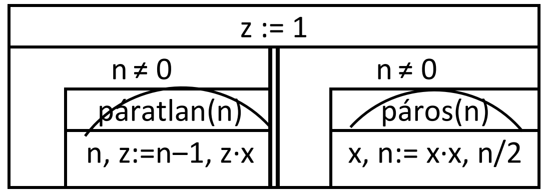
Mutassuk meg, hogy az alábbi párhuzamos program egy valós szám természetes számadik hatványát állítja elő.

$A = (x:\mathbb{R}, n:\mathbb{N}, z:\mathbb{R})$
$B = (x':\mathbb{R}, n':\mathbb{N})$
$Q = (x=x' \wedge n=n')$
$R = (z = x'^{n'})$



Annotáció:

Közbülső állítás: $Q' = (Q \wedge z=1)$

Ágak elő- és utófeltételei:	$Q_1 = Q_2 = P$	$R_1 = R_2 = (R \wedge n = 0)$
Közös invariáns és termináló függvény:	$P = (z \cdot x^n = x'^{n'})$	$t = n$.
Ciklusmagok utasításainak előfeltételei:	$pre(A_1) = (P \wedge n \neq 0)$	$pre(A_2) = P$

Kérdések:

1. Nem volna elég a várakozó utasítások helyett elágazást használni? Nem, mert az elágazás megszakítható a feltétel kiértékelése után, és ilyenkor a másik ág interferrálása miatt a feltétel érvényét veszítheti. Ez gondot okozna a 2. ágnál, ahol muszáj az n értékének párosnak lenni ahhoz, hogy az n felezése után fenn álljon a P.
2. Miért nem szerepel $pre(A_2)$-ben az $n\neq0$, hiszen amikor a 2. ág ciklusmagjába lép a vezérlés, akkor fenn áll a $P\wedge n\neq0$? Azért, mert amikor a ciklusmagba lép a vezérlés, akkor ez az ág itt megszakítható, és az 1. ág $n:=n-1$ értékadása el tudja „rontani" az $n\neq0$ feltételt. (Ez az interferencia vizsgálat során kiderülne.) A P-t viszont nem rontja el az 1. ág, másrészt a P következik a ciklusmagba lépés $P \wedge n\neq0$ feltételéből.
3. Miért nem használunk egy **if** $n\neq0$ **then** $x,n:= x\cdot x,n/2$ **fi** elágazást az A_2 várakozó utasítás törzsében, hiszen az előzőek szerint lehetséges, hogy itt már $n=0$ áll fenn, és ekkor felesleges még egyszer utoljára az $x,n:=x\cdot x,n/2$ értékadást végrehajtani? Mert ennek az eredményre, azaz a z változóra úgysincsen hatása, futási időben sem jelent veszteséget.

Kell (ST miatt): $Q \Longrightarrow lf(S, R)$

Elég (SzLSz miatt):

1. $Q \Longrightarrow lf(z := 1, Q') = (igaz \wedge Q'^{\,z\leftarrow1}) = (Q \wedge 1=1)$ ✓
2. $Q' \Longrightarrow lf(PAR, R)$

Elég (PLSz miatt):

be: $Q' \Longrightarrow Q_1 \wedge Q_2 = (z\cdot x^n = x'^{n'})$ ✓ (mert $z=1$, $x=x'$ és $n=n'$)

ki: $R_1 \wedge R_2 \Longrightarrow R$ ✓

1.ág: $Q_1 \Longrightarrow lf(S_1, R_1)$ lásd alább

2.ág: $Q_2 \Longrightarrow lf(S_2, R_2)$ lásd alább

Interferencia-mentes lásd később

Holtpont-mentes lásd később

1.ág: $Q_1 \Longrightarrow lf(S_1, R_1)$

Elég (CLSz miatt):

i. $Q_1 \Longrightarrow P$ ✓

ii. $P \Longrightarrow n\neq 0 \lor n=0$ ✓

iii. $P \land n=0 \Longrightarrow R_1$ ✓ (mert ekkor: $z \cdot x^0 = x'^{n'}$, azaz $z = x'^{n'}$)

iv. $P \land n\neq 0 \Longrightarrow t>0 = (n>0)$ ✓ (mert $n\neq 0$ és $n:\mathbb{N}$)

v. $P \land n\neq 0 \land t=t_0 \Longrightarrow lf(A_1, t<t_0)$

Elég (VLSz miatt):

a) $P \land n\neq 0 \land t=t_0 \Longrightarrow ptl(n) \lor \neg ptl(n)$ ✓

b) $P \land n\neq 0 \land t=t_0 \land ptl(n) \Longrightarrow lf(n,z:=n-1,z\cdot x, t<t_0) =$

