Σ_A formális rendszer

Axiómák:

$-A \to (B \to A)$,

$-(A \to (B \to C)) \to ((A \to B) \to (A \to C))$,

$-(\neg A \to \neg B) \to (B \to A)$.

Szabály:

$-A, A \to B \vdash B \quad$ (*modus ponens*)

Σ_P formális rendszer

Axiómák:

$-\Sigma_A$ minden axiómája,

$-x = x$,

$-x = y \to (A \to A_x(y))$.

Szabályok:

$-A, A \to B \vdash B \quad$ (*modus ponens*),

$-A \to B \vdash A \to \forall x B \quad$ (*generalization*),

ha A-ban x-nek nincs szabad előfordulása.

Σ_{TA} formális rendszer

Axiómák:

(taut) Minden tautologikusan érvényes formula,

(ax1) $\quad \neg \circ A \leftrightarrow \circ \neg A$,

(ax2) $\quad \circ (A \to B) \to (\circ A \to \circ B)$,

(ax3) $\quad \Box A \to A \land \circ \Box A$,

(ax4) $\quad \circ \Box \neg B \to A \,\mathbf{atnext} B$,

(ax5) $\quad A \,\mathbf{atnext} B \leftrightarrow \circ(B \to A) \land \circ(\neg B \to A \,\mathbf{atnext} B)$.

Szabályok:

(mp) $\quad A, A \to B \vdash B$,

(nex) $\quad A \vdash \circ A$,

(ind) $\quad A \to B, A \to \circ A \vdash A \to \Box B$.

Σ_{TP} formális rendszer

Axiómák:

A Σ_{TA} minden axiómája ((taut),
(ax1) - (ax5))
(ax6) $\forall x A \rightarrow A_x(t)$
ha t helyettesítheti x-et A-ban,
(ax7) $\forall x \circ A \rightarrow \circ \forall x A$,
(ax8) $A \rightarrow \circ A$
ha A nem tartalmaz lokális változót,
(eq1) $x = x$,
(eq2) $x = y \rightarrow (A \rightarrow A_y(x)$
ha A nem tartalmaz temporális operátort.

Szabályok:

A Σ_{TA} minden szabálya ((mp), (nex), (ind))
(gen) $A \rightarrow B \vdash (A \rightarrow \forall x B)$
ha A-ban x-nek nincs szabad előfordulása.

Σ^+_{TP} formális rendszer

Megegyezik a Σ_{TP} formális rendszerrel, kivéve az (ax8) *axiómát, amely helyett az alábbi axiómát kell tekinteni:*

(ax8$^+$) $A \rightarrow \circ A$
ha A nem tartalmaz sem lokális változót, sem logikai változót.

Bizonyítási technikák

Invariáns tulajdonságok bizonyítása

$$\text{(ind}''\text{)} \quad A \to B,\; B \to \circ B \vdash A \to \Box B$$

$$\begin{array}{ll} \text{(trans)} & \alpha \wedge A \to \circ B \quad \text{minden } \alpha \in \overline{\mathcal{M}}_\Pi, \\ & nil_\Pi \wedge A \to B \\ & \vdash A \to \circ B \end{array}$$

$$\begin{array}{ll} \text{(inv)} & A \to B, \\ & \alpha \wedge B \to \circ B \quad \text{minden } \alpha \in \overline{\mathcal{M}}_\Pi, \\ & \vdash A \to \Box B \end{array}$$

Precedencia-tulajdonságok igazolása

$$\begin{array}{ll} \text{(indatnext)} & A \to \circ(C \to B) \wedge \circ(\neg C \to A) \\ & \vdash A \to B \;\textbf{atnext}\; C \end{array}$$

$$\begin{array}{ll} \text{(atnext)} & \alpha \wedge A \to \circ(C \to B) \wedge \circ(\neg C \to A) \\ & \text{minden } \alpha \in \overline{\mathcal{M}}_\Pi, \\ & nil_\Pi \wedge A \to (C \to B) \\ & \vdash A \to B \;\textbf{atnext}\; C \end{array}$$

Program fogalma

$\mathcal{L}_P$: klasszikus elsőrendű logikai nyelv,
$\mathcal{E}$: elemi utasítások halmaza,
$\mathcal{S}$: szinkronizációs utasítások halmaza.
Szinkronizációs utasítás:

$$\textbf{await } \mathcal{B} \textbf{ then } a$$

vagy

$$\textbf{await } \mathcal{B},$$

ahol $\mathcal{B}$ $\mathcal{L}_P$ formula, $a \in \mathcal{E}$.
Legyen $\mathcal{A} = \mathcal{E} \cup \mathcal{S}$.
$\mathcal{L}_P$ és $\mathcal{A}$ feletti **program**:

$$\begin{array}{l} \textbf{initial} \quad \mathcal{R}; \\ \textbf{cobegin} \quad \Pi_1 \parallel ... \parallel \Pi_p \quad \textbf{coend} \end{array}$$

ahol $\mathcal{R}$ $\mathcal{L}_P$ formula - **kezdeti feltétel**, és

$$\Pi_i, 1 \leq i \leq p$$

ciklikus vagy
nem ciklikus parallel komponens.

