gyak10

2022. november 16., szerda 8:15

+/- Elágazás levezetési szabálya

12. feladatsor, 3. feladat:

$A = (x\colon \mathbb{N}, n\colon \mathbb{N}, z\colon \mathbb{N})$
$B = (x'\colon \mathbb{N}, n'\colon \mathbb{N})$
$Q = (x = x' \wedge n = n' \wedge x > 0)$
$R = \left(z = x'^{n'}\right)$

Jelölje S a következő annotált programot:

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

S_1:

$\{Inv\}$
while $n \neq 0$ do
$\{Inv \wedge n \neq 0\}$
$n, z := n - 1, z \cdot x$
od
$\{z = x'^{n'} \wedge n = 0\}$

S_2:

$\{Inv\}$
while $n \neq 0$ do
$\{Inv\}$
await $even(n)$ then
$x, n := x \cdot x, n/2$
ta
od
$\{z = x'^{n'} \wedge n = 0\}$

Inv jelölje a ciklusok invariánsát: $Inv = \left(z \cdot x^n = x'^{n'}\right)$
A ciklusok terminálófüggvénye: $t\colon n$

Mutassuk meg, hogy az S program megoldja a specifikált feladatot.

A specifikációs tétele szerint elég belátni, hogy $Q \Rightarrow lf(S, R)$

A korrekcia levezetési szabálya miatt elég belátni 2 másik állítást:

1) $x = x' \wedge n = n' \wedge x > 0 \Rightarrow lf(z := 1, Inv)$

$(z \cdot x^n = x'^{n'})_{z:=1} \wedge 1 \in \mathbb{N}$

$1 \cdot x^n = x'^{n'} \wedge$ igaz

$x^n = x^n$

2) $z \cdot x^n = x'^{n'} \Rightarrow lf(\text{parbegin } S_1 \| S_2 \text{ parend}, R)$

párhuzamos blokk levezetési szabálya:

1. Belépési feltétel

$Q \Rightarrow \bigwedge_{i=1}^{n} Q_i$

2. $k < i$ lépési feltétel

$\bigwedge R_i \Rightarrow R$

$\left(\forall i \in [1..n]: Q_i = pre(S_i) \wedge R_i = post(S_i)\right)$

3. A komponenseket önmagukban nézve helyesek:

$\forall i \in [1..n]: Q_i \Rightarrow lf(S_i, R_i)$

4. A 3. pontban belőtolt teljes helyességi formulák interferenciamentesek.

5. Holtpontmentesség

Ha ez az 5 állítás teljesül, akkor $Q \Rightarrow lg(\text{parbegin } S_1 \| \dots \| S_n \text{ parend } R)$

A párhuzamos blokk levezetési szabálya szerint elég belátni 5 másik állítást:

S_1:
$\{Inv\}$ ← $pre(S_1)$
while $n \neq 0$ do
$\{Inv \wedge n \neq 0\}$
$n, z := n - 1, z \cdot x$
od
$\{z = x'^{n'} \wedge n = 0\}$ ← $post(S_1)$

S_2:
$\{Inv\}$ ← $pre(S_2)$
while $n \neq 0$ do
$\{Inv\}$
await $even(n)$ then
$x, n := x \cdot x, n/2$
ta
od
$\{z = x'^{n'} \wedge n = 0\}$ ← $post(S_2)$

Inv jelölje a ciklusok invariánsát: $Inv = (z \cdot x^n = x'^{n'})$
A ciklusok terminálófüggvénye: $t: n$

Mutassuk meg, hogy az S program megoldja a specifikált feladatot.

I. Belépési feltétel:

$Inv \Rightarrow Inv \wedge Inv$

Inv ✓

II. Kilépési feltétel:

$(z = x^{1n'} \wedge n = 0) \wedge (z = x^{1n'} \wedge n = 0) \Rightarrow (z = x^{1n'})$ ✓

$z = x^{1n'} \wedge n = 0$

III. A komponensek teljesen helyesek:

S_1:

$\{Inv\}$
while $n \neq 0$ do
$\{Inv \wedge n \neq 0\}$
$n, z := n - 1, z \cdot x$
od
$\{z = x'^{n'} \wedge n = 0\}$

i) $Inv \Rightarrow lg(S_1, z = x^{1n'} \wedge n = 0)$

A ciklus levezetési szabálya szerint elég belátni 5 másik állítást:

(1) $Inv \Rightarrow Inv$ ✓

(2) $z \cdot x^n = x^{1n'} \wedge n = 0 \Rightarrow z = x^{1n'} \wedge n = 0$ ✓ ✓

$z \cdot x^0 = x^{1n'}$

$z \cdot 1 = x^{1n'}$

(3) $Inv \Rightarrow n \neq 0 \vee n = 0$ ✓ $n : \mathbb{N}$

Egy természetes szám vagy megegyezik 0-val vagy nem.

