A tétel direkt levezetése

$$\mathbf{A}: \quad \underset{i}{\Sigma}\times\underset{m}{\mathbb{N}_0}\times\underset{u}{\mathbb{L}}\times\underset{l}{\mathbb{L}}$$

$$\mathbf{B}: \quad \underset{i_1'}{\{(0,\dots,0)\}}\times\underset{i_2'}{\{(\sigma_1-1,\dots,\sigma_n-1)\}}$$

$$Q: (TRUE)$$

$$R: \big((u \leftrightarrow \exists j \in [i_1'..i_2'] : \overline{\rho}(j)) \wedge$$
$$\wedge (u \rightarrow (i \in [i_1'..i_2'] \wedge \overline{\rho}(i) \wedge \forall j \in [i_1'..i) : \neg\overline{\rho}(j))))\big)$$

Legyen

$$\begin{aligned} P :\big(& i \in [i_1'..i_2'] \wedge \ (\forall j \in [i_1'..i) : \neg\overline{\rho}(j)) \wedge \\ & \wedge \ (u \leftrightarrow \exists j \in [i_1'..i] : \overline{\rho}(j)) \wedge \\ & \wedge \ m \in [1..n] \wedge \\ & \wedge \ (\neg u \rightarrow (i \neq i_2' \rightarrow (\forall k \in [1..m) : \overline{\rho}_k(i) \wedge \neg\overline{\rho}_m(i) \wedge \forall k \in [m+1..n] : i_k = 0))) \wedge \\ & \wedge \ (u \rightarrow (m = n \wedge \forall k \in [1..n] : \overline{\rho}_k(i)))\big) \end{aligned}$$

1. $Q \not\Rightarrow P$
   ugyanakkor
   $Q \Rightarrow \mathrm{lf}(i := (0,\dots,0),\ i = (0,\dots,0))$
   Könnyen látható, hogy
   $i = (0,\dots,0) \not\Rightarrow P$.
   Keresni kell olyan S programot, amelyre
   $i = (0,\dots,0) \Rightarrow \mathrm{lf}(S,\ P)$.
   Legyen

$$\begin{aligned} P' : \big(i = (0,\dots,0) \wedge \ m \in [0..n] \ \wedge \forall k \in [1..m) : \overline{\rho}_k(i) \wedge \\ \wedge \ (u \leftrightarrow \forall k \in [1..m] : \overline{\rho}_k(i))\big) \end{aligned}$$

1'. $i = (0,\dots,0) \Rightarrow {P'}^{m,u \leftarrow 0,\uparrow}$.
2'. $P' \wedge \neg\pi \Rightarrow P$ teljesül, ha $\neg\pi :\ \neg u \vee m \geq n$.
    Tehát $\pi :\ u \wedge m < n$ alkalmas választás.

Typeset by $\mathcal{AMS}$-TEX

3'. $P' \wedge \pi \Rightarrow t > 0$ teljesül, ha $t:\ n-m$.

4'. $P' \wedge \pi \Rightarrow P'^{u \leftarrow \overline{\rho}_{m+1}(i)} \Leftrightarrow \mathrm{lf}(S_1,\ P'^{m \leftarrow m+1})$
ahol
$S_1:\ u := \overline{\rho}_{m+1}(i)$,
Mindebből már könnyen belátható, hogy

$$Q \Rightarrow \mathrm{lf}((i := (0,...,0); (m, u := 0, \uparrow; \mathrm{DO}(u \wedge m < n : (u := \overline{\rho}_{m+1}(i); m := m+1)))), P)$$

2. $P \wedge \neg\pi \Rightarrow R$ ha $\neg\pi:\ u \vee i = (\sigma_1 - 1, ..., \sigma_n - 1)$.
Tehát $\pi : \neg u \wedge i \neq (\sigma_1 - 1, ..., \sigma_n - 1)$ alkalmas választás.
3. $P \wedge \pi \Rightarrow t > 0$ teljesül, ha $t:\ |(i..i_2']|$.
4. Igazolni kell, hogy
$P \wedge \pi \Rightarrow \mathrm{lf}(S_1,\ P'')$,
illetve
$P'' \Rightarrow \mathrm{lf}(S_2,\ P)$,
ahol

$$\begin{aligned} P'' : \big(i \in [i_1'..i_2'] \wedge\ & (\forall j \in [i_1'..i) : \neg\overline{\rho}(j)) \wedge \\ & \wedge\ m \in [1..n] \wedge \\ & \wedge\ \forall k \in [1..m) : \overline{\rho}_k(i) \wedge \\ & \wedge\ (i \neq i_2' \rightarrow \forall k \in [m+1..n] : i_k = 0)\big) \end{aligned}$$

Legyen

$$\begin{aligned} \overline{P} : \big(i \in [i_1'..i_2'] \wedge\ & (\forall j \in [i_1'..i) : \neg\overline{\rho}(j)) \wedge \\ & \wedge\ m \in [1..n] \wedge \\ & \wedge\ \forall k \in [1..m) : \overline{\rho}_k(i) \wedge \\ & \wedge\ (u \leftrightarrow \forall k \in [1..m] : \overline{\rho}_k(i) \wedge \\ & \wedge\ (\neg u \rightarrow (i \neq i_2' \rightarrow \forall k \in [m+1..n] : i_k = 0))\big) \end{aligned}$$

1'. $P'' \Rightarrow \overline{P}^{m,u \leftarrow m-1,\uparrow}$

2'. $\overline{P} \wedge \neg\overline{\pi} \Rightarrow P$ ha $\neg\overline{\pi}:\ \neg u \vee m \geq n$
tehát $\overline{\pi}:\ u \wedge m < n$ alkalmas választás.

