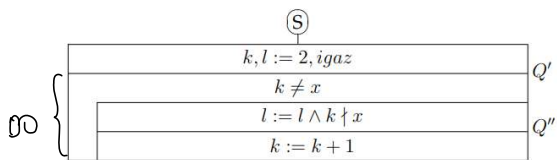


A specificació total de sintaxi és
 complet, on $Q \Rightarrow \mathcal{L}(S, R)$

- S sterbenia, csak elhelyez egy belátó 2
másiq állítást.

1) $Q \Rightarrow \underbrace{\text{eg}((x, l' = 2, \text{get}), Q \wedge x = 2 \wedge l = \text{iget})}$

$$\underbrace{(Q1 \otimes 2 \wedge 1 \otimes 1 = i \otimes 1)}_{\text{Q1} \wedge 2 = 2 \wedge 1 \otimes 1 = i \otimes 1} \wedge i \otimes 1$$



Lásd be hogy az S program megoldja a specifikált feladatot.

$$2) (Q \wedge x_2 = 2 \wedge e = iq_2) \Rightarrow \ell(00, 2)$$

Do egy kör, este elég belátni 5 állítást:

$$I. (\underbrace{Q}_{\sim} \wedge \underbrace{z}_{=2 \wedge l=i(z)} \Rightarrow (\underbrace{Q}_{\sim} \wedge \underbrace{l}_{=} (\forall j \in [2 \dots \underbrace{z-1}_{2}]: j \neq x) \wedge \underbrace{z}_{\in [2 \dots x]})$$

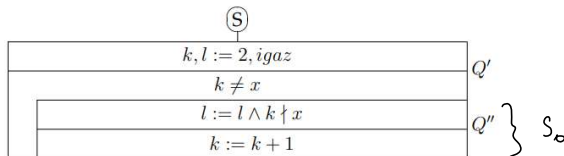
II. $P \wedge \neg \pi \Rightarrow Q$

$$(\underline{Q} \wedge l = (\forall j \in [1..x-1] : j \neq x) \wedge x \in [1..x] \wedge \underline{x=x}) \Rightarrow (\underline{Q} \wedge (\forall j \in [1..x-1] : j \neq x) = l)$$

III. $p \Rightarrow \pi \vee \neg \pi$
 $(x \neq x) \vee (x = x)$ ✓ $x: \text{N}^+$

IV. $p \wedge \pi \Rightarrow t \geq 0$

$x - 2 > 0 \quad \checkmark$
 $x \in [2..x]$
 \Downarrow
 $2 \leq x$
 $2 \neq x$
 $0 \leq x - 2$
 $0 \leq x - 2$
 $0 < x - 2$



- A program állapottér $(x:\mathbb{N}^+, \underline{k:\mathbb{N}^+}, l:\mathbb{L})$.

Lásd be hogy az S program megoldja a specifikált feladatot.

$$\text{V. } p \wedge q \wedge t = t_0 \Rightarrow \text{ef}(S_0, p \wedge t < t_0)$$

Mivel S_0 helyes, ezért elég csak belátni 2 másik állítást.

$$\text{i) } (Q \wedge l = (\underbrace{\forall j \in [2..x-1]: j \nmid x}_{\text{①}}) \wedge \underbrace{x \in [2..x]}_{\text{②}} \wedge \underbrace{x \neq 0}_{\text{③}}) \Rightarrow \text{ef}(l := 2 \wedge x \neq 0, Q)$$

$$(Q'')^L \Leftarrow l \wedge x \neq 0 \wedge l \wedge x \neq 0 \in \mathbb{L}$$

$$l \Leftarrow x \neq 0$$

$$(Q \wedge l \wedge x \neq 0) = (\underbrace{\forall j \in [2..x]: j \nmid x}_{\text{①}}) \wedge \underbrace{x \in [2..x]}_{\text{②}} \wedge \underbrace{x \neq 0}_{\text{③}} \Rightarrow x \neq 0 \wedge x \in \mathbb{N}^+$$

$$\text{① } l = \forall j \in [2..x-1]: j \nmid x$$

$$l \wedge x \neq 0 = \forall j \in [2..x-1]: j \nmid x \wedge x \neq 0$$

$$\forall j \in [2..x]: j \nmid x$$

1. A feladat informálisan: döntsük el hogy egy 1-nél nagyobb természetes szám prím-e.

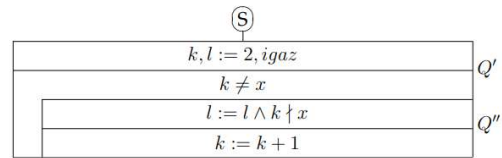
$$A = (x: \mathbb{N}^+, l: \mathbb{L})$$

$$B = (x': \mathbb{N}^+)$$

$$Q = (x = x' \wedge x > 1)$$

$$R = (Q \wedge l = (\forall j \in [2..x-1]: j \nmid x))$$

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



Legyen $Q' = (Q \wedge k = 2 \wedge l = \text{igaz})$ a szekvencia közbülső állítása, $t: x - k$ termináló-függvény.

