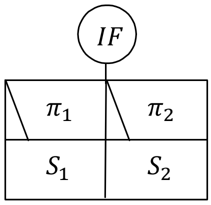
$A = [1..3]$

$S_1, S_2 \subseteq A \times (\bar{A} \cup \{fail\})^{**}$ programok:

$$S_1 = \begin{Bmatrix} 1 \to \langle 1,2 \rangle & 2 \to \langle 2 \rangle \\ 2 \to \langle 2,2,2,\dots \rangle & 3 \to \langle 3 \rangle \end{Bmatrix}$$

$$S_2 = \begin{Bmatrix} 1 \to \langle 1, fail \rangle & 2 \to \langle 2,3 \rangle \\ 3 \to \langle 3 \rangle & 3 \to \langle 3,2,1 \rangle \end{Bmatrix}$$



$\pi_1, \pi_2 \in A \to L$

$\pi_1 = \{ (1, igaz), (2, igaz), (3, hamis) \}$

$\pi_2 = \{ (1, igaz), \quad (3, hamis) \}$

$IF = (\pi_1 : S_1, \pi_2 : S_2)$

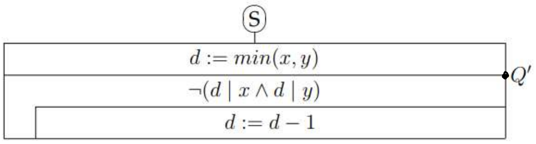
Határozd meg az IF programot halmazként.

$IF = \{ 1 \to \langle 1,2 \rangle \quad 1 \to \langle 1, fail \rangle$

$2 \to \langle 2 \rangle \quad 2 \to \langle 2,2,2,\dots \rangle \quad 2 \to \langle 2, fail \rangle$

$3 \to \langle 3, fail \rangle \}$

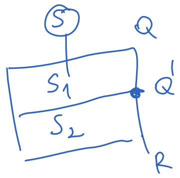
5. A feladat informálisan: határozzuk meg két pozitív egész legnagyobb közös osztóját.
   $A = (x{:}\mathbb{N}^+, y{:}\mathbb{N}^+, d{:}\mathbb{N}^+)$
   $B = (x'{:}\mathbb{N}^+, y{:}\mathbb{N}^+)$
   $Q = (x = x' \wedge y = y')$
   $R = (Q \wedge d \mid x \wedge d \mid y \wedge \forall k \in [d+1..min(x,y)]: \neg(k \mid x \wedge k \mid y))$
   A program állapottere $(x{:}\mathbb{N}^+, y{:}\mathbb{N}^+, d{:}\mathbb{N}^+)$.



Legyen $Q' = (Q \wedge d = min(x,y))$ a szekvencia közbülső állítása, $t : d$ terminálófüggvény.
$P = (Q \wedge \forall k \in [d+1..min(x,y)]: \neg(k \mid x \wedge k \mid y))$
Lásd be hogy az S program megoldja a specifikált feladatot.

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

Szekvencia levezetési szabálya:



Ha
1) $Q \Rightarrow lf(S_1, Q')$ és
2) $Q' \Rightarrow lf(S_2, R)$,
akkor $Q \Rightarrow lf(S,R)$

Mivel S szekvencia, ezért ehelyett elég belátni 2 másik állítást:

1) $Q \Rightarrow \underbrace{lf(d := min(x,y), Q')}_{(Q')^{d \leftarrow min(x,y)} \wedge min(x,y) \in \mathbb{N}^+}$

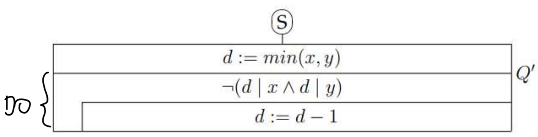
✓ ✓ ✓

$Q \wedge min(x,y) = min(x,y) \wedge min(x,y) \in \mathbb{N}^+$

O = O

$x, y : \mathbb{N}^+$

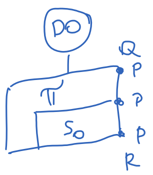
5. A feladat informálisan: határozzuk meg két pozitív egész legnagyobb közös osztóját.
   $A = (x{:}\mathbb{N}^+, y{:}\mathbb{N}^+, d{:}\mathbb{N}^+)$
   $B = (x'{:}\mathbb{N}^+, y{:}\mathbb{N}^+)$
   $Q = (x = x' \wedge y = y')$
   $R = (Q \wedge d \mid x \wedge d \mid y \wedge \forall k \in [d+1..min(x,y)]: \neg(k \mid x \wedge k \mid y))$
   A program állapottere $(x{:}\mathbb{N}^+, y{:}\mathbb{N}^+, d{:}\mathbb{N}^+)$.



