Definíciók és tételek

1. Felhasznált matematikai fogalmak

Jelölés

1. $\mathbb{N}$: a természetes számok halmaza, $\mathbb{Z}$: az egész számok halmaza
2. $\mathbb{L}$: a logikai értékek halmaza, $\mathbb{L} \overset{\text{def}}{=} \{$ igaz, hamis $\}$
3. véges sorozat: $\alpha = <\alpha_1, \ldots, \alpha_n>$, értelmezési tartománya: $\mathcal{D}_\alpha = \{1, \ldots, n\}$
4. az $\alpha =< \alpha_1, \ldots, \alpha_n >$ véges sorozat hossza: $|\alpha| = n$
5. végtelen sorozat: $\alpha = <\alpha_1, \ldots>$, értelmezési tartománya: $\mathcal{D}_\alpha = \mathbb{N}$
6. az A halmaz elemeiből képzett véges sorozatok halmaza: A^*
7. az A halmaz elemeiből képzett végtelen sorozatok halmaza: A^∞
8. az A halmaz elemeiből képzett véges és végtelen sorozatok halmaza: A^{**}

Definíció

1. az $\alpha \in A^*$ és a $\beta \in A^{**}$ sorozatok *konkatenáltja*: $\text{kon}(\alpha, \beta) \overset{\text{def}}{=} <\alpha_1, \ldots, \alpha_n, \beta_1 \ldots>$, ahol $n = |\alpha|$
2. Legyen $\alpha^1, \alpha^2, \ldots, \alpha^{n-1} \in A^*$, $\alpha^n \in A^{**}$. $\text{kon}(\alpha^1, \ldots, \alpha^n) = \text{kon}(\alpha^1, \text{kon}(\alpha^2, \ldots, \alpha^n))$
3. Az $\alpha \in A^{**}$ *redukáltjának* nevezzük, és $\text{red}(\alpha)$-val jelöljük azt a sorozatot, amit úgy kapunk, hogy az α minden azonos elemekből álló véges részsorozatát a részsorozat egyetlen elemével helyettesítjük.
4. Legyen $\alpha^1, \alpha^2, \ldots, \alpha^{n-1} \in A^*$, $\alpha^n \in A^{**}$. $\chi_n(\alpha^1, \ldots, \alpha^n) \overset{\text{def}}{=} \text{red}(\text{kon}(\alpha^1, \ldots, \alpha^n))$
5. Legyen $\alpha^i \in A^*$ $(i \in \mathbb{N})$. $\chi_\infty(\alpha^1, \alpha^2, \ldots) \overset{\text{def}}{=} \text{red}(\text{kon}(\alpha^1, \alpha^2, \ldots)$
6. Ha $\alpha =< \alpha_1, \ldots, \alpha_n >\in A^*$, akkor $\tau(\alpha) \overset{\text{def}}{=} \alpha_n$
7. Legyen $I = \{i_1, i_2, \ldots, i_n\} \subset \mathbb{N}$. Legyen A_i tetszőleges halmaz $(i \in I)$.
$\overset{n}{\underset{i \in I}{\times}} A_i \overset{\text{def}}{=} A_{i_1} \times \ldots \times A_{i_n} \overset{\text{def}}{=} \{(a_{i_1}, a_{i_2}, \ldots, a_{i_n}) \mid a_{i_j} \in A_{i_j} \wedge i_j \in I\}$, ahol $i_1 < i_2 < \ldots < i_n$.
8. Legyen $I = \{i_1, i_2, \ldots, i_n\} \subset \mathbb{N}$, $J = \{j_1, j_2, \ldots, j_m\} \subset \mathbb{N}$ $(m, n \in \mathbb{N})$.
$A = \overset{n}{\underset{k=1}{\times}} A_{i_k}$, $B = \overset{m}{\underset{k=1}{\times}} A_{j_k}$. A B halmaz az A halmaz *altere*, ha $J \subseteq I$.
9. Legyen $I = \{i_1, i_2, \ldots, i_n\} \subset \mathbb{N}$, $J = \{j_1, j_2, \ldots, j_m\} \subset \mathbb{N}$ $(m, n \in \mathbb{N},\ m < n)$.
$A = \overset{n}{\underset{k=1}{\times}} A_{i_k}$, $B = \overset{m}{\underset{k=1}{\times}} A_{j_k}$. A B tér *kiegészítő altere* az A-ra: $B' \overset{\text{def}}{=} \underset{k \in (I \setminus J)}{\times} A_k$.
10. Legyen $a \in A$ és B altere A-nak a $J = \{j_1, j_2, \ldots, j_m\} \subset \mathbb{N}$ indexhalmazzal. Ekkor a-nak a B-re vett *projekciója*
$\text{pr}_B(a) \overset{\text{def}}{=} (a_{j_1}, a_{j_2}, \ldots, a_{j_m})$.

