Szükséges fogalmak

Teljes helyesség leírása Hoare-hármassal

Amit eddig úgy jelöltünk hogy $Q \implies lf(S, R)$, jelölhetjük egy Hoare-hármassal is, a jelentésük ugyanaz: Q feltételnek eleget tevő állapotokból indulva garantált hogy az S program minden végrehajtása helyesen terminál, méghozzá olyan állapotban ahol R teljesül.

$$\{\{Q\}\}S\{\{R\}\}$$

Új programkonstrukciók levezetési szabályai

Továbbra is szekvenciális programokkal foglalkozunk, de bevezettünk három új programkonstrukciót. Ezeknek megadjuk a levezetési szabályait $\frac{a}{b}$ alakban, ami azt jelöli hogy a teljesülése esetén b-re tudunk következtetni. Vagy másképp: ahhoz hogy b-t belássuk, elegendő belátni a-t.

- Atomi utasítás levezetési szabálya

$$\frac{\{\{Q\}\}\ S\ \{\{R\}\}}{\{\{Q\}\}\ [S]\ \{\{R\}\}}$$

- Várakoztató utasítás levezetési szabálya

$$\frac{\begin{array}{c} Q \implies \beta \vee \neg\beta \\ \{\{Q \wedge \beta\}\}\ S\ \{\{R\}\} \end{array}}{\{\{Q\}\}\ \textbf{await}\ \beta\ \textbf{then}\ S\ \textbf{ta}\ \{\{R\}\}}$$

- Párhuzamos blokk levezetési szabálya

$$\frac{\begin{array}{c} Q \Rightarrow Q_1 \wedge \ldots \wedge Q_n \\ \forall i \in \{1, \ldots, n\} : \{\{Q_i\}\}S_i\{\{R_i\}\} \\ R_1 \wedge \ldots \wedge R_n \Rightarrow R \\ \text{a párhuzamos blokk holtpontmentes} \\ \{\{Q_i\}\}S_i\{\{R_i\}\}\text{teljes helyességi tételek interferencia-mentesek} \end{array}}{\{\{Q\}\}\ \textbf{parbegin}\ S_1 \parallel \cdots \parallel S_n\ \textbf{parend}\ \{\{R\}\}}$$

Az első három feltétel azt fejezi ki, hogy
- ha Q előfeltétel teljesül, akkor a párhuzamos blokk bármely S_i komponensprogramja elvégezhető, mert teljesül a Q_i előfeltétele (ezt nevezhetjük „belépési feltételnek”)
- minden S_i komponens önmagában teljesen helyes a Q_i előfeltételével és R_i utófeltételével adott feladatra nézve
- amikor a párhuzamos blokk terminál (az összes S_i komponens befejeződött, elérte utófeltételét) akkor jó helyen terminált: ott ahol R utófeltétel igaz (ezt nevezhetjük „kilépési feltételnek”)

Interferencia mentesség

- Azt mondjuk hogy az S_j komponens kritikus u utasítása (aminek előfeltételét jelölje pre_u) nem interferál a $\{\{Q_i\}\}S_i\{\{R_i\}\}$ teljes helyességi tétellel, ha
  - $\{\{pre_u \wedge R_i\}\}u\{\{R_i\}\}$ Azaz u végrehajtása nem rontja el S_i utófeltételét: ha R_i igaz volt a végrehajtás előtt akkor utána is igaz lesz.
  - $\{\{pre_u \wedge pre_s\}\}u\{\{pre_s\}\}$ Azaz u végrehajtása igaznak tartja meg S_i bármely s utasításának előfeltételét: ha s elvégezhető volt u végrehajtása előtt akkor utána is az lesz.
  - $\{\{pre_u \wedge P \wedge t = t_0\}\}u\{\{t \leq t_0\}\}\forall t_0 \in \mathbb{Z}$ Azaz u végrehajtása S_i bármely ciklusának t terminálófüggvényének értékét nem növeli meg (P ugyanezen ciklus invariánsát jelöli).

  Ezzel a fogalommal azt akarjuk kifejezni, hogy ha valamit már beláttunk az S_i komponens esetén, az a bizonyítás nem veszti érvényét egy S_i komponenssel párhuzamosan végrahajtott S_j komponensben lévő u utasítás végrehajtásával. Például, ne legyen az hogy már beláttuk hogy S_i egy ciklusának magjában a termináló függvény értéke csökken, a bizonyításunkat meg tönkreteszi u azáltal hogy meg tudja növelni az adott ciklus termináló függvényének értékét.
  Mivel értéket megváltoztatni csak az értékadás (legyen az akár egy await-en belül) tud, így u utasításként azokat kell figyelembe venni, nevezzük őket kritikus utasításnak.