Legyen $Q' = (Q \wedge d = min(x,y))$ a szekvencia közbülső állítása, $t : d$ terminálófüggvény.
$P = (Q \wedge \forall k \in [d+1..min(x,y)]: \neg(k \mid x \wedge k \mid y))$
Lásd be hogy az S program megoldja a specifikált feladatot.

2) $Q' \Rightarrow lf(DO, R)$

ciklus levezetési szabálya:



P: ciklusinvariáns

$t : A \to \mathbb{Z}$ terminálófüggvény

Ha

1) $Q \Rightarrow P$ és
2) $P \wedge \neg\pi \Rightarrow R$ és
3) $P \Rightarrow \pi \vee \neg\pi$ és
4) $P \wedge \pi \Rightarrow t > 0$ és
5) $P \wedge \pi \wedge t = t_0 \Rightarrow lf(S_0, P \wedge t < t_0)$ $(\forall t_0 \in \mathbb{Z}\text{-re})$,

akkor $Q \Rightarrow lf(DO, R)$

Mivel DO ciklus, így a 2. pont helyett elég belátni 5 másik állítást:

I. $Q' \Rightarrow P$ ✓

$(Q \wedge d = min(x,y)) \Rightarrow (Q \wedge \forall k \in [d+1..min(x,y)] : \neg(k|x \wedge k|y))$

$\forall k \in [min(x,y)+1..min(x,y)] : \dots$

$\forall k \in \emptyset : \neg(k|x \wedge k|y)$

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

$(Q \wedge \forall k \in [d+1..min(x,y)] : \neg(k|x \wedge k|y)$

$\wedge\ d|x \wedge d|y) \Rightarrow$

$(Q \wedge d|x \wedge d|y \wedge \forall k \in [d+1..min(x,y)] : \neg(k|x \wedge k|y))$

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

$\neg(d|x \wedge d|y) \vee (d|x \wedge d|y)$ ✓

Akkor teljesül, ha $d \neq 0$

állapottérben: $d : \mathbb{N}^+$

IV. $P \wedge \pi \Rightarrow t > 0$ ✓

$d > 0$ állapottérben. $d : \mathbb{N}^+$

5. A feladat informálisan: határozzuk meg két pozitív egész legnagyobb közös osztóját.
$A = (x{:}\mathbb{N}^+, y{:}\mathbb{N}^+, d{:}\mathbb{N}^+)$
$B = (x'{:}\mathbb{N}^+, y{:}\mathbb{N}^+)$
$Q = (x = x' \wedge y = y')$
$R = (Q \wedge d \mid x \wedge d \mid y \wedge \forall k \in [d+1..min(x,y)] : \neg(k \mid x \wedge k \mid y))$
A program állapottere $(x{:}\mathbb{N}^+, y{:}\mathbb{N}^+, d{:}\mathbb{N}^+)$.

(S)

$d := min(x,y)$	Q'
$\neg(d \mid x \wedge d \mid y)$	
$\quad d := d - 1$	

Legyen $Q' = (Q \wedge d = min(x,y))$ a szekvencia közbülső állítása, $t : d$ terminálófüggvény.
$P = (Q \wedge \forall k \in [d+1..min(x,y)] : \neg(k \mid x \wedge k \mid y))$
Lásd be hogy az S program megoldja a specifikált feladatot.

V. $P \wedge \pi \wedge t = t_0 \Rightarrow lf(S_0, P \wedge t < t_0)$ $(\forall t_0 \in \mathbb{Z}$-re$)$

$(Q \wedge \forall z \in [d+1..\min(x,y)] : \neg(z|x \wedge z|y) \wedge \neg(d|x \wedge d|y) \wedge d = t_0) \Rightarrow$

$\underbrace{lf(d := d-1, P \wedge d < t_0)}$

$(P \wedge d < t_0)^{d \leftarrow d-1} \wedge \underbrace{d-1 \in \mathbb{N}^+}$ $d:\mathbb{N}^+ \Rightarrow d-1 \in \mathbb{N}$

kell: $d > 1$

$(Q \wedge \underbrace{\forall z \in [\cancel{d-1}+1..\min(x,y)] : \neg(z|x \wedge z|y)} \wedge d-1 < t_0 \wedge d > 1)$

