MI-FME Cvičení 13

Tomáš Chvosta

Duben 2020

Zadání

Uvažujte proceduru s následujícím chováním:

procedure $p(a, r, x)$
Input: $a \in \mathcal{N}, r \in \mathcal{N}, x \in \mathcal{N}$ s.t. $r \geq 0$
Output: a^* s.t. $a^* = a + rx$

Dokažte že je následující fragment programu zcela korektní (všechny proměnné jsou typu integer):

assume $x \geq 10 \wedge k \geq 5$
$p(x, 2, k)$
@ $x \geq 15$

Dodržujte metody pro zpracování volání procedur, které jsou uvedené v přednáškách. Kromě toho také používejte dokazovací pravidla pro kvantifikátory. Můžete však libovolně využívat jakékoliv znalosti ohledně proměnných typů pole a integer.

Řešení

Nejprve vytvoříme logickou formuli pro proceduru p. Jelikož procedura mění a a potřebujeme odlišný název pro vstupní a výstupní proměnnou, uvedeme vstupní a výstupní hodnotu zvlášť. Zároveň v logické formuli změníme význam p na predikát:

$$(\forall a, a^*, r, x \in \mathcal{N})((r \geq 0 \wedge p(a, a^*, r, x)) \Rightarrow a^* = a + rx)$$

Tuto formuli můžeme nyní brát jako předpoklad pro důkazy, ve kterých se bude vyskytovat naše procedura p. Pojďme si nyní převést do logické formule i náš program. Abychom něco takového mohli udělat, budeme nejprve potřebovat SSA formu:

assume $x \geq 10 \wedge k \geq 5$
assume $p(x, x_1 2, k)$
@ $x_1 \geq 15$

Je potřeba brát ohled na to, že p v SSA formě představuje predikát. Logická formule z této SSA formy bude vypadat následovně:

$$(\forall x, x_1, k \in \mathcal{N})((x \geq 10 \wedge k \geq 5 \wedge p(x, x_1, 2, k)) \Rightarrow x_1 \geq 15)$$

Z předpokladu, který popisuje proceduru p pomocí logické formule po volbě $a \leftarrow x,\ a^* \leftarrow x_1,\ r \leftarrow 2,\ x \leftarrow k$, víme:

$$(\forall x, x_1, k \in \mathcal{N})((x \geq 10 \wedge k \geq 5 \wedge x_1 = x + 2k) \Rightarrow x_1 \geq 15)$$

Máme tedy tři předpolady $x \geq 10$, $k \geq 5$, $x_1 = x + 2k$ a máme dokázat $x_1 \geq 15$. Můžeme využít předpokladu $x_1 = x + 2k$ a upravit dokazovaný výraz na tvar $x + 2k \geq 15$. To můžeme snadno dokázat sporem. Předpokládáme tedy $\neg(x + 2k \geq 15)$, což je $x + 2k < 15$ a najdeme spor. Tento předpoklad můžeme upravit na tvar $2k < 15 - x$. Dále předpoklad $k \geq 5$ upravíme na tvar $2k \geq 10$. Složením předpokladů $2k < 15 - x$ a $2k \geq 10$ získáme $10 \leq 2k < 15 - x$ tedy $10 < 15 - x$, což můžeme upravit na tvar $x < 5$. To je však spor s předpokladem $x \geq 10$. Logická formule tedy platí a program je korektní.