<cyclic parallel component >::=
loop <statement sequence >**end**
<non-cyclic parallel component >::=
<statement sequence>;<label>:**stop**
<statement sequence >::= <statement>|
<statement>;<statement sequence>
<statement >::=
<label>:<unlabelled statement>
<unlabelled statement> ::=<element of $\mathcal{A}$>|
if<condition>
then<statement sequence>
else<statement sequence >**fi**|
if<condition>
then<statement sequence >**fi**|
while<condition>
do<statement sequence >**od**
<condition >::=<formula of $\mathcal{L}_P$>

Címkehalmaz: $\{\alpha_0, \alpha_1, \alpha_2, ..., \beta_0, \beta_1, \beta_2 ...\}$
Tetszőleges programban bármely két címke különböző.

Jelölések

$\alpha_0^{(i)}$: Π_i start címkéje,
$\alpha_e^{(i)}$: Π_i **stop** címkéje, ha Π_i nem ciklikus,
$\mathcal{M}_{\Pi_i}$: Π_i-ben előforduló címkék halmaza,
$\mathcal{M}_{\Pi}$: $\bigcup_{i=1}^{p} \mathcal{M}_{\Pi_i}$,
$\overline{\mathcal{M}}_{\Pi_i}$: $\mathcal{M}_{\Pi_i} \setminus \{\alpha_e^{(i)}\}$,
$\overline{\mathcal{M}}_{\Pi}$: $\bigcup_{i=1}^{p} \overline{\mathcal{M}}_{\Pi_i}$.

Jelölje $\mathcal{F}(\mathcal{L}_P)$ az $\mathcal{L}_P$ összes formuláinak halmazát.
Legyen ψ utasítássorozat $\mathcal{L}_P$ és $\mathcal{A}$ felett.
Jelölje $\mathcal{M}_\psi$ a ψ-ben előforduló címkék halmazát.

$$\begin{aligned}
&\text{entry}(\psi) \in \mathcal{M}_\psi,\\
&\text{trans}(\psi) \subset \mathcal{M}_\psi \times \mathcal{F}(\mathcal{L}_P) \times \mathcal{M}_\psi,\\
&\text{exit}(\psi) \subset \mathcal{M}_\psi \times \mathcal{F}(\mathcal{L}_P)
\end{aligned}$$

1. $\psi \equiv \alpha : < \mathcal{E}$ eleme $>$:

$$\begin{aligned}
&\text{entry}(\psi) = \alpha,\\
&\text{trans}(\psi) = \emptyset,\\
&\text{exit}(\psi) = \{(\alpha, \mathbf{true})\}
\end{aligned}$$

2. $\psi \equiv \alpha :$ **await** $\mathcal{B}$ **then** a vagy $\psi \equiv \alpha :$ **await** $\mathcal{B}$:

$$\begin{aligned}
&\text{entry}(\psi) = \alpha,\\
&\text{trans}(\psi) = \emptyset,\\
&\text{exit}(\psi) = \{(\alpha, \mathcal{B})\}
\end{aligned}$$

3. $\psi \equiv \alpha :$ **if** $\mathcal{B}$ **then** ψ_1 **else** ψ_2 **fi**:

$$
\begin{aligned}
&\mathrm{entry}(\psi) = \alpha,\\
&\mathrm{trans}(\psi) = \mathrm{trans}(\psi_1) \cup \mathrm{trans}(\psi_2) \cup\\
&\quad \cup \{(\alpha, \mathcal{B}, \mathrm{entry}(\psi_1)), (\alpha, \neg\mathcal{B}, \mathrm{entry}(\psi_2))\},\\
&\mathrm{exit}(\psi) = \mathrm{exit}(\psi_1) \cup \mathrm{exit}(\psi_2)
\end{aligned}
$$

4. $\psi \equiv \alpha :$ **if** $\mathcal{B}$ **then** ψ_1 **fi**:

$$
\begin{aligned}
&\mathrm{entry}(\psi) = \alpha,\\
&\mathrm{trans}(\psi) = \mathrm{trans}(\psi_1) \cup \{(\alpha, \mathcal{B}, \mathrm{entry}(\psi_1))\},\\
&\mathrm{exit}(\psi) = \mathrm{exit}(\psi_1) \cup \{(\alpha, \neg\mathcal{B})\}
\end{aligned}
$$