$d-1 < d \; / -d+1$

$0 < 1$

$\forall z \in [d+1..\min(x,y)] : \neg(z|x \wedge z|y)$

$\wedge \neg(d|x \wedge d|y)$

állapottérben. $d:\mathbb{N}^+$

π miatt: $d \geq 1$

$\neg(d|x \wedge d|y)$

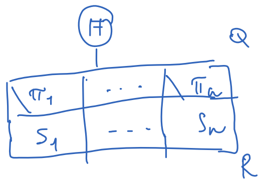
$\neg(1|x \wedge 1|y) =$ hamis

$d \neq 1$

$d > 1$

Beláttuk, hogy $Q \Rightarrow lf(S, R)$, tehát S megoldja a specifikált feladatot.

Elágazás levezetési szabálya:



Ha

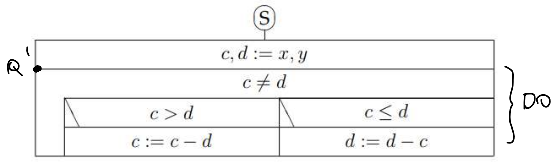
1) $Q \Rightarrow \bigwedge_{i=1}^{n} (\pi_i \vee \neg\pi_i)$ és

2) $Q \Rightarrow \bigvee_{i=1}^{n} \pi_i$ és

3) $\forall i \in [1..n] : Q \wedge \pi_i \Rightarrow lf(S_i, R)$,

akkor $Q \Rightarrow lf(IF, R)$.

2. $A = (x{:}\mathbb{N}^+, y{:}\mathbb{N}^+, d{:}\mathbb{N}^+)$
   $B = (x'{:}\mathbb{N}^+, y'{:}\mathbb{N}^+)$
   $Q = (x = x' \wedge y = y')$
   $R = (Q \wedge d = lnko(x, y))$
   Az S program alap-állapottere $(x{:}\mathbb{N}^+, y{:}\mathbb{N}^+, c{:}\mathbb{N}^+, d{:}\mathbb{N}^+)$.



Legyen $Q' = (Q \wedge x = c \wedge y = d)$ a szekvencia közbülső állítása, $P = (Q \wedge lnko(x, y) = lnko(c, d))$ ciklusinvariáns és $t : c + d$ terminálófüggvény. Lássuk be hogy $Q \Longrightarrow lf(S, R)$.

Az $lnko$ függvény tulajdonságai (ahol a és b pozitív egészek):

$$lnko(a, b) = \begin{cases} a & \text{ha} \quad a = b \\ lnko(a - b, b) & \text{ha} \quad a > b \\ lnko(a, b - a) & \text{ha} \quad a < b \end{cases}$$

Mivel S szekvencia, ezért ehelyett elég belátni 2 másik állítást:

szimultán értékadás

1) $Q \Rightarrow \underbrace{lf((c, d := x, y), Q \wedge x = c \wedge y = d)}$

$\underbrace{(Q \wedge x = c \wedge y = d)^{c \leftarrow x, d \leftarrow y}}$ $\wedge x, y \in \mathbb{N}^+$

$Q \wedge x = x \wedge y = y \wedge$ igaz

2) $Q' \Rightarrow lf(DO, R)$

Mivel DO ciklus, ezért ehelyett elég belátni 5 másik állítást:

I. $Q' \Rightarrow P$

$(Q \wedge x = c \wedge y = d) \Rightarrow (Q \wedge lnko(x, y) = lnko(\overset{x}{c}, \overset{y}{d}))$

$lnko(x, y) = lnko(x, y)$

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

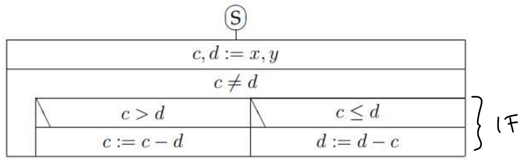
$(Q \wedge lnko(x,y) = lnko(c,d) \wedge c=d) \Rightarrow (Q \wedge d = lnko(x,y))$

$lnko(d,d)$ (a definíció szerint)

$lnko(x,y) = d$

$$lnko(a,b) = \begin{cases} a & \text{ha} \quad a = b \\ lnko(a-b,b) & \text{ha} \quad a > b \\ lnko(a,b-a) & \text{ha} \quad a < b \end{cases}$$

2. $A = (x{:}\mathbb{N}^+, y{:}\mathbb{N}^+, d{:}\mathbb{N}^+)$
   $B = (x'{:}\mathbb{N}^+, y'{:}\mathbb{N}^+)$
   $Q = (x = x' \wedge y = y')$
   $R = (Q \wedge d = lnko(x,y))$
   Az S program alap-állapottere $(x{:}\mathbb{N}^+, y{:}\mathbb{N}^+, c{:}\mathbb{N}^+, d{:}\mathbb{N}^+)$.