3'. $\overline{P} \wedge \overline{\pi} \Rightarrow t > 0$ teljesül, ha $t:\ n-m$.

4'. $\overline{P} \wedge \overline{\pi} \Rightarrow \mathrm{lf}(S_1,\ \overline{P}^{m \leftarrow m+1})$ teljesül, ha $S_1:\ u := \overline{\rho}_{m+1}(i)$,
ugyanis $\overline{P} \wedge \overline{\pi} \Rightarrow \overline{P}^{m \leftarrow m+1\, u \leftarrow \overline{\rho}_{m+1}}$.

Tehát

$$P'' \Rightarrow \mathrm{lf}((m, u \leftarrow m-1, \uparrow; \mathrm{DO}(u \wedge m < n,\ (u := \overline{\rho}_{m+1}; m := m+1))),\ P)$$

Könnyen látható, hogy

$$P \wedge \pi \wedge [i_{1,..,m}] = (\sigma_1 - 1, ..., \sigma_m - 1) \Rightarrow P''^{\,i \leftarrow (\sigma_1 - 1, ..., \sigma_n - 1)},$$

tehát

$$P \wedge \pi \wedge [i_{1,..,m}] = (\sigma_1 - 1, ..., \sigma_m - 1) \Rightarrow \mathrm{lf}(i := (\sigma_1 - 1, ..., \sigma_n - 1)\ , P'').$$

Legyen

$$\begin{aligned}
\overline{\overline{P}} : \big(i \in & [i'_1..i'_2] \wedge\ m \in [1..n] \wedge \\
& \wedge\ \forall k \in (m, n] : i_k = 0 \wedge \\
& \wedge\ \exists k \in [1..m] : i_m \neq \sigma_m - 1 \wedge \\
& \wedge\ (l \leftrightarrow \exists k \in [m..n] : i_k \neq 0) \wedge \\
& \wedge\ (l \rightarrow \forall k \in [1..m) : \overline{\rho}_k(i)) \wedge \\
& \wedge\ (\neg l \rightarrow \forall k \in [1..m-1) : \overline{\rho}_k(i)) \wedge \\
& \wedge\ (l \rightarrow \forall j \in [i'_1..(i_1, ...i_m, 0, ..., 0)) : \neg\overline{\rho}(j)) \wedge \\
& \wedge\ (\neg l \leftrightarrow \forall j \in [i'_1..([i_{1,...m}]^+, 0, ..., 0)) : \neg\overline{\rho}(j))\big)
\end{aligned}$$

1'. $P \wedge \pi \wedge [i_{1,..,m}] \neq (\sigma_1 - 1, ..., \sigma_m - 1) \Rightarrow \overline{\overline{P}}^{m,l \leftarrow m+1,\downarrow}$

2'. $\overline{\overline{P}} \wedge \neg\overline{\overline{\pi}} \Rightarrow P''$, ha $\overline{\overline{\pi}} :\ l$.

3'. $\overline{\overline{P}} \wedge \overline{\overline{\pi}} \Rightarrow t > 0$ teljesül, ha $t :\ m$

4'. $\overline{\overline{P}} \wedge \overline{\overline{\pi}} \wedge i_{m-1} = \sigma_{m-1} \Rightarrow \overline{\overline{P}}^{m \leftarrow m-1\, i_{m-1} \leftarrow 0}$,
hasonlóan
$\overline{\overline{P}} \wedge \overline{\overline{\pi}} \wedge i_{m-1} \neq \sigma_{m-1} \Rightarrow \overline{\overline{P}}^{m \leftarrow m-1\, i_{m-1}, l \leftarrow i_{m-1}-1, \uparrow}$.

Tehát

$P \wedge \pi \wedge [i_{1,..,m}] \neq (\sigma_1 - 1, ..., \sigma_m - 1) \Rightarrow$
$\mathrm{lf}((m, l := m + 1, \downarrow;$
$\mathrm{DO}(\neg l,$
$(\mathrm{IF}(i_{m-1} = \sigma_{m-1} - 1 : i_{m-1} := 0, i_{m-1} \neq \sigma_{m-1} - 1 : i_{m-1}, l := i_{m-1} + 1, \uparrow);$
$m := m - 1)))\ , P'').$

Mindezekből már következik, hogy a származtatott program valóban megoldása a feladatnak.