5. $\psi \equiv \alpha :$ **while** $\mathcal{B}$ **do** ψ_1 **od**:

$$
\begin{aligned}
&\mathrm{entry}(\psi) = \alpha,\\
&\mathrm{trans}(\psi) = \mathrm{trans}(\psi_1) \cup\\
&\quad \{(\alpha, \mathcal{B}, \mathrm{entry}(\psi_1))\} \cup \{(\beta, \mathcal{C}, \alpha) \mid (\beta, \mathcal{C}) \in \mathrm{exit}(\psi_1)\},\\
&\mathrm{exit}(\psi) = \{(\alpha, \neg\mathcal{B})\}
\end{aligned}
$$

6. $\psi \equiv \alpha :\ \psi_1; \psi_2$ (ψ_1 unlabelled satement ψ_2 statement sequence):

$$
\begin{aligned}
&\mathrm{entry}(\psi) = \alpha,\\
&\mathrm{trans}(\psi) = \mathrm{trans}(\psi_1) \cup \mathrm{trans}(\psi_2) \cup\\
&\quad \{(\beta, \mathcal{C}, \mathrm{entry}(\psi_2)) \mid (\beta, \mathcal{C}) \in \mathrm{exit}(\psi_1)\},\\
&\mathrm{exit}(\psi) = \mathrm{exit}(\psi_2)
\end{aligned}
$$

$\mathrm{trans}(\Pi_i) \subset \mathcal{M}_{\Pi_i} \times \mathcal{F}(\mathcal{L}_P) \times \mathcal{M}_{\Pi_i}$

1. $\Pi_i \equiv \psi; \alpha :$ **stop** (ψ statement sequence):

$$\mathrm{trans}(\Pi_i) = \mathrm{trans}(\psi) \cup \{(\beta, \mathcal{C}, \alpha) \mid (\beta, \mathcal{C}) \in \mathrm{exit}(\psi)\}$$

2. $\Pi_i \equiv$ **loop** ψ **end** (ψ statement sequence):

$$\mathrm{trans}(\Pi_i) = \mathrm{trans}(\psi) \cup \{(\beta, \mathcal{C}, \mathrm{entry}(\psi)) \mid (\beta, \mathcal{C}) \in \mathrm{exit}(\psi)\}$$

$\alpha \in \overline{\mathcal{M}}_\Pi : \quad E_\alpha \in \mathcal{L}_P$

$$E_\alpha = \begin{cases} \mathcal{B} & \text{ha } \alpha \quad \textbf{await } \mathcal{B} \ (\textbf{then } a) \text{ alakú utasítást címkéz,} \\ \textbf{true} & \text{különben.} \end{cases}$$

Programállapot

Legyen **S** struktúra $\mathcal{L}_P$-hez,
Π $\mathcal{L}_P$ és $\mathcal{A}$ feletti program.

Π *program állapota:*

$$\eta = (\mu,\ \lambda_1, ..., \lambda_p,\ \kappa),$$

ahol
- μ programváltozó-értékelés,
- $\lambda_i \in \mathcal{M}_{\Pi_i}$,
- $\kappa \in \{0, 1, ..., p\}$.

Program végrehajtási sorozata

Legyen ξ globális változó értékelés. A Π *program végrehajtási sorozata* ($\mathbf{S}$ és ξ mellett):

$$\mathbf{W}_\Pi = \{\eta_0, \eta_1, \eta_2, ...\}$$

programállapotok végtelen sorozata, amely a következő tulajdonságokkal rendelkezik:

- $\eta_0 = (\mu_0,\ \alpha_0^{(1)}, ..., \alpha_0^{(p)},\ \kappa_0)$ és $\mathbf{S}^{(\xi,\mu_0)}(R) = \mathbf{t}$
- Ha $\eta_j = (\mu,\ \lambda_1, ..., \lambda_i, ..., \lambda_k, i)$, akkor $\eta_{j+1} = (\mu',\ \lambda_1, ..., \lambda_i', ..., \lambda_k, \kappa')$, $(\lambda_i, C, \lambda_i') \in \mathrm{trans}(\Pi_i)$ és $\mathbf{S}^{(\xi,\mu)}(C) = \mathbf{t}$. Továbbá, ha λ_i olyan utasítást címkéz, amelyre $\notin \mathcal{A}$, akkor $\mu = \mu'$.
- Ha $\eta_j = (\mu,\ \lambda_1, ..., \lambda_k, 0)$, akkor $\eta_{j+1} = \eta_j$, és minden i-re, $i = 1, ..., p$: $\mathbf{S}^{(\xi,\mu)}(E_{\lambda_i}) = \mathbf{f}$ vagy $\lambda_i = \alpha_e^{(i)}$.

$\mathcal{L}_{TP\Pi}$ logikai nyelv

$\mathcal{L}_{TP\Pi}$ az $\mathcal{L}_{TP}$ logikai nyelv kiterjesztése a következő **logikai változókkal**:

- λ minden $\lambda \in \overline{\mathcal{M}_\Pi}$,
- at λ minden $\lambda \in \mathcal{M}_\Pi$.

