MI-FME Cvičení 12

Tomáš Chvosta

Duben 2020

Zadání

Uvažujte funkci s následujícím chováním:

function $s(a, k)$
Input: $a \in \mathcal{A}, k \in \mathcal{N}$ s.t. $k \geq 1$
Output: $1 + \sum_{i \in \{0,\ldots,k-1\}} a[i]$

Dokažte že je následující program zcela korektní (p je pole proměnných typu integer, ostatní proměnné jsou typu integer):

assume $\forall i \,.\, p[i] \geq 5$
$r \leftarrow s(p, 2)$
@ $r \geq 8$

Dodržujte metody pro zpracování volání funkcí, 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 si můžeme všimnout, že výstup ve specifikaci funkce nemá přiřazený žádný název, tedy žádnou výstupní proměnnou. Upravíme tedy specifikaci na následující tvar:

function $s(a, k)$
Input: $a \in \mathcal{A}, k \in \mathcal{N}$ s.t. $k \geq 1$
Output: r s.t. $r = 1 + \sum_{i \in \{0,\ldots,k-1\}} a[i]$

Upravená specifikace poté odpovídá následující logické formuli:

$$(\forall a \in \mathcal{A}, k, r \in \mathcal{N})((k \geq 1 \land r = s(a, k)) \Rightarrow (r = 1 + \sum_{i=0}^{k-1} a[i]))$$

Tuto formuli můžeme nyní brát jako předpoklad pro důkazy, ve kterých se bude vyskytovat naše funkce s. Pojďme si nyní převést do logické formule i náš program. Program je v SSA formě, takže rovnou získáváme logickou formuli:

$$(\forall i, r \in \mathcal{N}, p \in \mathcal{A})((p[i] \geq 5 \wedge r = s(p, 2)) \Rightarrow (r \geq 8))$$

Z předpokladu, který popisuje funkci s po volbě $a \leftarrow p,\ k \leftarrow 2$, víme:

$$(\forall i, r \in \mathcal{N}, p \in \mathcal{A})((p[i] \geq 5 \wedge r = 1 + \sum_{i=0}^{1} p[i]) \Rightarrow (r \geq 8))$$

Máme tedy předpoklady $p[i] \geq 5$ a $r = 1 + p[0] + p[1]$ a máme dokázat $r \geq 8$. Víme, že předpoklad $p[i] \geq 5$ platí pro všechna i, po volbách $i \leftarrow 0$ a $i \leftarrow 1$ získáváme nové předpoklady $p[0] \geq 5$ a $p[1] \geq 5$. Dále můžeme využít předpoklad $r = 1 + p[0] + p[1]$ a upravit dokazovaný výraz na tvar $1 + p[0] + p[1] \geq 8$ tedy $p[0] + p[1] \geq 7$. To můžeme dokázat například sporem. Předpokládáme $\neg(p[0] + p[1] \geq 7)$ tedy $p[0] + p[1] < 7$ a pokusíme se najít spor. Tento nový předpoklad můžeme upravit na tvar $p[0] - 7 < -p[1]$. Dále pak předpoklad $p[1] \geq 5$ upravíme a získáme předpoklad $-p[1] \leq -5$ a také upravíme předpoklad $p[0] \geq 5$ a získáme předpoklad $p[0] - 7 \geq 5 - 7$ tedy $p[0] - 7 \geq -2$. Pokud spojíme předpoklady $p[0] - 7 < -p[1]$, $-p[1] \leq -5$ a $p[0] - 7 \geq -2$ získáme $-2 \leq p[0] - 7 < -p[1] \leq -5$ tedy $-2 \leq -5$, čímž jsme došli ke sporu a naše formule platí. Program je tedy korektní.