11. Legyen B altér A-ban és legyen B' a B kiegészítő altere A-hoz. "$\otimes$" bináris művelet: $\otimes : B \times B' \to A$. Tetszőleges $b \in B$ és $b' \in B'$ esetén $b \otimes b'$ A azon eleme, amelyre $\mathrm{pr}_B(b \otimes b') = b$ és $\mathrm{pr}_{B'}(b \otimes b') = b'$.

12. Legyen $\alpha \in A^{**}$. $\mathrm{pr}_B(\alpha) \overset{\text{def}}{=} < \mathrm{pr}_B(\alpha_1), \mathrm{pr}_B(\alpha_2), \ldots > \in B^{**}$.

13. Legyen $R \subseteq C \times D$, A altere C-nek, B altere D-nek.
$\mathrm{pr}_{A \times B}(R) \overset{\text{def}}{=} \{(pr_A(c), pr_B(d)) \mid (c,d) \in R\}$.

14. Legyen $R \subseteq A \times A$, B altere A-nak. $\mathrm{pr}_B(R) \overset{\text{def}}{=} \mathrm{pr}_{B \times B}(R)$.

15. Legyen $R \subseteq A \times A^{**}$, B altere A-nak. $\mathrm{pr}_B(R) \overset{\text{def}}{=} \mathrm{pr}_{B \times B^{**}}(R)$.

16. Az $R \subseteq A \times B$ halmazt *bináris relációnak* nevezzük.

17. Az $R \subseteq A \times B$ reláció képe $a \in A$ pontban: $R(a) \overset{\text{def}}{=} \{b \in B \mid (a,b) \in R\}$.

18. Az $R \subseteq A \times B$ reláció képe $H \subseteq A$ halmazon: $R(H) \overset{\text{def}}{=} \{b \in B \mid \exists a \in H : (a,b) \in R\}$.

19. Az $R \subseteq A \times B$ reláció *értelmezési tartománya*: $\mathcal{D}_R \overset{\text{def}}{=} \{a \in A \mid \exists b \in B : (a,b) \in R\}$.

20. Az $R \subseteq A \times B$ reláció *értékkészlete*: $\mathcal{R}_R \overset{\text{def}}{=} \{b \in B \mid \exists a \in A : (a,b) \in R\}$.

21. Az $R \subseteq A \times B$ reláció *determinisztikus reláció* (parciális függvény), ha
$\forall a \in \mathcal{D}_R : |R(a)| = 1$.

22. Az $R \subseteq A \times B$ reláció *függvény*, ha R parciális függvény és $\mathcal{D}_R = A$.

23. Az $R \subseteq A \times B$ reláció *inverze*: $R^{(-1)} \overset{\text{def}}{=} \{(b,a) \in B \times A \mid (a,b) \in R\}$.

24. A $H \subseteq B$ halmaz $R \subseteq A \times B$ reláció szerinti *inverz képe*:
$R^{(-1)}(H) \overset{\text{def}}{=} \{a \in A \mid \exists h \in H : (a,h) \in R\}$.

25. Az $R \subseteq A \times B$ reláció *komplementere*: $\overline{R} \overset{\text{def}}{=} \{(a,b) \in A \times B \mid (a,b) \notin R\}$.