$\mathbf{W}_\Pi$-nek feleljen meg a következő temporális $\mathbf{K} = (\mathbf{S}, \xi, \mathbf{W})$ (**Kripke**) struktúra:

ha $\eta_i = (\mu,\ \lambda_1, ..., \lambda_i, ..., \lambda_k, \kappa)$, akkor a megfelelő $\eta_i = (\eta_i^{(1)}, \eta_i^{(2)})$ értékelésre:

- $\eta_i^{(1)}(a) = \mu(a)$ a programváltozókra,
- $\eta_i^{(2)}(\lambda) = \mathbf{t}$ iff, $\lambda = \lambda_\kappa$ és $\kappa \neq 0$,
- $\eta_i^{(2)}(\mathrm{at}\lambda) = \mathbf{t}$ iff, $\lambda = \lambda_j$ valamely $j = 1, ..., p$-re.

Programaxiómák

- *Struktúrális axiómák.*

Minden programra érvényes tulajdonságokat fogalmaznak meg.

- *Specifikációs axiómák.*

Csak az adott programra jellemző axiómák.

Jelölések:

$\overline{\mathcal{M}}_\Pi = \{\alpha_1, ..., \alpha_l\}$

$start_\Pi : \quad \mathrm{at}\alpha_0^{(1)} \wedge ... \wedge \mathrm{at}\alpha_0^{(p)} \wedge R$

$nil_\Pi : \quad \neg\alpha_1 \wedge \neg\alpha_2 \wedge ... \wedge \neg\alpha_l$

Struktúrális axiómák

(B1) $start_\Pi \rightarrow \Box A \vdash A$

(B2) $nil_\Pi \wedge A \rightarrow \circ(nil_\Pi \wedge A)$

(Π_1) $\lambda \rightarrow \neg\lambda'$ ha $\lambda \not\equiv \lambda'$

(Π_2) $\lambda \rightarrow \mathrm{at}\lambda$

(Π_3) $\mathrm{at}\alpha_j^{(i)} \rightarrow \neg\mathrm{at}\alpha_k^{(i)}$

ha $j \neq k$, $k = 0, 1, ..., m_i$, $i = 1, ..., p$,

(Π_4) $\mathrm{at}\lambda \wedge E_\lambda \rightarrow \neg nil_\Pi$

(Π_5) $\mathrm{at}\lambda \wedge \neg\lambda \rightarrow \circ\mathrm{at}\lambda$

(Π_6) $\mathrm{at}\alpha_e^{(i)} \rightarrow \circ\mathrm{at}\alpha_e^{(i)}$

$i = 1, ..., p$

(Π_7) $\mathrm{at}\lambda \wedge P \rightarrow \circ P$

ha λ olyan utasítást címkéz,
amely $\notin \mathcal{A}$, és P P-formula.

Specifikációs axiómák

(CS) $\lambda \rightarrow (C_1 \wedge \circ\mathrm{at}\lambda_1) \vee ... \vee (C_q \wedge \circ\mathrm{at}\lambda_q)$

ahol $(\lambda, C_1, \lambda_1), ..., (\lambda, C_q, \lambda_q) \in \mathrm{trans}(\Pi_i)$
valamely i-re, $i = 1, ..., p$, és $\mathrm{trans}(\Pi_i)$ nem
tartalmaz más $(\lambda, ...)$ alakú elemet.

($data$) $\mathrm{Th}(\mathbf{S}_\Pi)$ minden formulája

Az elemi utasítások hatásának
axiómatikus specifikációja:

$$\lambda \wedge P \rightarrow \circ Q$$

Például:

($assign$) $\lambda \wedge P_a(t) \rightarrow \circ P$ (P P-formula)

minden $\lambda :\ a := t$ vagy
$\lambda :$ **await** B **then** $a := t$
alakú utasításra, amely Π-ben előfordul.

Programszemantika

Definíció:
A $\mathbf{K} = (\mathbf{S}, \xi, \mathbf{W})$ **Kripke** struktúra
Π-*megfelelő*, ha
- $\mathbf{S}$ a Π-hez tartozó $\mathbf{S}_\Pi$ struktúra,
- $\mathbf{W}$ a Π valamely legális végrehajtási sorozatának felel meg,
- ξ globális változóértékelés.

Definíció:
Az $\mathcal{L}_{TP\Pi}$ logikai nyelv valamely
$\mathcal{A}$ formulája Π-*érvényes*, ha $\mathcal{A}$ érvényes
minden Π-*megfelelő* $\mathbf{K} = (\mathbf{S}, \xi, \mathbf{W})$ **Kripke**
struktúrában.