$= (n\geq 1 \land (n<t_0)^{n,z\leftarrow n-1,z\cdot x}) = (n\geq 1 \land n-1<t_0)$ ✓

(mert $n\neq 0$ miatt $n\geq 1$, és $n-1<n=t=t_0$)

vi. $P \land n\neq 0 \Longrightarrow lf(A_1, P)$

Elég (VLSz miatt):

a) $P \land n\neq 0 \Longrightarrow ptl(n) \lor \neg ptl(n)$ ✓

b) $P \land n\neq 0 \land ptl(n) \Longrightarrow lf(n,z:=n-1,z\cdot x, P) = (n\geq 1 \land P^{n,z\leftarrow n-1,z\cdot x}) =$

$= (n\geq 1 \land z\cdot x\cdot x^{n-1} = x'^{n'}) = (n\geq 1 \land z\cdot x^n = x'^{n'}) = (n\geq 1 \land P)$ ✓

(mert $n\neq 0$ miatt $n\geq 1$, és $z\cdot x\cdot x^{n-1} = z\cdot x^n$)

2.ág: $Q_2 \Longrightarrow lf(S_2, R_2)$

Elég (CLSz miatt):

i. $Q_2 \Longrightarrow P$ ✓

ii. $P \Longrightarrow n\neq 0 \lor n=0$ ✓

iii. $P \land n=0 \Longrightarrow R_2$ ✓ (mert ekkor: $z \cdot x^0 = x'^{n'}$, azaz $z = x'^{n'}$)

iv. $P \land n\neq 0 \Longrightarrow t>0 = (n>0)$ ✓ (mert $n\neq 0$ és $n:\mathbb{N}$)

v. $P \land n\neq 0 \land t=t_0 \Longrightarrow lf(A_2, t<t_0)$

Elég (VLSz miatt):

a) $P \land n\neq 0 \land t=t_0 \Longrightarrow ps(n) \lor \neg ps(n)$ ✓

b) $P \land n\neq 0 \land t=t_0 \land ps(n) \Longrightarrow lf(x,z:=x\cdot x,n/2, t<t_0) =$

$= (n<t_0)^{x,n\leftarrow x\cdot x,n/2} = (n/2<t_0)$ ✓

(mert $n\neq 0$ miatt $n/2<n$ és $n=t=t_0$)

vi. $P \land n\neq 0 \Longrightarrow P \Longrightarrow lf(A_2, P)$

Elég (VLSz miatt):

a) $P \Longrightarrow ps(n) \lor \neg ps(n)$ ✓

b) $P \land ps(n) \Longrightarrow lf(x,z:=x\cdot x,n/2, P) = P^{x,n\leftarrow x\cdot x,n/2} =$

$= (z \cdot (x\cdot x)^{n/2} = x'^{n'}) = (z \cdot x^n = x'^{n'}) = P$ ✓

(mert $ps(n)$ miatt $n/2\in\mathbb{N}$ és ezért $(x\cdot x)^{n/2} = x^n$)