26. Az $R_1 \subseteq A \times B$ és az $R_2 \subseteq B \times C$ relációk *kompozíciója*:
$R_2 \circ R_1 \overset{\text{def}}{=} \{(a,c) \in A \times C \mid \exists b \in B : (a,b) \in R_1 \wedge (b,c) \in R_2\}$.

27. Az $R_1 \subseteq A \times B$ és az $R_2 \subseteq B \times C$ relációk *szigorú kompozíciója*:
$R_2 \odot R_1 \overset{\text{def}}{=} \{(a,c) \in A \times C \mid R_1(a) \subseteq \mathcal{D}_{R_2} \wedge \exists b \in B : (a,b) \in R_1 \wedge (b,c) \in R_2\}$.

28. $R \subseteq A \times A$. $\mathrm{id}_A \overset{\text{def}}{=} R^0 \overset{\text{def}}{=} \{(a,a) \in A \times A\}$.

29. Az $R \subseteq A \times A$ reláció *n. hatványa*: $R^n \overset{\text{def}}{=} R \circ R^{n-1}$ $(n \in \mathbb{N})$.

30. A $H \subseteq B$ halmaz $R \subseteq A \times B$ reláció szerinti *ősképe*:
$R^{-1}(H) \overset{\text{def}}{=} \{a \in A \mid R(a) \subseteq H \wedge R(a) \neq \emptyset\}$.

31. Az $R \subseteq A \times A$ reláció $\alpha_0 \in A$ kezdőpontú, *véges pontláncainak* halmaza:
$L_R(\alpha_0) \overset{\text{def}}{=} \{< \alpha_0, \alpha_1, \ldots, \alpha_q > \in A^* \mid q \in \mathbb{N}_0 \wedge \forall i \in [1,q] : \alpha_i \in R(\alpha_{i-1}) \wedge \alpha_q \notin \mathcal{D}_R\}$.

32. Az $R \subseteq A \times A$ reláció $\alpha_0 \in A$ kezdőpontú *végtelen pontláncainak* halmaza:
$L_R^\infty(\alpha_0) \overset{\text{def}}{=} \{< \alpha_0, \alpha_1, \ldots > \in A^\infty \mid \forall i \in \mathbb{N} : \alpha_i \in R(\alpha_{i-1})\}$.

33. Az $R \subseteq A \times A$ reláció *lezártja*:
$\mathcal{D}_{\overline{R}} \overset{\text{def}}{=} \{a \in A \mid L_R^\infty(a) = \emptyset\}$ és $\forall a \in \mathcal{D}_{\overline{R}} : \overline{R}(a) \overset{\text{def}}{=} \{\tau(\alpha) \mid \alpha \in L_R(a)\}$.

34. Az $R \subseteq A \times A$ reláció *korlátos lezártja*:
$\mathcal{D}_{\overline{\overline{R}}} \overset{\text{def}}{=} \{a \in A \mid L_R^{\infty}(a) = \emptyset \wedge \exists n_a \in \mathbb{N}: \ \forall \alpha \in L_R(a) : |\alpha| \leq n_a\}$ és
$\forall a \in \mathcal{D}_{\overline{\overline{R}}}: \ \overline{\overline{R(a)}} \overset{\text{def}}{=} \{\tau(\alpha) \mid \alpha \in L_R(a)\}$.

35. Az $f \subseteq A \times \mathbb{L}$ reláció *logikai függvény (állítás)*, ha függvény.

36. Az f logikai függvény *igazsághalmaza*: $[f] \overset{\text{def}}{=} \{a \in A \mid f(a) = \text{igaz}\}$.

37. A $H \subseteq A$ halmaz *indikátorfüggvénye*: $P(H) : A \to \mathbb{L}$, $P(H)(a) \overset{\text{def}}{=} a \in H \ \ (a \in A)$.

38. Az $R \subseteq A \times \mathbb{L}$ reláció *igazsághalmaza*: $[R] \overset{\text{def}}{=} R^{-1}(\{ \text{ igaz } \})$.