Definíció:
Az $\mathcal{L}_{TP\Pi}$ logikai nyelv valamely
$\mathcal{A}$ formulája Π-*szemantikus* következménye
a zárt formulákból álló
az $\mathcal{F}$ formula halmaznak - $\mathcal{F} \Vdash_\Pi \mathcal{A}$ -, ha $\mathcal{A}$ érvényes
minden olyan Π-*megfelelő* **Kripke**
struktúrában, amelyben $\mathcal{F}$ minden formulája
érvényes.

Definíció:
Az $\mathcal{L}_{TP\Pi}$ logikai nyelv valamely
$\mathcal{A}$ formulája Π-*szemantikus* következménye
az $\mathcal{F}$ formula halmaznak - $\mathcal{F} \Vdash_\Pi \mathcal{A}$ -,
ha $\mathcal{A}$ Π-*szemantikus* következménye
az $\mathcal{F}$-hez tartozó formulák univerzális
lezártjainak.

Jelölje Spec(Π) a (B1) szabály kivételével
a programaxiómák halmazát.

Definíció:
Az $\mathcal{A}$ formula Π-*levezethető* - $\Pi \vdash \mathcal{A}$ -, ha

$$\mathrm{Spec}(\Pi) \vdash \mathcal{A}$$

a $\Sigma_{TP} + (\mathrm{B1})$ formális rendszerben.

Tétel:
Legyen Π program. Legyen $\mathcal{A}$ az $\mathcal{L}_{TP\Pi}$ logikai nyelv valamely formulája, és legyen $\mathcal{F}$ $\mathcal{L}_{TP\Pi}$-hez tartozó formulákból álló halmaz. Ha

$$\mathcal{F} \cup \mathrm{Spec}(\Pi) \vdash \mathcal{A}$$

a $\Sigma_{TP} + (\mathrm{B1})$ formális rendszerben, akkor

$$\mathcal{F} \Vdash_{\Pi} \mathcal{A}.$$

$$
\begin{array}{rl}
\Psi \equiv \textbf{initial} & nextinput = u_0 \wedge nr = 1 \wedge \\
 & \wedge\ ls = mn = a = 0; \\
\textbf{cobegin} & \\
\textbf{loop} & \\
\alpha_0 : & \\
 & \textbf{if}\ ls = a\ \textbf{then} \\
 & ls := ls \oplus 1; d := nextinput\ \textbf{fi}; \\
\alpha_1 : & \\
 & send(ls, d)\ to\ (mn, inf) \\
\textbf{end} & \\
\| & \\
\textbf{loop} & \\
\beta_0 : & \\
 & \textbf{if}\ mn = nr\ \textbf{then} \\
 & nextoutput := inf; \\
 & nr := nr \oplus 1\ \textbf{fi}; \\
\beta_1 : & \\
 & send(nr \oplus 1)\ to\ (a) \\
\textbf{end} & \\
\textbf{coend} &
\end{array}
$$

A Ψ program specifikációja

– $\alpha_1 \to \circ[\ (mn, inf) = (ls, d) \lor$
$(mn, inf) = (error, error)]$

– $\alpha_1 \land P \to \circ P$
minden P P-formulára, amely nem
tartalmazza az mn és *inf* változókat.

– $\beta_1 \to \circ(a = nr \oplus 1 \lor a = error)$

– $\beta_1 \land P \to \circ P$
minden P P-formulára, amely nem
tartalmazza a-t.

– $\alpha_0 \land ls = a \land\ nextinput = u_i \land ls = ls_0 \to$
$\circ(nextinput = u_{i+1} \land$
$ls = ls_0 \oplus 1 \land d = u_i)$

– $\alpha_0 \land P \to \circ P$
minden P P-formulára, amely nem
tartalmazza az *ls* és d változókat.

– $\alpha_0 \land ls \neq a \land P \to \circ P$
minden P P-formulára.

– $\beta_0 \land\ mn = nr \land nr = nr_0 \to$
$\circ(nextoutput = inf \land nr = nr_0 \oplus 1)$

– $\beta_0 \land P \to \circ P$
minden P P-formulára, amely nem
tartalmazza az *nextoutput* és nr változókat.

– $\beta_0 \land mn \neq nr \land P \to \circ P$
minden P P-formulára.