Egy ciklus interferencia-vizsgálatához külön igazoljuk a ciklusinvariáns megőrzését kifejező ($P \wedge \pi \Longrightarrow lf(S_0, P)$) és a ciklus leállását biztosító ($P \wedge \pi \wedge t=t_0 \Longrightarrow lf(S_0, t<t_0)$) kritériumokat. Az S_0 ciklusmag több helyen is megszakítható, ha máshol nem, a legelején, a ciklusfeltétel kiértékelése után biztosan. Ezért az annotáció a ciklusmag minden megszakítási pontjához megadja a következő lépés előfeltételét, amely eltérhet az előző lépés utófeltételétől: elég, ha csak következik abból. (Például a $P \wedge n \neq 0$-ből következik a $pre(A_2)=P$.) Ezt a ciklusinvariáns megőrzésének igazolásánál figyelembe kell venni. (A $P \wedge n\neq 0 \Longrightarrow lf(A_2,P)$ állítás helyett a $P \Longrightarrow lf(A_2,P)$ állítást kell igazolni.) Az interferencia-vizsgálatnak az egyes lépések előfeltételeire, valamint a ciklusmag utófeltételére kell majd irányulnia.
A leállást biztosító kritérium interferencia-vizsgálatánál viszont csak azt kell megmutatni, hogy egy párhuzamos kritikus utasítás nem képes a t értékét növelni, azaz nem dolgozik a ciklus terminálása ellen.

Interferencia-mentesség:

1.ág kritikus utasításai $\leadsto$ 2.ág annotációs állításai

$A_1 \leadsto Q_2, R_2, P, t=t_0$

1. $Q_2 \wedge pre(A_1) \Longrightarrow lf(A_1, Q_2)$

   Elég (VLSz miatt):

   a) $Q_2 \wedge P \wedge n\neq 0 \Longrightarrow ptl(n) \vee \neg ptl(n)$ ✓

   b) $Q_2 \wedge P \wedge n\neq 0 \wedge ptl(n) \Longrightarrow lf(n,z:= n-1,z\cdot x, Q_2) = (n\geq 1 \wedge Q_2^{n,z\leftarrow n-1,z\cdot x}) =$

   $= (n\geq 1 \wedge z\cdot x\cdot x^{n-1} = x'^{n'}) = (n\geq 1 \wedge z\cdot x^n = x'^{n'}) = (n\geq 1 \wedge Q_2)$ ✓

   (mert $n\neq 0$ miatt $n\geq 1$)

2. $R_2 \wedge pre(A_1) \Longrightarrow lf(A_1, R_2)$

   Elég (VLSz miatt):

   a) $R_2 \wedge P \wedge n\neq 0 \Longrightarrow ptl(n) \vee \neg ptl(n)$ ✓

   b) $R_2 \wedge P \wedge n\neq 0 \wedge ptl(n) \Longrightarrow lf(n,z:=n-1,z\cdot x, R_2)$ ✓

   (mert a premissza hamis, hiszen $n\neq 0$ de R_2 miatt $n=0$ is fen áll)

3. $P \wedge pre(A_1) \Longrightarrow lf(A_1, P)$

   Elég (VLSz miatt):

   a) $P \wedge P \wedge n\neq 0 \Longrightarrow ptl(n) \vee \neg ptl(n)$ ✓

   b) $P \wedge P \wedge n\neq 0 \wedge ptl(n) \Longrightarrow lf(n,z:=n-1,z\cdot x, P) = (n\geq 1 \wedge P^{n,z\leftarrow n-1,z\cdot x}) =$

   $= (n\geq 1 \wedge z\cdot x\cdot x^{n-1} = x'^{n'}) = (n\geq 1 \wedge z\cdot x^n = x'^{n'}) = (n\geq 1 \wedge P)$ ✓

   (mert $n\neq 0$ miatt $n\geq 1$)

4. $t=t_0 \wedge pre(A_1) \Longrightarrow lf(A_1, t\leq t_0)$

   Elég (VLSz miatt):

   a) $t=t_0 \wedge P \wedge n\neq 0 \Longrightarrow ptl(n) \vee \neg ptl(n)$ ✓

   b) $t=t_0 \wedge P \wedge n\neq 0 \wedge ptl(n) \Longrightarrow lf(n,z:=n-1,z\cdot x, t\leq t_0) = (n\geq 1 \wedge (t\leq t_0)^{n,z\leftarrow n-1,z\cdot x}) =$

   $= (n\geq 1 \wedge n-1\leq t_0)$ ✓ (mert $n\neq 0$ miatt $n\geq 1$, és $n-1<n=t=t_0$)

