Programozáselmélet

9. gyakorlat

Boda Bálint

2022. őszi félév

3. (10. feladatsor) Lássa be, hogy az S program megoldja a következő feladatot:

$A = (x : \mathbb{Z}^n)$
$B = (x' : \mathbb{Z}^n)$
$Q = (x = x')$
$R = (\forall k \in [1..n] : x[k] = x'[k] + 1)$

Informálisan: adott egy egész számokat tartalmazó vektor. Növeljük meg az összes elemét eggyel.

Az program állapottere $(x : \mathbb{Z}^n, i : \mathbb{N})$.

S

$i := 1$
$i \neq n+1$
$\quad x[i] := x[i] + 1$
$\quad i := i + 1$

$Q' = (Q \wedge i = 1)$ a szekvencia közbülső állítása

$Q'' \wedge n+1-i = t_0$ a ciklusmag mint szekvencia közbülső állítása, ahol $Q'' = P^{i \leftarrow i+1}$

Legyen továbbá:

$t = n + 1 - i$ a termináló függvény és

$P = (\forall k \in [1..i-1] : x[k] = x'[k] + 1 \wedge i \in [1..n+1] \wedge \forall k \in [i..n] : x[k] = x'[k])$ a ciklusinvariáns.

Megoldás.

A szekvencia levezetési szabálya szerint azt kell belátni, hogy:

1. $Q \implies \mathrm{lf}\,(i := 1, Q')$

$$Q \implies (Q')^{i \leftarrow 1}$$
$$Q \implies (Q \wedge 1 = 1)\checkmark$$

2. $Q' \implies \mathrm{lf}\,(DO, R)$, ahol DO jelöli a struktogramban szereplő ciklust.
A ciklus levezetési szabálya alapján:

(a) $Q' \implies P$. Q' miatt $i = 1$, így:

$$(Q \wedge i = 1) \implies (\underbrace{\forall k \in [1..0] : x[k] = x'[k] + 1}_{\forall x \in \emptyset \text{ típusú állítás igaz}} \wedge \underbrace{1 \in [1..n+1]}_{\substack{n \text{ egy tömb hossza} \\ \text{ezért:} n \geq 0 \text{ tehát az} \\ \text{intervallum mindig} \\ \text{tartalmazza egyet}}} \wedge \underbrace{\forall k \in [1..n] : x[k] = x'[k]}_{\iff x = x' \text{, ami } Q})$$

$$(Q \wedge i = 1) \implies Q\checkmark$$

(b) $(P \wedge \neg\pi) \implies R$. Mivel $\neg\pi \iff (i = n+1)$:

$$(\underbrace{\forall k \in [1..n] : x[k] = x'[k] + 1}_{R} \wedge \underbrace{n+1 \in [1..n+1]}_{igaz} \wedge \underbrace{\forall k \in [n+1..n] : x[k] = x'[k]}_{\forall x \in \emptyset \text{:... igaz}}) \implies R\checkmark$$

(c) $P \implies (\pi \vee \neg\pi)$

$$P \implies \big((i \neq n+1) \vee (i = n+1)\big)$$

Ez nyilván teljesül, mert az egyenlőségvizsgálat eredménye csak igaz vagy hamis lehet.

(d) $(P \wedge \pi) \implies t > 0$. π miatt $i \neq n+1$ így:

$$(\forall k \in [1..i-1] : x[k] = x'[k] + 1 \wedge \underline{i \in [1..n]} \wedge \forall k \in [i..n] : x[k] = x'[k]) \implies n + 1 - i > 0$$

Mivel i értéke maximum n lehet ezért $n + 1 - i > 0$.