Ψ-invariáns tulajdonságok:

$$\vdash_{\Sigma_{TP\Psi}} ((nr = 0 \ \vee \ nr = 1) \wedge (ls = 0 \ \vee \ ls = 1)) \tag{1}$$

$$\vdash_{\Sigma_{TP\Psi}} (d = u_i \to nextinput = u_{i+1}) \tag{2}$$

$$\begin{aligned}\vdash_{\Sigma_{TP\Psi}} (\quad & (mn = nr \to nr = ls \wedge inf = d) \wedge \\ & (ls = a \to nr \neq ls))\end{aligned} \tag{3}$$

Állítások:

$$\begin{aligned}\vdash_{\Sigma_{TP\Psi}} \quad & start_\Psi \to \\ & inf = u_0 \mathbf{atnext}(\beta_0 \wedge mn = nr)\end{aligned} \tag{4}$$

$$\begin{aligned}\vdash_{\Sigma_{TP\Psi}} \quad & \beta_0 \wedge mn = nr \wedge inf = u_i \to \\ & inf = u_{i+1} \mathbf{atnext}(\beta_0 \wedge mn = nr)\end{aligned} \tag{5}$$

Ha érvényes:

$$\Box \diamond (at_\lambda \wedge E_\lambda) \to \diamond \lambda \tag{6}$$

minden λ -ra, $\lambda \in \overline{\mathcal{M}}_{\Pi_i}$
fair ütemezési feltétel, akkor

$$\begin{aligned}\{\diamond(\alpha_0 \quad & \wedge a \neq error), \diamond(\beta_0 \wedge mn \neq error)\} \\ & \vdash_{\Sigma_{TP\Psi}} \diamond(\beta_0 \wedge mn = nr)\end{aligned} \tag{7}$$

Legyen

$$B_i: \begin{array}{rl} (ls \neq nr & \rightarrow nextinput = u_i) \wedge \\ & \wedge (ls = nr \rightarrow d = u_i) \end{array} \tag{8}$$

Könnyen látható, hogy

$$\gamma \wedge B_i \rightarrow \circ B_i \tag{9}$$

Ψ-invariáns, ha $\gamma \in \{\alpha_0, \alpha_1, \beta_1\}$.
(3)-ból közvetlen következik, hogy

$$mn = nr \wedge B_i \rightarrow inf = u_i \tag{10}$$

Ψ-invariáns.
Ebből adódik, hogy

$$B_i \rightarrow (D \wedge mn = nr \rightarrow inf = u_i) \tag{11}$$

Ψ-invariáns tetszés szerinti D esetén.
Ugyanakkor nyilván

$$B_i \rightarrow (C \rightarrow (B_i \wedge C) \tag{12}$$

Ψ-invariáns tetszés szerinti C esetén.

Mindezek alapján

$$\begin{array}{rl} \gamma \wedge E \wedge B_i \rightarrow & \circ(D \wedge mn = nr \rightarrow inf = u_i) \wedge \\ \wedge & \circ(C \rightarrow C \wedge B_i) \end{array} \tag{13}$$

Ψ-invariáns minden γ-ra,
amelye $\gamma \in \{\alpha_0, \alpha_1, \beta_1\}$.
Innen látható, hogy ha
$C: \neg(D \wedge mn = nr)$, $E: C$, és $D: \beta_0$,
akkor

$$\begin{array}{rl} \gamma \wedge \neg(\beta_0 & \wedge mn = nr) \wedge B_i \rightarrow \\ & \circ(\beta_0 \wedge mn = nr \rightarrow inf = u_i) \wedge \\ \wedge & \circ(\neg(\beta_0 \wedge mn = nr) \rightarrow \\ & \neg(\beta_0 \wedge mn = nr) \wedge B_i) \end{array} \tag{14}$$

Ψ-invariáns minden γ-ra,
amelye $\gamma \in \{\alpha_0, \alpha_1, \beta_0, \beta_1\}$.

Mivel a program ciklikus,
és nincs benne **await** utasítás, ezért

$$\neg nil_\Psi \tag{15}$$

Ψ-invariáns.
Tehát

$$\begin{aligned} nil_\Psi \wedge \neg(\beta_0 \; & \wedge mn = nr) \wedge B_i \rightarrow \\ & \circ(\beta_0 \wedge mn = nr \rightarrow inf = u_i) \wedge \\ \wedge \; & \circ(\neg(\beta_0 \wedge mn = nr) \rightarrow \\ & \neg(\beta_0 \wedge mn = nr) \wedge B_i) \end{aligned} \tag{16}$$

is **Ψ-invariáns.**
Mindezekből adódik, hogy

$$\begin{aligned} \neg(\beta_0 \; & \wedge mn = nr) \wedge B_i \rightarrow \\ & \circ(\beta_0 \wedge mn = nr \rightarrow inf = u_i) \wedge \\ \wedge \; & \circ(\neg(\beta_0 \wedge mn = nr) \rightarrow \\ & \neg(\beta_0 \wedge mn = nr) \wedge B_i) \end{aligned} \tag{17}$$

Ψ-invariáns, ahonnan

$$\begin{aligned} \neg(\beta_0 \; & \wedge mn = nr) \wedge B_i \rightarrow \\ & inf = u_i \mathbf{atnext}(\beta_0 \wedge mn = nr) \end{aligned} \tag{18}$$

Ψ-invariáns.