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

$c \neq d \vee c = d$

$c,d : \mathbb{N}^+$

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

$c + d > 0$

$c,d : \mathbb{N}^+$

Legyen $Q' = (Q \wedge x = c \wedge y = d)$ a szekvencia közbülső állítása, $P = (Q \wedge lnko(x,y) = lnko(c,d))$ ciklusinvariáns és $t : c + d$ terminálófüggvény. Lássuk be hogy $Q \implies lf(S,R)$.

Az $lnko$ függvény tulajdonságai (ahol a és b pozitív egészek):

$$lnko(a,b) = \begin{cases} a & \text{ha} \quad a = b \\ lnko(a-b,b) & \text{ha} \quad a > b \\ lnko(a,b-a) & \text{ha} \quad a < b \end{cases}$$

V. $P \wedge \pi \wedge t = t_0 \Rightarrow lf(IF, P \wedge t < t_0)$ $(\forall t_0 \in \mathbb{Z}\text{-re})$

Mivel IF elágazás, ezért ehelyett elég belátni 3 másik állítást:

① $P \wedge \pi \wedge t = t_0 \Rightarrow \underbrace{(c > d \vee c \le d) \wedge (c \le d \vee c > d)}_{c > d \vee c \le d}$ $\quad c,d : \mathbb{N}^+$

② $P \wedge \pi \wedge t = t_0 \Rightarrow c > d \vee c \le d$ $\quad c,d : \mathbb{N}^+$

③ i) $P \wedge \pi \wedge t = t_0 \wedge c > d \Rightarrow lf(c := c-d, P \wedge t < t_0)$

$(Q \wedge lnko(x,y) = lnko(c,d) \wedge c \neq d \wedge c + d = t_0 \wedge c > d) \Rightarrow$

$\underbrace{lf(c := c-d, P \wedge t < t_0)}$

$(P \wedge t < t_0)^{c \leftarrow c-d} \wedge c - d \in \mathbb{N}^+$ $\quad c,d : \mathbb{N}^+ \Downarrow c - d \in \mathbb{Z}$ $\quad$ kell: $c - d > 0$, $c > d$

"

$(Q \wedge \underbrace{lnko(x,y)}_{lnko(c,d)} = lnko(c-d, d) \wedge c - \cancel{d} + \cancel{d} < t_0 \wedge c > d)$

$c + d$ / $-c$

$0 < d$ $\quad d . \mathbb{N}^+$

$$lnko(a,b) = \begin{cases} a & \text{ha} \quad a = b \\ lnko(a-b,b) & \text{ha} \quad a > b \\ lnko(a,b-a) & \text{ha} \quad a < b \end{cases}$$

ii) $P \wedge \pi \wedge t = t_0 \wedge c \leq d \Rightarrow wp(d := d - c,\ P \wedge t < t_0)$

$(Q \wedge lnko(x,y) = lnko(c,d) \wedge c \neq d \wedge c + d = t_0 \wedge c \leq d) \Rightarrow$

$c < d$

$\underbrace{wp(d := d - c,\ P \wedge d + c < t_0)}$

$(P \wedge d + c < t_0)^{d \leftarrow d - c} \wedge d - c \in \mathbb{N}^+$

$d, c : \mathbb{N}^+$

$\Downarrow$

$d - c : \mathbb{Z}$

$d - c > 0$

$d > c$

$lnko(c, d)$

$(Q \wedge lnko(x,y) = lnko(c, d - c) \wedge d - \cancel{d} + c < t_0 \wedge d > c)$

$$lnko(a,b) = \begin{cases} a & \text{ha} \quad a = b \\ lnko(a-b,b) & \text{ha} \quad a > b \\ lnko(a,b-a) & \text{ha} \quad a < b \end{cases}$$

$d < c + d \ / - d$

$0 < c \quad c : \mathbb{N}^+$