2.ág kritikus utasításai ↝ 1.ág annotációs állításai

A_2 ↝ Q_1, R_1, P, $t=t_0$

5. $\underline{Q_1 \wedge pre(A_2) \Longrightarrow lf(A_2, Q_1)}$

   Elég (VLSz miatt):

   a) $Q_1 \wedge P \Longrightarrow ps(n) \vee \neg ps(n)$ ✓

   b) $Q_1 \wedge P \wedge ps(n) \Longrightarrow lf(x,z{:=}x\cdot x,n/2, Q_1) = (\text{ igaz } \wedge Q_1{}^{x,n \leftarrow x\cdot x,n/2}) =$

   $= (z\cdot(x\cdot x)^{n/2} = x'^{n'}) = (z\cdot x^n = x'^{n'}) = Q_1$ ✓

   (mert ps(n) miatt $n/2 \in \mathbb{N}$ és ezért $(x\cdot x)^{n/2} = x^n$)

6. $\underline{R_1 \wedge pre(A_2) \Longrightarrow lf(A_2, R_1)}$

   Elég (VLSz miatt):

   a) $R_1 \wedge P \Longrightarrow ps(n) \vee \neg ps(n)$ ✓

   b) $R_1 \wedge P \wedge ps(n) \Longrightarrow lf(x,z{:=}x\cdot x,n/2, R_1) = (\text{ igaz } \wedge R_1{}^{x,n \leftarrow x\cdot x,n/2}) = (z = x'^{n'} \wedge n/2 = 0)$ ✓

   (mert egyrészt R_1 miatt $z = x'^{n'}$, másrészt R_1 miatt $n=0$, ezért $n/2 = 0$)

7. $\underline{P \wedge pre(A_2) \Longrightarrow lf(A_2, P)}$

   Elég (VLSz miatt):

   a) $P \wedge P \Longrightarrow ps(n) \vee \neg ps(n)$ ✓

   b) $P \wedge P \wedge ps(n) \Longrightarrow lf(x,z{:=}x\cdot x,n/2, P) = (\text{ igaz } \wedge P^{x,n \leftarrow x\cdot x,n/2}) = (z\cdot(x\cdot x)^{n/2} = x'^{n'}) =$

   $= (z\cdot x^n = x'^{n'}) = P$ ✓ (mert ps(n) miatt $n/2 \in \mathbb{N}$ és ezért $(x\cdot x)^{n/2} = x^n$)

8. $\underline{t=t_0 \wedge pre(A_2) \Longrightarrow lf(A_2, t \le t_0)}$

   Elég (VLSz miatt):

   a) $t=t_0 \wedge P \Longrightarrow ps(n) \vee \neg ps(n)$ ✓

   b) $t=t_0 \wedge P \wedge ps(n) \Longrightarrow lf(x,z{:=}x\cdot x,n/2, t \le t_0) = (\text{ igaz } \wedge (t \le t_0)^{x,n \leftarrow x\cdot x,n/2}) = (n/2 \le t_0)$ ✓

Holtpont-mentesség:

Három féleképpen alakulhat ki a párhuzamos blokkban holtpont:

1. Mindkét ág blokkolt a várakozó utasítás őrfeltételénél:

   $pre(A_1) \wedge \neg ptl(n) \wedge pre(A_2) \wedge \neg ps(n) =$

   $P \wedge n \neq 0 \wedge \neg ptl(n) \wedge P \wedge \neg ps(n)$ ez ellentmondás

2. Baloldali ág blokkolt a várakozó utasítás őrfeltételénél, jobboldali ág befejeződött:

   $pre(A_1) \wedge \neg ptl(n) \wedge R_2 =$

   $P \wedge n \neq 0 \wedge \neg ptl(n) \wedge R \wedge n=0$ ez ellentmondás

3. Baloldali ág befejeződött, jobboldali ág blokkolt a várakozó utasítás őrfeltételénél:

   $R_1 \wedge pre(A_2) \wedge \neg ps(n) =$

   $R \wedge n=0 \wedge P \wedge \neg ps(n)$ ez ellentmondás

Mindhárom feltétel hamis, így az összevagyoltjuk is az, tehát a program holtpontmentes.

A párhuzamos blokk annotációjánál bevezetett R_i-k n=0 feltételére sem a kilépési kritériumnak, sem az ágak helyességének bizonyításánál nem lenne szükség, de a holtpont-mentességhez, és az interferencia-mentességhez szükséges.