Programozáselmélet

8. gyakorlat

Boda Bálint

2022. őszi félév

Bár sok program helyessége könnyen belátható a megoldás definíciójával vagy a specifikáció tételével, könnyű meggondolni, hogy kellően bő állapotterekre ez a két módszer lehetetlenül sok számolást igényelne. Az alábbi tételek a specifikáció tételének $\forall b \in B : Q_b \implies \text{lf}(S, R))$ feltételének belátására használhatók.

1. A szekvencia levezetési szabálya

Tétel. Legyen $S = (S_1; S_2)$, ahol A az S_1 és S_2 programok közös állapottere. Legyenek továbbá Q, R, Q' logikai függvények A-n. Ekkor, ha

1. $Q \implies \text{lf}(S_1, Q')$
2. $Q' \implies \text{lf}(S_2, R)$

akkor $Q \implies \text{lf}(S, R))$.

Megjegyzés. A tétel azt fejezi ki, hogy a program egy olyan pontról ahol Q igaz el tud jutni egy olyan pontra, ahol igaz R egy közbülső Q' logikai feltételen keresztül.

2. Az elágazás levezetési szabálya

Legyen $IF = (\pi_1 : S_1, \ldots, \pi_n : S_n)$ a közös A állapotterű S_i programokból képzett A feletti π_i logikai függvényekkel meghatározott elágazás. Legyenek továbbá Q és R logikai függvények. Ha

1. $Q \implies \bigvee_{i=1}^{n} \pi_i$ (ha Q igaz legalább az egyik feltétel teljesül)
2. $Q \implies \bigwedge_{i=1}^{n} (\pi_i \vee \neg\pi_i)$ (ha Q igaz minden feltétel kiértékelhető)
3. $\forall i \in [1..n] : (Q \wedge \pi_i) \implies \text{lf}(S_i, R)$

akkor $Q \implies \text{lf}(IF, R)$.

3. A ciklus levezetési szabálya

Definíció (ciklusinvariáns)**.** Legyen $DO = (\pi, S_0)$ egy ciklus az A állapottér felett. Ekkor ciklusinvariánsnak nevezzük P a logikai feltétel, ha a DO ciklus minden végrehajtása esetén P igaz.

Definíció (termináló függvény)**.** Legyen $DO = (\pi, S_0)$ egy ciklus az A állapottér felett. Ekkor termináló függvénynek nevezzük a $t : A \to \mathbb{Z}$ függvényt, ha a DO ciklus minden végrehajtása esetén a t függvénye értéke kisebb lesz mint az előző végrehajtás esetén.

Tétel (ciklus levezetési szabálya)**.** Legyen $DO = (\pi, S_0)$ egy ciklus az A állapottér felett. Továbbá legyenek P, Q és R logikai függvények A-n és $t : A \to \mathbb{Z}$ függvény adottak. Ha

1. $Q \implies P$
   (ha az előfeltétel teljesül akkor a ciklusinvariáns is)

2. $P \land \neg\pi \implies R$
   (ha a ciklusinvariáns teljesül de a ciklusfeltétel nem akkor az utófeltétel teljesül)

3. $P \implies \pi \lor \neg\pi$
   (ha a ciklusinvariáns teljesül akkor a ciklusfeltétel kiértékelhető)

4. $P \land \pi \implies t > 0$
   (ha a ciklusinvariáns teljesül akkor a termináló függvény értéke pozitív)

5. $P \land \pi \implies \mathrm{lf}(S_0, P)$
   (ha a ciklusinvariáns és a ciklusfeltétel teljesül, akkor a program helyesen terminál úgy az invariáns igaz marad)

6. $P \land \pi \land t = t_0 \implies \mathrm{lf}(S_0, t < t_0)$
   (ha a ciklusinvariáns, a ciklusfeltétel és $t = t_0$ teljesül, akkor a program helyesen terminál úgy hogy csökken a termináló függvény értéke)

akkor $Q \implies \mathrm{lf}(DO, R)$

Megjegyzés. A tétel 5. és 6. pontjai összevonhatóak a következő módon:

$$P \land \pi \land t = t_0 \implies \mathrm{lf}(S_0, t < t_0) \land lf(S_0, P) = \mathrm{lf}(S_0, P \land t < t_0)$$

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

$$
\begin{aligned}
A &= \big(x : \mathbb{N}^+, l : \mathbb{L}\big)\\
B &= \big(x' : \mathbb{N}^+\big)\\
Q &= (x = x' \,\wedge\, x > 1)\\
R &= (Q \,\wedge\, l = (\forall j \in [2..x-1] : j \not| \, x))
\end{aligned}
$$

Az program állapottere $(x : \mathbb{N}^+, k : \mathbb{N}^+, l : \mathbb{L})$.

S

$k, l := 2, igaz$	
$k \neq x$	
	$l := l \,\wedge\, k \not| \, x$
	$k := k + 1$

$Q' = (Q \wedge k = 2 \wedge l = igaz)$ a szekvencia közbülső állítása

$Q'' = (Q \wedge l = (\forall j \in [2..k] : j \not| \, x) \wedge k+1 \in [2..x] \wedge x - k = t_0)$ a ciklusmag mint szekvencia közbülső állítása

Legyen továbbá: $t = x - k$ a termináló függvény és

$P = (Q \wedge l = (\forall j \in [2..k-1] : j \not| \, x) \wedge k \in [2..x])$ a ciklusinvariáns.