$$\begin{aligned} start_\Psi \; & \rightarrow \\ & \neg(\beta_0 \wedge mn = nr) \wedge B_0 \end{aligned} \tag{19}$$

miatt a (4) állítás következik (18) és (19)-ból.
Ha $\gamma \in \{\alpha_0, \alpha_1, \beta_1\}$,
akkor tetszőleges V formula esetén

$$\begin{aligned} \gamma \; & \wedge((\beta_0 \wedge mn = nr) \rightarrow V) \wedge \\ & \wedge(\neg(\beta_0 \wedge mn = nr) \rightarrow B_{i+1}) \rightarrow \gamma \wedge B_{i+1} \end{aligned} \tag{20}$$

Ψ-levezethető. Ugyanakkor

$$\begin{aligned} \neg(\beta_0 \; & \wedge mn = nr) \wedge B_{i+1}) \rightarrow \\ & ((\beta_0 \wedge mn = nr) \rightarrow V) \wedge \\ & \wedge(\neg(\beta_0 \wedge mn = nr) \rightarrow B_{i+1}) \end{aligned} \tag{21}$$

miatt

$$\begin{aligned}\gamma \quad & \wedge((\beta_0 \wedge mn = nr) \to V)\wedge \\ & \wedge(\neg(\beta_0 \wedge mn = nr) \to B_{i+1}) \to \\ & \quad \circ(\beta_0 \wedge mn = nr \to inf = u_{i+1})\wedge \\ & \wedge \circ (\neg(\beta_0 \wedge mn = nr) \to \\ & \qquad ((\beta_0 \wedge mn = nr) \to V)\wedge \\ & \quad \wedge(\neg(\beta_0 \wedge mn = nr) \to B_{i+1})\end{aligned} \tag{22}$$

Ψ-invariáns, ha $\gamma \in \{\alpha_0, \alpha_1, \beta_1\}$.
A V formulát úgy kell megválasztani, hogy

$$\begin{aligned}(\quad & \beta_0 \wedge mn = nr) \wedge ((\beta_0 \wedge mn = nr) \to V)\wedge \\ & \wedge(\neg(\beta_0 \wedge mn = nr) \to B_{i+1}) \to \circ B_{i+1}\end{aligned} \tag{23}$$

teljesüljön.

$$\begin{aligned}(\quad & \beta_0 \wedge mn = nr) \wedge ((\beta_0 \wedge mn = nr) \to V) \to \\ & \beta_0 \wedge mn = nr \wedge mn = ls \wedge d = inf \wedge V \to \\ & \circ(nr \neq ls \wedge d = inf \wedge V)\end{aligned} \tag{24}$$

Innen látható, hogy

$$nr \neq ls \wedge d = inf \wedge V \to B_{i+1} \tag{25}$$

teljesül, ha

$$V: \quad inf = u_i \tag{26}$$

mivel ekkor

$$\begin{aligned}& nr \neq ls \wedge d = inf \wedge inf = u_i \to \\ & nr \neq ls \wedge nextinput = u_{i+1} \to B_{i+1}\end{aligned} \tag{27}$$

(2) alapján. Mivel

$$\begin{aligned}(\quad & \beta_0 \wedge mn \neq nr) \wedge ((\beta_0 \wedge mn = nr) \to V)\wedge \\ & \wedge(\neg(\beta_0 \wedge mn = nr) \to B_{i+1}) \to \\ & \beta_0 \wedge \neg(\beta_0 \wedge mn = nr) \wedge B_{i+1}\end{aligned} \tag{28}$$

ezért (22) teljesül $\gamma = \beta_0$ esetén is.

Tehát

$$\begin{aligned}& ((\beta_0 \wedge mn = nr) \to inf = u_i)\wedge \\ & \wedge(\neg(\beta_0 \wedge mn = nr) \to B_{i+1}) \to \\ & \quad inf = u_{i+1}\,\mathbf{atnext}(\beta_0 \wedge mn = nr)\end{aligned} \tag{29}$$

Mivel

$$\begin{aligned}(\beta_0 \quad & \wedge mn = nr) \wedge inf = u_i \to \\ & ((\beta_0 \wedge mn = nr) \to inf = u_i) \wedge \\ & \wedge(\neg(\beta_0 \wedge mn = nr) \to B_{i+1})\end{aligned} \tag{30}$$

ezért (5) következik (29) és (30)-ból.