(e) $(P \wedge \pi \wedge t = t_0) \implies \mathrm{lf}(S_0, P \wedge t < t_0)$, ahol S_0 a DO ciklus ciklusmagja.
Így a szekvencia levezetési szabálya alapján:

i. $(P \wedge \pi \wedge t = t_0) \implies \mathrm{lf}(x[i] \coloneqq x[i] + 1, Q'' \wedge n + 1 - i = t_0)$

$$\begin{aligned} Q'' &= P^{i \leftarrow i+1} \\ &= (\forall k \in [1..i] : x[k] = x'[k] + 1 \wedge i + 1 \in [1..n+1] \wedge \forall k \in [i+1..n] : x[k] = x'[k]) \\ &= \begin{pmatrix} \forall k \in [1..i-1] : x[k] = x'[k] + 1 \wedge \\ x[i] = x'[i] + 1 \wedge \\ i + 1 \in [1..n+1] \wedge \\ \forall k \in [i+1..n] : x[k] = x'[k] \end{pmatrix} \end{aligned}$$

Mivel értékadás tömbelemekkel dolgozik be kell vezetünk az $i \in [1..n]$ feltételt, hogy elkerüljük a túlindexelést. Így:

$$(P \wedge \pi \wedge n + 1 - i = t_0) \implies (Q'' \wedge n + 1 - i = t_0 \wedge i \in [1..n])^{x[i] \leftarrow x[i]+1}$$

Elvégezve a behelyettesítést:

$$(P \wedge \pi \wedge \underline{n + 1 - i = t_0}) \implies \left((Q'')^{x[i] \leftarrow x[i]+1} \wedge \underline{n + 1 - i = t_0} \wedge i \in [1..n]\right)$$

Az aláhúzott rész mindkét oldalon teljesül ezért az kell még belátni, hogy:

$$\begin{pmatrix} \forall k \in [1..i-1] : x[k] = x'[k] + 1 \wedge \\ i \in [1..n+1] \wedge \\ \forall k \in [i..n] : x[k] = x'[k] \wedge \\ i \neq n+1 \end{pmatrix} \implies \begin{pmatrix} \forall k \in [1..i-1] : x[k] = x'[k] + 1 \wedge \\ x[i] + 1 = x'[i] + 1 \wedge \\ i + 1 \in [1..n+1] \wedge i \in [1..n] \wedge \\ \forall k \in [i+1..n] : x[k] = x'[k] \end{pmatrix}$$

Összevonva a bal oldal $i \in [1..n+1]$ és $i \neq n+1$ feltételét:

$$\begin{pmatrix} \underline{\forall k \in [1..i-1] : x[k] = x'[k] + 1} \wedge \\ i \in [1..n] \wedge \\ \forall k \in [i..n] : x[k] = x'[k] \wedge \end{pmatrix} \implies \begin{pmatrix} \underline{\forall k \in [1..i-1] : x[k] = x'[k] + 1} \wedge \\ x[i] + 1 = x'[i] + 1 \wedge \\ i + 1 \in [1..n+1] \wedge i \in [1..n] \wedge \\ \forall k \in [i+1..n] : x[k] = x'[k] \end{pmatrix}$$

Az első állítás mindkét oldalon szerepel, azzal több teendőnk nincs. Az $i \in [1..n]$ állítás szintén megtalálható mindkét oldalon. Nyilván emiatt a jobb oldal $i + 1 \in [1..n+1]$ állítása igaz lesz. Vegyük észre, hogy, ha azt mondjuk, hogy $x[i] + 1 = x'[i] + 1$, az ugyan az mintha azt mondanánk, hogy $x[i] = x'[i]$, ezért ezt a feltételt összevonhatjuk a $\forall k \in [i+1..n] : x[k] = x'[k]$ kifejezéssel. Így a két oldal megegyezik:

$$\begin{pmatrix} \forall k \in [1..i-1] : x[k] = x'[k] + 1 \wedge \\ i \in [1..n] \wedge \\ \forall k \in [i..n] : x[k] = x'[k] \wedge \end{pmatrix} \implies \begin{pmatrix} \forall k \in [1..i-1] : x[k] = x'[k] + 1 \wedge \\ i + 1 \in [1..n+1] \wedge i \in [1..n] \wedge \\ \forall k \in [i..n] : x[k] = x'[k] \end{pmatrix}$$