$$P = (Q \wedge l = (\forall j \in [2..k-1]: j \nmid x) \wedge k \in [2..x])$$

Legyen a ciklusmagnak mint szekvenciának a közbülső állítása Q'' , ahol $Q'' = (Q \wedge l = (\forall j \in [2..k]: j \nmid x) \wedge k + 1 \in [2..x] \wedge x - k = t_0)$.

Lásd be hogy az S program megoldja a specifikált feladatot.

$$\text{ii) } (Q \wedge l = (\underbrace{\forall j \in [2..x]: j \nmid x}_{\text{①}}) \wedge \underbrace{x \in [2..x]}_{\text{②}} \wedge \underbrace{x \neq 0}_{\text{③}}) \Rightarrow \text{ef}(l := x+1, p \wedge t < t_0)$$

$$(p \wedge t < t_0) \wedge x+1 \in \mathbb{N}^+$$

$$(Q \wedge l = (\underbrace{\forall j \in [2..x-1]: j \nmid x}_{\text{①}}) \wedge \underbrace{x \in [2..x]}_{\text{②}} \wedge \underbrace{x-1 < t_0}_{\text{③}} \wedge \underbrace{\text{igaz}}_{\text{④}})$$

$$0 < 1$$

feladat, hogy $Q \Rightarrow \text{ef}(S, R)$, tehát S megoldja a specifikált feladatot.

3. A feladat informálisan: adott x egész számokat tartalmazó vektor minden elemét növeljük meg eggyel.

$$A = (x: \mathbb{Z}^n)$$

$$B = (x': \mathbb{Z}^n)$$

$$Q = (x = x')$$

$$R = (\forall k \in [1..n]: x[k] = x'[k] + 1)$$

A program állapottere $(x: \mathbb{Z}^n, i: \mathbb{N})$.

Specifikáció feltétele szerint elég bebizonyítani

$$\text{ha} \mathbb{Q} \Rightarrow \mathcal{H}(S, R)$$

S szekvenciát ezért elég bebizonyítani 2 másik állítást:

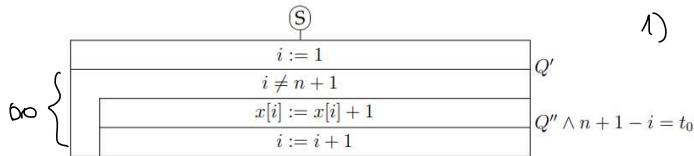
$$1) \mathbb{Q} \Rightarrow \mathcal{H}(i := 1, \mathbb{Q} \wedge i = 1)$$

$$(\mathbb{Q} \wedge i = 1) \wedge i \in \mathbb{N} \wedge 1 \in \mathbb{N}$$

Legyen $Q' = (Q \wedge i = 1)$ a szekvencia közbülső állítása, $t: n+1-i$ terminálófüggvény.

$$P = (\forall k \in [1..i-1]: x[k] = x'[k] + 1 \wedge i \in [1..n+1] \wedge \forall k \in [i..n]: x[k] = x'[k])$$

Legyen a ciklusmagnak mint szekvenciának a közbülső állítása $Q'' \wedge n+1-i = t_0$, ahol $Q'' = P^{i \leftarrow i+1}$. Lásd be hogy az S program megoldja a specifikált feladatot.



$$2) \mathbb{Q} \Rightarrow \mathcal{H}(DO, R) \text{ mivel } DO \text{ ciklus ezért elég bebizonyítani 5 másik állítást}$$

$$I. (\mathbb{Q} \wedge i = 1) \Rightarrow (\forall q \in [1..i-1] : x[q] = x'[q] + 1 \wedge i \in [1..n+1] \wedge \forall q \in [i..n] : x[q] = x'[q])$$

$$II. P \wedge \pi \Rightarrow R$$

$$(\forall q \in [1..i-1] : x[q] = x'[q] + 1 \wedge i \in [1..n+1] \wedge \forall q \in [i..n] : x[q] = x'[q] \wedge i = n+1) \Rightarrow \forall q \in [1..n] : x[q] = x'[q] + 1$$

$$III. P \Rightarrow \pi \vee \pi$$

$$IV. P \wedge \pi \Rightarrow n+1-i > 0$$

$$i \in [1..n+1] \wedge i \leq n+1 \wedge 0 \leq n+1-i \wedge n+1-i \geq 0 \wedge n+1-i$$