39. Legyen $R \subseteq A \times B$, $H \subseteq A$. Az R reláció leszűkítése a H halmazra:
$R|_H \overset{\text{def}}{=} (R \cap (H \times B))$.

40. Legyen $R \subseteq A \times A$ és $\pi : A \to \mathbb{L}$. Az R reláció megszorítása a π feltételre:
$R|_\pi \overset{\text{def}}{=} (R \cap ([\pi] \times A)) \cup \{(a, a) \in A \times A \mid a \in [\pi] \setminus \mathcal{D}_R\}$.
Megjegyzés: $R|_\pi \neq R|_{[\pi]}$!

41. $\overline{R|_\pi}$ az R reláció π feltételre vonatkozó lezártja, $\overline{\overline{R|_\pi}}$ az R reláció π feltételre vonatkozó korlátos lezártja.

Állítás

1. $[f] \ = \ f^{-1}(\{ \text{ igaz } \})$.

2. Ha $\forall n \in \mathbb{N}: \ |A| > n$, akkor $\exists R \subseteq A \times A: \ \overline{R} \neq \overline{\overline{R}}$.

2. Alapvető definíciók és tételek

Definíció

1. Legyen $n \in \mathbb{N}$ és $A_1, \ldots, A_n$ tetszőleges halmaz. Az $A \overset{\text{def}}{=} A_1 \times \ldots \times A_n$ halmazt *állapottér*nek, az A_i halmazokat *típusértékhalmazok*nak nevezzük.

2. Az állapottér elemeit (az $a = (a_1, \ldots, a_n) \in A$ pontokat) *állapotok*nak nevezzük.

3. Az $a_i : A \to A_i$ projekciókat *változók*nak nevezzük ($i = 1, \ldots, n$).

4. Az $F \subseteq A \times A$ relációt *feladat*nak nevezzük.

5. Az $S \subseteq A \times A^{**}$ relációt *program*nak nevezzük, ha

1. $\mathcal{D}_S = A$
2. $\forall a \in A: \ \forall \alpha \in S(a): \ \alpha_1 = a$
3. $\forall \alpha \in \mathcal{R}_S: \ \alpha = \text{red}(\alpha)$

6. Legyen $S \subseteq A \times A^{**}$ program. A $p(S) \subseteq A \times A$ relációt, amelyre

1. $\mathcal{D}_{p(S)} = \{a \in A \mid S(a) \subseteq A^*\}$
2. $\forall a \in \mathcal{D}_{p(S)}: \ p(S)(a) = \{b \in A \mid \exists \alpha \in S(a): \ \tau(\alpha) = b\}$

az S program *programfüggvényé*nek nevezzük.

7. Az $S \subseteq A \times A^{**}$ program *megoldja* az $F \subseteq A \times A$ feladatot, ha

1. $\mathcal{D}_F \subseteq \mathcal{D}_{p(S)}$
2. $\forall a \in \mathcal{D}_F : \; p(S)(a) \subseteq F(a)$.

8. $S_1, S_2 \subseteq A \times A^{**}$ programok. S_1 és S_2 *ekvivalensek*, ha $p(S_1) = p(S_2)$.

9. Legyen B altere az A állapottérnek. Az $F \subseteq B \times B$ *feladat kiterjesztése* az A térre: $F' = \{(a_1, a_2) \in A \times A \mid (\mathrm{pr}_B(a_1), \mathrm{pr}_B(a_2)) \in F\}$.

10. Legyen B altere az A állapottérnek, B' a B altér kiegészítő altere az A-ra. Az $S \subseteq B \times B^{**}$ *program kiterjesztése* A-ra:
$S' = \{(a, \alpha) \in A \times A^{**} \mid (\mathrm{pr}_B(a), \mathrm{pr}_B(\alpha)) \in S \wedge \forall i \in \mathcal{D}_\alpha : \; \mathrm{pr}_{B'}(\alpha_i) = \mathrm{pr}_{B'}(a)\}$.

11. Legyen B közös altere A_1-nek és A_2-nek. S_1 program A_1-en, S_2 program A_2-n. S_1 és S_2 *ekvivalensek B-n*, ha $\mathrm{pr}_B(p(S_1)) = \mathrm{pr}_B(p(S_2))$.

