

Feladat: Határozzuk meg — a hatványozás műveletének használata nélkül — az x szám n -edik hatványát!

Specifikáció:

$$A = \mathbb{Z} \times \mathbb{N} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$$

$\begin{matrix} x & n & r & b & k \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \mathbb{Z} & \mathbb{N} & \mathbb{Z} & \mathbb{Z} & \mathbb{Z} \end{matrix}$

$$B = \mathbb{Z} \times \mathbb{N}$$

$\begin{matrix} x' & n' \\ \downarrow & \downarrow \\ \mathbb{Z} & \mathbb{N} \end{matrix}$

$$Q = (x = x' \wedge n = n' \wedge n \neq 0)$$

$$R = (Q \wedge r = x^n)$$

Megoldás:

Most keressük meg a specifikációnak megfelelő megoldó programot! A megoldást úgy sejtjük, hogy egy ciklussal találhatjuk meg. Nos, mi legyen ennek a ciklusnak az invariánsa?

$$P = (Q \wedge k \in [0..n] \wedge x^n = r * b^k)$$

Ellenőrizzük le a ciklus feltételeit:

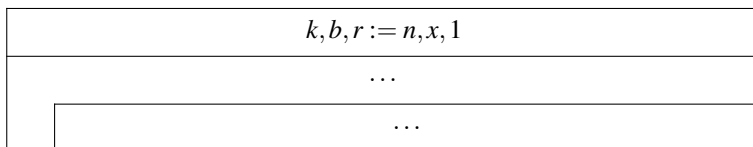
1. $Q \Rightarrow P$

Jól láthatóan nem teljesül, sőt fordítva igaz. Ezért megpróbálunk egy olyan közbülső állapotot felírni, ami a Q -ből könnyedén (egy értékadással) elérhető és ugyanakkor ez a kívánt feltétel teljesül rá. Amennyiben ez sikerül, akkor már csak egy szekvencia közbülső feltételeként kell pillantani erre az új Q' feltételre és máris felírható lesz a kívánt program egy értékadás és egy ciklus szekvenciájaként.

$$Q' = (Q \wedge k = n \wedge b = x \wedge r = 1)$$

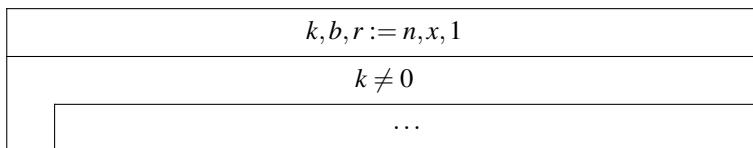
Látható, hogy $Q' \Rightarrow P$ és $Q \Rightarrow \text{If}(k, b, r := n, x, 1, Q') = Q$.

Tehát a program valahogy így néz ki:



2. $P \wedge \neg \pi \Rightarrow R$

Ez a feltétel kezünkbe adja a ciklusfeltételt, hiszen P és R összehasonlításából $\neg \pi$ -re $k = 0$ adódik. Tehát $\pi = (k \neq 0)$. (Megjegyzés: jelenleg $b = 1$ -re is gondolhatnánk, de az nem lenne jó.)



3. $P \wedge \pi \Rightarrow t > 0$

Jelen esetben ez: $Q \wedge k \in [1..n] \wedge x^n = r * b^k \Rightarrow t > 0$. Tehát $t := k$ egy megfelelő terminálófüggvény.

5. $P \wedge \pi \wedge t = t_0 \Rightarrow \text{If}(S_0, t < t_0)$

Előrevéve az utolsó feltételt már most biztosíthatjuk, hogy a programunk lefutása véges legyen. Mivel $t = k$, a megoldás csak k csökkentése lehet. Nézzük az alábbi struktogramot S_0 -ként:



Annak bizonyítását, hogy ez az elágazás mindig csökkenti k értékét, az olvasóra bízom.

4. $P \wedge \pi \Rightarrow \text{lf}(S_0, P)$

Ezen állítás igazolásához az elágazás levezetési szabályának feltételeit kell ellenőriznünk:

4/1. $P \wedge \pi \Rightarrow \left(\bigvee_{i=1}^n \pi_i \right)$

A fenti formájú egyszerűsített elágazásoknál ez mindig igaz, hiszen a második feltétel igazából az első pontos negáltja, így az állapottér összes pontjában igaz kettőjük valamelyike.

4/2. $\forall i \in [1..n] : P \wedge \pi \wedge \pi_i \Rightarrow \text{lf}(S_i, P)$

1. $2|k$:

$$Q \wedge k \in [1..n] \wedge x^n = r * b^k \wedge 2|k \stackrel{?}{\Rightarrow} Q \wedge k/2 \in [0..n] \wedge x^n = r * (b * b)^{k/2} \checkmark$$

2. $\neg(2|k)$:

$$Q \wedge k \in [1..n] \wedge x^n = r * b^k \wedge \neg(2|k) \stackrel{?}{\Rightarrow} Q \wedge k-1 \in [0..n] \wedge x^n = r * b * b^{k-1} \checkmark$$

Figyeljük meg, hogy ebben a feladatmegoldásban már az 5. pont megfontolásakor olyan ciklusmagot találtunk (a k növeléséhez), hogy azt már nem kellett megváltoztatnunk a 4. pont bizonyításakor, mint egyéb esetekben. (Természetesen ez nem volt véletlen.)

| | |
|----------------------|----------------------|
| $k, b, r := n, x, 1$ | |
| $k \neq 0$ | |
| $2 k$ | |
| $k, b := k/2, b * b$ | $k, r := k-1, r * b$ |