ii. $Q'' \wedge n + 1 - i = t_0 \implies \mathrm{lf}(i \coloneqq i + 1, P \wedge (t < t_0))$

$$\begin{aligned} Q'' \wedge n + 1 - i = t_0 &\implies \mathrm{lf}(i \coloneqq i + 1, P \wedge (n + 1 - i < t_0)) \\ Q'' \wedge n + 1 - i = t_0 &\implies (P \wedge (n + 1 - i < t_0))^{i \leftarrow i+1} \\ P^{i \leftarrow i+1} \wedge n + 1 - i = t_0 &\implies (P^{i \leftarrow i+1} \wedge n + 1 - (i+1) < t_0) \\ P^{i \leftarrow i+1} \wedge n + 1 - i = t_0 &\implies (P^{i \leftarrow i+1} \wedge n - i < t_0) \end{aligned}$$

Mivel $t_0 = n + 1 - i$, ezért $n - i < n - i + 1$ nyilván teljesül.

Így S megoldja a specifikált feladatot.

2. Lássa be, hogy az S program megoldja a következő feladatot:

$$A = (n : \mathbb{N}, s : \mathbb{N}) \qquad Fib(n) = \begin{cases} 0 & \text{ha } n = 1 \\ 1, & \text{ha } n = 2 \\ Fib(n-1) + Fib(n-2), & \text{ha } n > 2 \end{cases}$$

$$B = (n' : \mathbb{N})$$

$$Q = (n = n' \wedge n > 2)$$

$$R = (Q \wedge s = Fib(n))$$

Informálisan: Adjuk meg az n. Fibonacci számot.

Az program állapottere $(n : \mathbb{N}, s : \mathbb{N}, z : \mathbb{N}, i : \mathbb{N})$.

S

$i, s, z := 3, 1, 0$
$i \leq n$
$\quad i, s, z := i + 1, s + z, s$

$Q' = (Q \wedge i = 3 \wedge s = 1 \wedge z = 0)$ a szekvencia közbülső állítása

Legyen továbbá:

$t = n + 1 - i$ a termináló függvény és

$P = (Q \wedge s = Fib(i-1) \wedge z = Fib(i-2) \wedge i \in [3..n+1])$ a ciklusinvariáns.

Megoldás.

A szekvencia levezetési szabálya alapján a következőket kell belátni:

1. $Q \implies \mathrm{lf}(i, s, z := 3, 1, 0; Q')$

$$Q \implies (Q \wedge i = 3 \wedge s = 1 \wedge z = 0)^{i \leftarrow 3, s \leftarrow 1, z \leftarrow 0}$$

$$Q \implies (Q \wedge 3 = 3 \wedge 1 = 1 \wedge 0 = 0)\checkmark$$

2. $Q' \implies \mathrm{lf}(S_2, R)$, ahol S_2 egy ciklus ezért a ciklus levezetési szabálya alapján:

(a) $Q' \implies P$

$$(Q \wedge \underline{i = 3 \wedge s = 1 \wedge z = 0}) \implies (Q \wedge s = Fib(i-1) \wedge z = Fib(i-2) \wedge i \in [3..n+1])$$

$$(Q \wedge i = 3 \wedge s = 1 \wedge z = 0) \implies (Q \wedge \underbrace{1 = Fib(2)}_{\checkmark} \wedge \underbrace{0 = Fib(1)}_{\checkmark} \wedge \underbrace{3 \in [3..n+1]}_{\checkmark})\checkmark$$

(b) $(P \wedge \neg\pi) \implies R$

$$\big((Q \wedge s = Fib(i-1) \wedge z = Fib(i-2) \underbrace{\wedge i \in [3..n+1]) \wedge i > n}_{i>n \text{ csak akkor lehet ha } i=n+1}\big) \implies (Q \wedge s = Fib(n))$$

$$\big((Q \wedge s = Fib(i-1) \wedge z = Fib(i-2) \wedge \underline{i = n+1}\big) \implies (Q \wedge s = Fib(n))$$

$$\big((Q \wedge s = Fib(n) \wedge z = Fib(n-1)\big) \implies (Q \wedge s = Fib(n))$$

