $i = 0$, $i < n$ a pokusíme se dokázat pravou stranu formule $x = x_0 + \sum_{k=0}^{i-1} a[k]$. Můžeme využít předpokladu $i = 0$, který dosadíme do sumy a získáme $\sum_{k=0}^{-1} a[k] = 0$. Máme tedy dokázat $x = x_0$, což je ale jeden z předpokladů. Ověřovací podmínka pro základní cestu 2 platí.

Základní cesta 3:

$$(\forall x, x_0, x_1, i, i_1, n, a)$$

$$([x = x_0 + \sum_{k=0}^{i-1} a[k] \wedge x_1 = x + a[i] \wedge i_1 = i + 1 \wedge i_1 < n] \Rightarrow x_1 = x_0 + \sum_{k=0}^{i_1-1} a[k])$$

Máme tedy předpoklady $x = x_0 + \sum_{k=0}^{i-1} a[k]$, $x_1 = x + a[i]$, $i_1 = i + 1$, $i_1 < n$ a potřebujeme dokázat $x_1 = x_0 + \sum_{k=0}^{i_1-1} a[k]$. Můžeme využít předpokladů $x = x_0 + \sum_{k=0}^{i-1} a[k]$ a $x_1 = x + a[i]$, dosadit první do druhého, čímž získáme nový předpoklad $x_1 = x_0 + \sum_{k=0}^{i} a[k]$. Pokud použijeme předpoklad $i_1 = i + 1$ a dosadíme ho do dokazovaného výrazu $x_1 = x_0 + \sum_{k=0}^{i_1-1} a[k]$, získáme $x_1 = x_0 + \sum_{k=0}^{i} a[k]$, což už je ale jeden z předpokladů. Formule je tedy dokázána a ověřovací podmínka pro základní cestu 3 platí.

Základní cesta 4:

$$(\forall x, x_0, x_1, i, i_1, n, a)$$
$$([x = x_0 + \sum_{k=0}^{i-1} a[k] \land x_1 = x + a[i] \land i_1 = i + 1 \land \neg(i_1 < n)] \Rightarrow x_1 = x_0 + \sum_{k=0}^{n-1} a[k])$$

Máme tedy předpoklady $x = x_0 + \sum_{k=0}^{i-1} a[k]$, $x_1 = x + a[i]$, $i_1 = i + 1$, $\neg(i_1 < n)$ a potřebujeme dokázat $x_1 = x_0 + \sum_{k=0}^{n-1} a[k]$. Můžeme využít předpokladů $x = x_0 + \sum_{k=0}^{i-1} a[k]$ a $x_1 = x + a[i]$, dosadit první do druhého, čímž získáme nový předpoklad $x_1 = x_0 + \sum_{k=0}^{i} a[k]$. Dále můžeme podobným způsobem využít předpoklady $i_1 = i + 1$, $\neg(i_1 < n)$ a získat nový předpoklad $i \geq n - 1$. Nyní můžeme dosadit předpoklad $x_1 = x_0 + \sum_{k=0}^{i} a[k]$ do dokazované formule $x_1 = x_0 + \sum_{k=0}^{n-1} a[k]$ a po úpravě získáme $\sum_{k=0}^{i} a[k] = \sum_{k=0}^{n-1} a[k]$, což je třeba dokázat. To však platí pouze pro $i = n - 1$, ale dle předpokladu je $i \geq n - 1$. Pro $i > n - 1$ tedy formule nemusí platit a tedy ověřovací podmínka pro základní cestu 4 neplatí.

Můžeme si ukázat jednoduchý protipříklad, pro který formule neplatí. Například tento protipříklad:

$$\{x \mapsto 40, x_0 \mapsto 10, x_1 \mapsto 70, i \mapsto 2, i_1 \mapsto 3, n \mapsto 2, a \mapsto [10, 20, 30]\}$$

Toto ohodnocení proměnných splňuje levou stranu formule, avšak nesplňuje pravou stranu. Z toho můžeme usoudit, že formule neplatí.

Cvičení 10c

Zadání

Zkontrolujte všechny ověřovací podmínky. Pokud nějaká ověřovací podmínka neplatí, upravte assertaci v cyklu tak, aby všechny ověřovací podmínky platily. Neměňte však assertaci na konci programu.

Řešení

V předchozí sekci si můžeme všimnout, že platí všechny podmínky kromě ověřovací podmínky u základní cesty 4. Tato ověřovací podmínka neplatí v případě, že $i > n - 1$ v průběhu cyklu. Podíváme-li se do původního programu, zjistíme, že k takové situaci nemůže dojít, jelikož je u while cyklu podmínka $i < n$. Stačí tedy tuto podmínku přidat i do assertace na začátku while cyklu. Program tedy po úpravě bude vypadat následovně:

$x_0 \leftarrow x$
$i \leftarrow 0$
while $i < n$ **do**

$@ \; x = x_0 + \sum_{k=0}^{i-1} a[k] \wedge i < n$
$x \leftarrow x + a[i]$
$i \leftarrow i + 1$
$@ \; x = x_0 + \sum_{k=0}^{n-1} a[k].$

Pojďme se nyní podívat, jak se změní ověřovací podmínky v předchozí sekci po této úpravě.

Změna v základní cestě 1:
Základní cesta 1 zůstává beze změny a tedy i její ověřovací podmínka.

Změna v základní cestě 2:
V závěru základní cesty přibyde $\wedge(i < n)$, což je triviálně dokázáno díky předpokladu $i < n$.

Změna v základní cestě 3:
Přibyde předpoklad $(i < n)$, který v našem případě nemá žádný vliv na platnost ověřovací podmínky.

Změna v základní cestě 4:
Přibyde předpoklad $(i < n)$, díky kterému ověřovací podmínka platí.