(4) $Inv \wedge n \neq 0 \Rightarrow n > 0$ ✓

$n : \mathbb{N}$, $n \neq 0$ $\Rightarrow n > 0$

5) $(z \cdot x^n = x'^{n'} \wedge n \neq 0 \wedge n = t_0) \Rightarrow$ $wf(h; z := n-1, z \cdot x)$, $Inv \wedge n < t_0$

$(z \cdot x^n = x'^{n'} \wedge n < t_0)^{n \leftarrow n-1,\ z \leftarrow z \cdot x} \wedge n-1 \in \mathbb{N} \wedge$ igaz

$h : \mathbb{N}$

$z \cdot x \cdot x^{n-1} = x'^{n'} \wedge n-1 < t_0 \wedge n > 0 \wedge$ igaz

$n-1 < n \ /-n+1$, $n \neq 0$, $n : \mathbb{N}$ $\Big\}$ $n > 0$

$0 < 1$

$z \cdot x^1 \cdot x^{n-1} = x'^{n'}$

x^{1+n-1}

S_2:

$\{Inv\}$
while $n \neq 0$ do
$\{Inv\}$
await $even(n)$ then
$x, n := x \cdot x, n/2$
ta
od
$\{z = x'^{n'} \wedge n = 0\}$

A

ii) $Inv \Rightarrow wf(S_2,\ z = x'^{n'} \wedge n = 0)$

A ciklus levezetési szabálya miatt elég belátni 5 másik állítást:

1) $Inv \Rightarrow Inv$ ✓

2) $Inv \wedge n = 0 \Rightarrow post(S_2)$ ✓ Előbb belátjuk

3) $Inv \Rightarrow n \neq 0 \vee n = 0$ ✓ Belátjuk

4) $Inv \wedge n \neq 0 \Rightarrow n > 0$ ✓

2) H. i. pontban belátjuk.

5) $Inv \wedge n \neq 0 \wedge n = t_0 \Rightarrow wf(A,\ Inv \wedge n < t_0)$

Várakoztató utasítás levezetési szabálya:

1. $Q \Rightarrow \beta \vee \neg\beta$
2. $Q \wedge \beta \Rightarrow wf([S], R)$,

akkor $Q \Rightarrow wf(\text{await } \beta \text{ then } S \text{ ta}, R)$

Atomi utasítás levezetési szabálya:

Ha $Q \Rightarrow wf(S, R)$, akkor $Q \Rightarrow wf([S], R)$

A várakoztató utasítás levezetési szabálya miatt elég belátnunk 2 másik állítást:

a) $Inv \Rightarrow even(n) \vee odd(n)$

$2 | n \vee 2 \nmid n$

$n : \mathbb{N}$ bármely természetes szám vagy páros, vagy páratlan

S_2:

$\{Inv\}$
while $n \neq 0$ do
$\{Inv\}$
await $even(n)$ then
$x, n := x \cdot x, n/2$
ta
od
$\{z = x'^{n'} \wedge n = 0\}$

b) $z \cdot x^n = x^{1+n'} \wedge n \neq 0 \wedge n = t_0 \wedge 2 \mid n \Rightarrow lf((x, n := x \cdot x, n/2), lnw \wedge n < t_0)$

$(lnw \wedge n < t_0)^{x \in x \cdot x,\ n \in n/2}$

$\wedge$ igaz $\wedge$ $n/2 \in \mathbb{N}$

$n : \mathbb{N}$

mert: $2 \mid n$

$(z \cdot (x \cdot x)^{n/2} = x^{1+n'} \wedge n/2 < t_0 \wedge$ igaz $\wedge$ $2 \mid n)$

$n/2 < n$ ✓ $2 \mid n$ ✓

$(x^n)^{n/2}$

$x^{2 \cdot n/2}$ ✓

$z \cdot x^n = x^{1+n'}$

maisrip:

$x^{n/2} \cdot x^{n/2}$

x^n

$z \cdot x^n = y^{1+n'}$