Megoldás.

A szekvencia levezetési szabálya alapján a program helyes, ha:

1. $Q \implies \mathrm{lf}(S_1, Q')$

$$
\begin{aligned}
Q &\implies \mathrm{lf}(k, l := 2, igaz; (Q \wedge k = 2 \wedge l = igaz))\\
Q &\implies Q^{k \leftarrow 2, l \leftarrow igaz}\\
Q &\implies Q \wedge 2 = 2 \wedge igaz = igaz \text{ ami nyilván teljesül}
\end{aligned}
$$

2. $Q' \implies \mathrm{lf}(S_2, R)$ S_2 egy ciklus ezért a ciklus levezetési szabályát kell használnunk:

(a) $Q' \implies P$

$$
\begin{aligned}
\big(Q \wedge \underline{k = 2 \wedge l = igaz}\big) &\implies (Q \wedge l = (\forall j \in [2..k-1] : j \not| \, x) \wedge k \in [2..x])\\
Q' &\implies (Q \wedge igaz = \underbrace{(\forall j \in [2..1] : j \not| \, x)}_{\forall x \in \emptyset : \cdots \iff igaz} \wedge \underbrace{2 \in [2..x]}_{\substack{Q \text{ miatt } x>1 \\ \text{ezért } \forall x \in \mathbb{N}: \\ 2 \in [2..x]}})
\end{aligned}
$$

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

$$
\begin{aligned}
&(Q \wedge l = (\forall j \in [2..k-1] : j \not| \, x) \wedge k \in [2..x] \wedge \underline{k = x}) \implies R\\
&(Q \wedge l = (\forall j \in [2..x-1] : j \not| \, x) \wedge \underbrace{x \in [2..x]}_{\iff x>1}) \implies R\\
&(Q \wedge l = (\forall j \in [2..x-1] : j \not| \, x)) \implies (Q \,\wedge\, l = (\forall j \in [2..x-1] : j \not| \, x))
\end{aligned}
$$

(c) $P \implies \pi \vee \neg\pi$ Mivel $k, x \in \mathbb{N}^+$ ezért minden esetben kiértékelhetők, ezért az állítás teljesül.

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

$$(Q \land l = (\forall j \in [2..k-1] : j \nmid x) \land k \in \underline{[2..x]} \land \underline{x \neq k}) \implies x - k > 0$$
$$(Q \land l = (\forall j \in [2..k-1] : j \nmid x) \land k \in \underbrace{[2..x-1]}_{x>k}) \implies x - k > 0$$

Mivel $x > k$ ezért $x - k > 0$

(e) $P \land \pi \land t = t_0 \implies \text{lf}\,(S_0, P \land t < t_0)$, ahol S_0 az S_2 ciklusmagja

$$(P \land x \neq k \land x - k = t_0) \implies \text{lf}\,(S_0, P \land x - k < t_0)$$

S_0 egy szekvencia ezért a következőket kell belátni:

i. $(P \land x \neq k \land x - k = t_0) \implies \text{lf}((l := l \land k \nmid x), Q'')$

$$(P \land x \neq k \land x - k = t_0) \implies Q''^{l \leftarrow l \land k \nmid x}$$
$$\big(\underline{Q} \land l = (\forall j \in [2..k-1] : j \nmid x) \land k \in [2..x] \land x \neq k \land \underline{x - k = t_0}\big)$$
$$\implies \big(\underline{Q} \land (l \land k \nmid x) = (\forall j \in [2..k] : j \nmid x) \land k + 1 \in [2..x] \land \underline{x - k = t_0}\big)$$

Átalakítva az $\forall j \in [2..k]$ tagot:

$$(l \land k \nmid x) = ((\forall j \in [2..k-1] : j \nmid x) \land k \nmid x) \land k + 1 \in [2..x]$$

Az invariánsból tudjuk, hogy $l = (\forall j \in [2..k-1] : j \nmid x)$, ezért:

$$(l \land k \nmid x) = (l \land k \nmid x) \land k + 1 \in [2..x]$$

Így már csak azt kell belátni, hogy:

$$k \in [2..x] \land k \neq x \implies k + 1 \in [2..x]$$
$$k \in [2..x-1] \implies k + 1 \in [3..x]$$

Ami igaz mert $[3..x] \subset [2..x]$.

ii. $Q'' \implies \text{lf}\,(k := k + 1, P \land x - k < t_0)$

$$Q'' \implies (P \land x - k < t_0)^{k \leftarrow k+1}$$
$$Q'' \implies (\underbrace{(Q \land l = (\forall j \in [2..k] : j \nmid x) \land k + 1 \in [2..x])}_{Q'' \text{ része}} \land x - k - 1 < t_0)$$

Tudjuk továbbá, Q'' miatt, hogy $x - k = t_0$ így:

$$x - k - 1 < t_0 \iff t_0 - 1 < t_0$$

ami nyilván igaz.

Így a specifikáció tétele alapján S megoldja a feladatot.