A bal oldal a jobb oldal egy szigorúbb változata ezért a maga után vonás igaz. ✓

(c) $P \implies (\pi \vee \neg\pi)$

$$\big(Q \wedge s = Fib(i-1) \wedge z = Fib(i-2) \wedge i \in [3..n+1]\big) \implies (i \leq n \vee i > n)$$

$$\big(Q \wedge s = Fib(i-1) \wedge z = Fib(i-2) \wedge i \in \underbrace{[3..n+1]}_{\substack{Q \text{ miatt mindig} \\ \text{tartalmazza 3-at}}}\big) \implies (i \leq n \vee i > n)$$

A bal oldal igaz a jobb oldal pedig minden lehetséges esetet lefed ezért a feltétel teljesül. ✓

(d) $(P \wedge \pi) \implies t > 0$

$$\Big((Q \wedge s = Fib(i-1) \wedge z = Fib(i-2) \wedge \underbrace{i \in [3..n+1]) \wedge i \leq n}_{\substack{i \text{ maximum n lehet, ezért} \\ \text{a jobb oldal mindig pozitív}}}\Big) \implies n+1-i > 0 \checkmark$$

(e) $(P \wedge \pi \wedge t = t_0) \implies \operatorname{lf}(i, s, z := i+1, s+z, s; P \wedge t < t_0)$

$$(P \wedge \pi \wedge t = t_0) \implies (P \wedge t < t_0)^{i \leftarrow i+1, s \leftarrow s+z, z \leftarrow s}$$
$$(P \wedge \pi \wedge t = t_0) \implies (Q \wedge s+z = Fib(i) \wedge s = Fib(i-1) \wedge i+1 \in [3..n+1] \wedge n+i < t_0)$$

A bal oldalból tudjuk, hogy: $t_0 = n+1-i$, így a termináló függvény csökkenésére vonatkozó feltétel nyilván teljesül. Így már csak a következőt kell belátni:

$$\begin{aligned} & Q \wedge s = Fib(i-1) \wedge z = Fib(i-2) \wedge i \in [3..n+1] \wedge i \leq n \\ \implies & Q \wedge s+z = Fib(i) \wedge s = Fib(i-1) \wedge i+1 \in [3..n+1] \end{aligned}$$

Átalakítva a bal oldalt és $i \leq n$ miatt:

$$\begin{aligned} & Q \wedge s = Fib(i-1) \wedge z = Fib(i-2) \wedge i \in [3..n] \\ \implies & Q \wedge s+z = Fib(i) \wedge s = Fib(i-1) \wedge i \in [2..n] \end{aligned}$$

További átalakítások után:

$$\begin{aligned} & Q \wedge s = Fib(i-1) \wedge z = Fib(i-2) \wedge i \in [3..n] \\ \implies & Q \wedge s = Fib(i-1) \wedge z = Fib(i) - s \wedge i \in [2..n] \end{aligned}$$

Q miatt tudjuk, hogy $n > 2$ ezért, mivel $2 < i \leq n$ ezért $s = Fib(i-1)$ így:

$$\begin{aligned} & Q \wedge s = Fib(i-1) \wedge z = Fib(i-2) \wedge i \in [3..n] \\ \implies & Q \wedge s = Fib(i-1) \wedge z = Fib(i) - Fib(i-1) \wedge i \in [2..n] \end{aligned}$$

Mivel $n > 2$, $Fib(i) = Fib(i-1) + Fib(i-2)$, ezért $Fib(i-2) = Fib(i) - Fib(i-1)$:

$$\begin{aligned} & Q \wedge s = Fib(i-1) \wedge z = Fib(i-2) \wedge i \in [3..n] \\ \implies & Q \wedge s = Fib(i-1) \wedge z = Fib(i-2) \wedge i \in [2..n] \end{aligned}$$

A bal oldalon a jobb oldal egy szigorúbb változata van, ezért a maga után vonás igaz. ✓

Így az S program megoldja a feladatot.