12. Legyen B altere A-nak. A $G \subseteq A \times A$ feladat *vetítéstartó* a B altér felett, ha minden $a_1, a_2 \in \mathcal{D}_G$-re: ha $\mathrm{pr}_B(a_1) = \mathrm{pr}_B(a_2)$ akkor $\mathrm{pr}_B(G(a_1)) = \mathrm{pr}_B(G(a_2))$.

13. Legyen B altere A-nak és legyen B' kiegészítő altér B-hez A-ban. A $G \subseteq A \times A$ feladat *bővített identitás* a B altér és a B' kiegészítő altér felett, ha minden $(a_1, a_2) \in G$ esetén $(a_1, a_3) \in G$ is teljesül, ahol $\mathrm{pr}_B(a_3) = \mathrm{pr}_B(a_2)$ és $\mathrm{pr}_{B'}(a_3) = \mathrm{pr}_{B'}(a_1)$.

Állítás

Legyen B altere A-nak, B' B kiegészítő altere A-ra, S program B-n, $F \subseteq B \times B$ feladat, S' illetve F' S-nek, illetve F-nek kiterjesztése A-ra, $\overline{S} \subseteq A \times A^{**}$ S-sel ekvivalens program B-n, $\overline{F} \subseteq A \times A$ feladat és $F = \mathrm{pr}_B(\overline{F})$.

1. S' megoldja F'-t akkor és csak akkor, ha S megoldja F-et.

Bizonyítás

Tekintettel arra, hogy S' ekvivalens S-sel B-n, $\mathrm{pr}_B(F') = F$, valamint F' vetítéstartó B felett és bővített identitás B és B' felett, ezért a tétel állítása következik a a *változó bevezetésének tétele* és a *részfeladat kiválasztásának tételé*-ből.

2. Ha $\overline{S}$ megoldja F'-t, akkor S megoldja F-et (a *változó bevezetésének tétele*).

Bizonyítás

Először belátjuk, hogy $\mathcal{D}_F \subseteq \mathcal{D}_{p(S)}$. Legyen $a \in \mathcal{D}_F$ tetszőleges. Ekkor $\mathcal{D}_F$ definíciójából következik, hogy van olyan $b \in B$, amelyre $(a, b) \in F$. $\mathrm{pr}_B(F') = F$ miatt van olyan $\overline{a}, \overline{b} \in A$, amelyre $(\overline{a}, \overline{b}) \in F'$ és $\mathrm{pr}_B(\overline{a}) = a$ és $\mathrm{pr}_B(\overline{b}) = b$. $(\overline{a}, \overline{b}) \in F'$ miatt $\overline{a} \in \mathcal{D}_{F'}$. A feltétel szerint $\overline{S}$ megoldja az F' feladatot, ezért $\overline{a} \in \mathcal{D}_{p(\overline{S})}$. Ebből következik, hogy van olyan $\overline{\overline{b}} \in A$, amleyre, $(\overline{a}, \overline{\overline{b}}) \in p(\overline{S})$, de $\mathrm{pr}_B(\overline{S}) = p(S)$ igaz a feltevések szerint, ezért $(\mathrm{pr}_B(\overline{a}), \mathrm{pr}_B(\overline{\overline{b}})) \in p(S)$. mivel $\mathrm{pr}_B(\overline{a}) = a$, ezért $(a, \mathrm{pr}_B(\overline{\overline{b}})) \in p(S)$, tehát $a \in \mathcal{D}_p(S)$. Mivel $a \in \mathcal{D}_F$ tetszőleges volt, $\mathcal{D}_F \subseteq \mathcal{D}_p(S)$ igaz.