3. A feladat informálisan: adott x egész számokat tartalmazó vektor minden elemét növeljük meg eggyel.

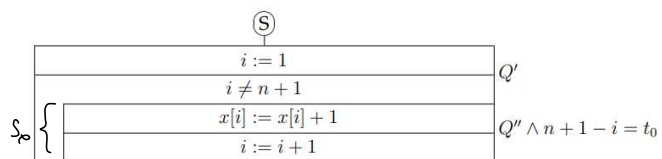
$$A = (x: \mathbb{Z}^n)$$

$$B = (x': \mathbb{Z}^n)$$

$$Q = (x = x')$$

$$R = (\forall k \in [1..n]: x[k] = x'[k] + 1)$$

A program állapottere $(x: \mathbb{Z}^n, i: \mathbb{N})$



Legyen $Q' = (Q \wedge i = 1)$ a szekvencia közbülső állítása, $t: n+1-i$ terminálófüggvény.

$$P = (\forall k \in [1..i-1]: x[k] = x'[k] + 1 \wedge i \in [1..n+1] \wedge \forall k \in [i..n]: x[k] = x'[k])$$

Legyen a ciklusmagnak mint szekvenciának a közbülső állítása $Q'' \wedge n+1-i = t_0$, ahol $Q'' = P^{i \leftarrow i+1}$. Lásd be hogy az S program megoldja a specifikált feladatot.

$$V. \quad P \wedge t = t_0 \Rightarrow pf(S_0, P \wedge t < t_0) \quad (\forall t_0 \in \mathbb{Z} - \mathbb{N})$$

A bizonyítás levezetési szabályra szerint elég belátni 2 állítást:

$$i) \quad (\forall j \in [1..i-1] : x[j] = x'[j] + 1 \wedge i \in [1..n+1] \wedge \forall j \in [i..n] : x[j] = x'[j] \wedge i \neq n+1 \wedge n+1-i = t_0)$$

①

②

④

$$\Rightarrow pf(x[i] := x[i] + 1, P \wedge i+1 \wedge n+1-i = t_0)$$

③ $i \in [1..n]$

$$(\forall j \in [1..i+1-1] : x[j] = x'[j] + 1 \wedge i+1 \in [1..n+1] \wedge \forall j \in [i+1..n] : x[j] = x'[j] \wedge n+1-i = t_0)$$

$$\wedge x[i] + 1 \in \mathbb{Z} \wedge i \in [1..n]$$

↑
értéktárolás helyes
nem indexelési hiba

$$(\forall j \in [1..i-1] : x[j] = x'[j] + 1 \wedge x[i] + 1 = x'[i] + 1 \wedge i-1$$

①

$$\wedge i+1 \in [1..n+1] \wedge \forall j \in [i+1..n] : x[j] = x'[j] \wedge n+1-i = t_0 \wedge \text{igaz} \wedge i \in [1..n])$$

$$\begin{aligned} i &\in [0..n] \\ \uparrow \\ \textcircled{5} \quad i &\in [1..n] \end{aligned}$$

$$ii) \quad (\forall j \in [1..i] : x[j] = x'[j] + 1 \wedge i+1 \in [1..n+1] \wedge \forall j \in [i+1..n] : x[j] = x'[j] \wedge n+1-i = t_0)$$

$pi \leftarrow i+1$

$$\Rightarrow pf(i := i+1, P \wedge n+1-i < t_0)$$

$$(P \wedge n+1-i < t_0)^{i \leftarrow i+1} \wedge i+1 \in \mathbb{N}$$

$$(\forall j \in [1..i] : x[j] = x'[j] + 1 \wedge i+1 \in [1..n+1] \wedge \forall j \in [i+1..n] : x[j] = x'[j] \wedge n+1-i-1 < t_0)$$

$pi \leftarrow i+1$

$$\begin{aligned} n-i &< n+1-i-1 \quad | -n+i \\ 0 &< -1 \end{aligned}$$

Belátjuk, hogy $Q \Rightarrow pf(Q)$, tehát S megoldja a specifikált feladatot.