- Azt mondjuk hogy a $\{\{Q_i\}\}S_i\{\{R_i\}\}$ és $\{\{Q_j\}\}S_j\{\{R_j\}\}$ (ahol $i \neq j$) teljes helyességi tételek nem interferálnak, ha S_j bármely u kritikus utasítása nem interferál a $\{\{Q_i\}\}S_i\{\{R_i\}\}$ teljes helyességi tétellel (és hasonló igaz S_i bármely kritikus utasítására).

- A $\{\{Q_i\}\}S_i\{\{R_i\}\}$ teljes helyességi tételek ($i \in [1..n]$) interferencia mentesek, ha közülük egyik pár sem interferál.

Feladatok

1. $A = (x{:}\mathbb{Z})$

S_1:	S_2:
$\{x = 0 \vee x = 3\}$ $x := x + 2$ $\{x = 2 \vee x = 5\}$	$\{x = 0 \vee x = 2\}$ $x := x + 3$ $\{x = 3 \vee x = 5\}$

   Bizonyítsuk be hogy $\{\{x = 0\}\}$ **parbegin** $S_1 \parallel S_2$ **parend** $\{\{x = 5\}\}$ teljesül.

2. $A = (x{:}\mathbb{Z})$

$S_1:$
$\{x = 0 \lor x = 1\}$
await $x = 1$ then SKIP ta
$\{x = 1\}$

$S_2:$
$\{x = 0\}$
$x := 1$
$\{x = 1\}$

Bizonyítsuk be hogy $\{\{x = 0\}\}$ **parbegin** $S_1 \parallel S_2$ **parend** $\{\{x = 1\}\}$ teljesül.

3. $A = (x{:}\mathbb{N}, n{:}\mathbb{N}, z{:}\mathbb{N})$

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

   $Q = (x = x' \land n = n' \land x > 0)$

   $R = (z = x'^{n'})$

   Jelölje S a következő programot:

   $\{x > 0\}$
   $z := 1;$
   $\{Inv\}$
   parbegin $S_1 \| S_2$ **parend**
   $\{z = x'^{n'}\}$

   $\{Inv\}$
   $S_1:$

   $\{Inv\}$
   ```
   while n ≠ 0 do
   {Inv ∧ n ≠ 0}
      n,z := n−1,z·x
   od
   ```
   $\{z = x'^{n'} \land n = 0\}$

   $\{Inv\}$
   $S_2:$

   $\{Inv\}$
   ```
   while n ≠ 0 do
   {Inv}
      await even(n) then
         x,n := x·x,n/2
      ta
   od
   ```
   $\{z = x'^{n'} \land n = 0\}$

   Inv jelöli a ciklusok invariánsát: $Inv = (z \cdot x^n = x'^{n'})$
   A ciklusok termináló függvénye: $t\colon n$

   – Lássuk be hogy teljesül az interferencia-mentesség.
   – Mutassuk meg hogy S program megoldja a specifikált feladatot.

4. $A = (a : \mathbb{Z}^n, b : \mathbb{Z}^n)$

$i, j := 1, 1;$

$\{a = a' \wedge i = 1 \wedge j = 1\}$

parbegin $S_1 \| S_2$ **parend**

$\{Inv\}$
$S_1:$
 	
$\{Inv\}$
while $i \leq n$ do
   $\{Inv \wedge i \leq n\}$
   await $i = j$ then
      $x, i := a[i], i + 1$
   ta
   $\{Inv\}$
do
$\{Inv \wedge i = n + 1\}$
	$\{Inv\}$
	$S_2:$
	
	$\{Inv\}$
	while $j \leq n$ do
	   $\{Inv \wedge j \leq n\}$
	   await $i > j$ then
	      $b[j], j := x, j + 1$
	   ta
	   $\{Inv\}$
	do
	$\{Inv \wedge j = n + 1\}$

$Inv = (a = a' \wedge 0 \leq i - 1 \leq j \leq i \leq n + 1 \wedge \forall k \in [1..j - 1] \colon b[k] = a[k]) \wedge (i > j \to x = a[i - 1]))$

$i : \mathbb{N}$ és $j : \mathbb{N}$ segédváltozók. S_1 ciklusának terminiáló függvénye $n + 1 - i$, S_2-é $n + 1 - j$. Mutassuk meg az interferencia-mentességet.