Az állítás igazolásához be kell még látni, hogy minden $a \in \mathcal{D}_F$-re: $p(S)(a) \subseteq F(a)$. Legyen $a \in \mathcal{D}_F$ tetszőleges. Az előzőek miatt $a \in \mathcal{D}_p(S)$ is teljesül. Legyen $b \in p(S)(a)$ tetszőleges. Ebből nyilván következik, hogy $(a, b) \in p(S)$. A $\mathrm{pr}_B(p(\overline{S})) = p(S)$ eqvivalencia feltétel miatt van olyan $\overline{a}, \overline{b} \in A$, amelyre $(\overline{a}, \overline{b}) \in p(\overline{S})$ és $\mathrm{pr}_B(\overline{a}) = a$, valamint $\mathrm{pr}_B(\overline{b}) = b$.

$\mathrm{pr}_B(\overline{a}) = a$-ból és $a \in \mathcal{D}_F$ következik, hogy $\overline{a} \in \mathcal{D}_{F'}$, mert $a \in \mathcal{D}_F$-ből következik, hogy van olyan $b \in B$, amelyre $(a,b) \in F$ és F' definíciója miatt, ha $\overline{\overline{b}} \in A$ olyan, amelyre $\mathrm{pr}_B(\overline{\overline{b}}) = b$, akkor $(\overline{a}, \overline{\overline{b}}) \in F'$. Ilyen $\overline{\overline{b}}$ biztosan létezik, tehát $\overline{a} \in \mathcal{D}_{F'}$.
A feltevés szerint $\overline{S}$ megoldja F'-et, ezért $\overline{a} \in \mathcal{D}_p(\overline{S})$ is igaz, és $(\overline{a}, \overline{b}) \in F'$ is teljesül a $p(\overline{S})(\overline{a}) \subseteq F'(\overline{a})$ tartalmazás miatt. Ha viszont $(\overline{a}, \overline{b}) \in F'$, akkor $\mathrm{pr}_B(F') = F$ miatt $(\mathrm{pr}_B(\overline{a}), \mathrm{pr}_B(\overline{b})) \in F$, azaz $(a,b) \in F$, tehát $b \in F(a)$. Mivel $b \in p(S)(a)$ tetszőleges volt, beláttuk, hogy tetszőleges $a \in \mathcal{D}_F$-re: $p(S)(a) \subseteq F(a)$. Amit bizonyítani kellett.

3. Ha S' megoldja $\overline{F}$-et, akkor S megoldja F-et.

Bizonyítás

$\mathcal{D}_F \subseteq \mathcal{D}_{p(S)}$ bizonyítása pontosan úgy történik, mint a *a változó bevezetésének tétele* bizonyítása esetén. A $\mathrm{pr}_B(p(S') = p(S)$ és $\mathrm{pr}_B(\overline{F}) = F$ feltételek teljesülnek, valamint S' megoldja az $\overline{F}$ feladatot, és a *a változó bevezetésének tétele* bizonyításának megfelelő részében csak ezeket a tulajdonságokat használtuk ki.

Az állítás igazolásához be kell még látni, hogy minden $a \in \mathcal{D}_F$-re: $p(S)(a) \subseteq F(a)$. Legyen $a \in \mathcal{D}_F$ tetszőleges. Az előzőek miatt $a \in \mathcal{D}_p(S)$ is teljesül. Legyen $b \in p(S)(a)$ tetszőleges. $a \in \mathcal{D}_F$ miatt van olyan $b^* \in B$, amelyre $(a, b^*) \in F$. A $\mathrm{pr}_B(\overline{F}) = F$ feltétel miatt van olyan $\overline{a}, \overline{b} \in A$, amelyre $(\overline{a}, \overline{b}) \in \overline{F}$ és $\mathrm{pr}_B(\overline{a}) = a$, valamint $\mathrm{pr}_B(\overline{b}) = b^*$. Abból a feltevésből, hogy S' megoldja $\overline{F}$-et következik, hogy $\overline{a} \in \mathcal{D}_{\overline{F}}$ miatt $\overline{a} \in \mathcal{D}_{p(S')}$ is teljesül.
$p(S') = \{(\overline{a}, \overline{b}) \in A \times A | (\mathrm{pr}_B(\overline{a}), \mathrm{pr}_B(\overline{b})) \in p(S) \quad \text{és} \quad \mathrm{pr}_{B'}(\overline{a}) = \mathrm{pr}_{B'}(\overline{b})\}$ összefüggés miatt $(\overline{a}, b \otimes \mathrm{pr}_{B'}(\overline{a})) \in p(S')$. Abból, hogy S' megoldja $\overline{(F)}$-et és $\overline{a} \in \mathcal{D}_{F'}$ következik, hogy $(\overline{a}, b \otimes \mathrm{pr}_{B'}(\overline{a})) \in \overline{F}$. Ugyanakkor $\mathrm{pr}_B(\overline{F}) = F$ miatt $(\mathrm{pr}_B(\overline{a}), \mathrm{pr}_B(b \otimes \mathrm{pr}_{B'}(\overline{a}))) \in F$, azaz $\mathrm{pr}_B(\overline{a}) = a$, valamint $\mathrm{pr}_B(b \otimes \mathrm{pr}_{B'}(\overline{a})) = b$ miatt $(a,b) \in F$, tehát $b \in F(a)$. Mivel $b \in p(S)(a)$ tetszőleges volt, beláttuk, hogy tetszőleges $a \in \mathcal{D}_F$-re: $p(S)(a) \subseteq F(a)$. Amit bizonyítani kellett.