A (7) állítás bizonyítása
Igazak a következő:

$$\diamond B \ \vdash \ \Box A \rightarrow \diamond(B \wedge \Box A) \tag{31}$$
$$\diamond B \ \vdash \ \Box A \rightarrow \diamond(B \wedge A) \tag{32}$$

vagy ezekkel ekvivalens

$$\neg\Box\neg B \ \vdash \ \Box A \rightarrow \neg\Box(\Box A \rightarrow \neg B) \tag{33}$$
$$\neg\Box\neg B \ \vdash \ \Box A \rightarrow \neg\Box(A \rightarrow \neg B) \tag{34}$$

levezethetőségek.
Ezek igazolhatók a Σ_{TA} teljességére
történő hivatkozással.

$$\beta_0 \wedge mn = nr \equiv \neg(\beta_0 \rightarrow mn \neq nr)$$

miatt

$$\diamond(\beta_0 \wedge mn = nr) \equiv \neg\Box(\beta_0 \rightarrow mn \neq nr)$$

A (7) állítás levezetésének logikai lépései

$$\begin{aligned} \Box(\beta_0 \rightarrow mn \neq nr) \quad &\rightarrow \quad \diamond(nr = ls) \\ (nr = ls) \quad &\rightarrow \quad \diamond(\beta_0 \wedge mn = nr) \\ \Box(\beta_0 \rightarrow mn \neq nr) \quad &\rightarrow \quad \diamond(\beta_0 \wedge mn = nr) \end{aligned} \tag{35}$$

$$\diamond\,(\beta_0 \wedge mn = nr) \tag{36}$$

$$\begin{aligned} &\diamond\beta_1 \\ &\diamond(a = nr \oplus 1 \vee a = error) \end{aligned}$$

$$\begin{aligned} \Box(\beta_0 \ &\rightarrow mn \neq nr) \wedge \Box(nr \neq ls) \rightarrow \\ \diamond \ &[(a = nr \oplus 1 \vee a = error) \wedge \\ &\wedge \Box(\beta_0 \rightarrow mn \neq nr) \wedge \Box(nr \neq ls)] \end{aligned}$$

$$\begin{aligned} &(a = nr \oplus 1 \vee a = error) \wedge \\ &\wedge \Box(\beta_0 \rightarrow mn \neq nr) \wedge \Box(nr \neq ls) \rightarrow \\ &\Box(a = nr \oplus 1 \vee a = error) \wedge \\ &\wedge \Box(\beta_0 \rightarrow mn \neq nr) \wedge \Box(nr \neq ls) \end{aligned}$$

$$\diamond(\alpha_0 \wedge a \neq error)$$

$$\begin{aligned}\Box(a = nr \oplus 1 \quad \vee a = error) \wedge \Box(nr \neq ls) \rightarrow \\ \diamond \quad (\alpha_0 \wedge a = ls \wedge nr \neq ls)\end{aligned}$$

$$\alpha_0 \wedge a = ls \wedge nr \neq ls \rightarrow \circ(nr = ls)$$

$$\Box(\beta_0 \rightarrow mn \neq nr) \wedge \Box(nr \neq ls) \rightarrow \diamond(nr = ls)$$

$$\Box(\beta_0 \rightarrow mn \neq nr) \rightarrow \diamond(nr = ls)$$

$$\begin{aligned}\Box(\beta_0 \rightarrow \quad & mn \neq nr) \wedge (nr = ls) \rightarrow \\ & \Box(ls = nr \wedge a \neq ls)\end{aligned}$$

$$\begin{aligned}&\diamond\alpha_1 \\ &\diamond(mn = ls \vee mn = error)\end{aligned}$$

$$\begin{aligned}&\Box(\beta_0 \rightarrow mn \neq nr) \wedge (nr = ls) \rightarrow \\ &\diamond[(mn = ls \vee mn = error) \wedge \\ &\wedge \Box(\beta_0 \rightarrow mn \neq nr) \wedge \Box(ls = nr \wedge a \neq ls)]\end{aligned}$$

$$\begin{aligned}&(mn = ls \vee mn = error) \wedge \\ &\wedge \Box(\beta_0 \rightarrow mn \neq nr) \wedge \Box(ls = nr \wedge a \neq ls) \rightarrow \\ &\Box(mn = ls \vee mn = error) \wedge \\ &\wedge \Box(\beta_0 \rightarrow mn \neq nr) \wedge \Box(ls = nr \wedge a \neq ls)\end{aligned}$$

$$\begin{aligned}&\Box(mn = ls \vee mn = error) \wedge \\ &\quad \wedge \Box(ls = nr \wedge a \neq ls) \rightarrow \\ &\Box(mn = nr \vee mn = error)\end{aligned}$$

$$\diamond(\beta_0 \wedge mn \neq error)$$

$$\Box(mn = nr \vee mn = error) \rightarrow \diamond(\beta_0 \wedge mn = nr)$$

$$\begin{aligned}\Box(\beta_0 \rightarrow \quad & mn \neq nr) \wedge (nr = ls) \rightarrow \\ & \diamond(\beta_0 \wedge mn = nr)\end{aligned}$$

$$(nr = ls) \rightarrow \diamond(\beta_0 \wedge mn = nr)$$