4. Ha S megoldja F-et, $\overline{F}$ vetítéstartó B felett, és bővített identitás B és B' felett, akkor S' megoldja $\overline{F}$-et (*részfeladat kiválasztásának tétele*).

Bizonyítás

Először belátjuk, hogy $\mathcal{D}_{\overline{F}} \subseteq \mathcal{D}_{p(S')}$. Legyen $\overline{a} \in \mathcal{D}_{\overline{F}}$ tetszőleges. Ekkor $\mathcal{D}_{\overline{F}}$ definíciójából következik, hogy van olyan $\overline{b} \in A$, amelyre $(\overline{a}, \overline{b}) \in \overline{F}$. $\mathrm{pr}_B(\overline{F}) = F$ miatt $(\mathrm{pr}_B(\overline{a}), \mathrm{pr}_B(\overline{b})) \in F$, tehát $\mathrm{pr}_B(\overline{a}) \in \mathcal{D}_F$. A feltétel szerint S megoldja az F feladatot, ezért $\mathrm{pr}_B(\overline{a}) \in \mathcal{D}_{p(S)}$. Ez azt jelenti, hogy van olyan $b \in B$, amelyre $(\mathrm{pr}_B(\overline{a}), b) \in p(S)$. Mivel $p(S') = \{(\overline{a}, \overline{b}) \in A \times A | (\mathrm{pr}_B(\overline{a}), \mathrm{pr}_B(\overline{b})) \in p(S) \quad \text{és} \quad \mathrm{pr}_{B'}(\overline{a}) = \mathrm{pr}_{B'}(\overline{b})\}$, ezért $(\overline{a}, b \otimes \mathrm{pr}_{B'}(\overline{a})) \in p(S')$, tehát $\overline{a} \in \mathcal{D}_{p(S')}$. Mivel $\overline{a} \in \mathcal{D}_{\overline{F}}$ tetszőleges volt, $\mathcal{D}_{\overline{F}} \subseteq \mathcal{D}_{p(S')}$ igaz.

Az állítás igazolásához be kell még látni, hogy minden $\overline{a} \in \mathcal{D}_{\overline{F}}$-re: $p(S')(\overline{a}) \subseteq \overline{F}(\overline{a})$. Legyen $\overline{a} \in \mathcal{D}_{\overline{F}}$ tetszőleges. Az előzőek miatt $\overline{a} \in \mathcal{D}_p(S')$ is teljesül. Legyen $\overline{b} \in p(S')(\overline{a})$ tetszőleges. Ekkor $(\overline{a}, \overline{b}) \in p(S')$. Felhasználva a $p(S)$ és a $p(S')$ között a már említett összefüggést, adódik, hogy $\mathrm{pr}_{B'}(\overline{a}) = \mathrm{pr}_{B'}(\overline{b})$ és $(\mathrm{pr}_B(\overline{a}), \mathrm{pr}_B(\overline{b})) \in p(S)$.

Ha lenne olyan $\overline{\overline{b}} \in A$, amelyre $(\overline{a}, \overline{\overline{b}}) \in \overline{F}$ és $\mathrm{pr}_B(\overline{b}) = \mathrm{pr}_B(\overline{\overline{b}})$, akkor a bővített identitás feltétele miatt $(\overline{a}, \overline{b}) \in \overline{F}$ is teljesülne és akkor $\overline{b} \in \overline{F}(a)$ is igaz lenne.

$\overline{a} \in \mathcal{D}_{\overline{F}}$ feltevésből és abból, hogy $\mathrm{pr}_B(\overline{F}) = F$ következik, hogy $\mathrm{pr}_B(\overline{a}) \in \mathcal{D}_F$. Feltétel szerint S megoldja az F feladatot, ezért $\mathrm{pr}_B(\overline{a}) \in \mathcal{D}_F$ és $(\mathrm{pr}_B(\overline{a}), \mathrm{pr}_B(\overline{b})) \in p(S)$-ből következik, hogy $(\mathrm{pr}_B(\overline{a}), \mathrm{pr}_B(\overline{b})) \in F$. A $\mathrm{pr}_B(\overline{F}) = F$ feltétel miatt van olyan $(\overline{a}', \overline{b}') \in A \times A$, amelyre $(\overline{a}', \overline{b}') \in \overline{F}$ és $\mathrm{pr}_B(\overline{a}') = \mathrm{pr}_B(\overline{a})$, valamint $\mathrm{pr}_B(\overline{b}') = \mathrm{pr}_B(\overline{b})$. Az $\overline{F}$ feladat vetítéstartó tulajdonsága miatt $\mathrm{pr}_B(\overline{a}') = \mathrm{pr}_B(\overline{a})$-ből következik, hogy $\mathrm{pr}_B(\overline{F}(\overline{a}')) = \mathrm{pr}_B(\overline{F}(\overline{a}))$, viszont $\overline{b}' \in \overline{F}(\overline{a}')$ és ezért $\mathrm{pr}_B(\overline{b}') \in \mathrm{pr}_B(\overline{F}(\overline{a}'))$. Ebből viszont $\overline{F}$ vetítéstartás miatt következik, hogy van olyan $\overline{b}'' \in \overline{F}(\overline{a})$, amelyre $\mathrm{pr}_B(\overline{b}'') = \mathrm{pr}_B(\overline{b}') = \mathrm{pr}_B(\overline{b})$. $\overline{F}$ bővített identitás tulajdonsága miatt $(\overline{a}, \mathrm{pr}_B(\overline{b}'') \otimes \mathrm{pr}_{B'}(\overline{a})) \in \overline{F}$ is teljesül. $\mathrm{pr}_B(\overline{b}'') = \mathrm{pr}_B(\overline{b})$ felhasználásával kapjuk, hogy $(\overline{a}, \mathrm{pr}_B(\overline{b}) \otimes \mathrm{pr}_{B'}(\overline{a})) \in \overline{F}$. $\mathrm{pr}_{B'}(\overline{a}) = \mathrm{pr}_{B'}(\overline{b})$ figyelembevételével adódik, hogy $(\overline{a}, \mathrm{pr}_B(\overline{b}) \otimes \mathrm{pr}_{B'}(\overline{b})) \in \overline{F}$, azaz $(\overline{a}, \overline{b}) \in \overline{F}$. Mivel $\overline{b} \in p(S')(\overline{a})$ tetszőleges volt, beláttuk, hogy tetszőleges $\overline{a} \in \mathcal{D}_{\overline{F}}$-re: $p(S')(\overline{a}) \subseteq \overline{F}(\overline{a})$. Amit bizonyítani kellett.

5. Ha $\overline{S}$ megoldja $\overline{F}$-et és tetszőleges $\overline{a} \in \mathcal{D}_{p(\overline{S})}$-ra: ha $(\mathrm{pr}_B(\overline{a}) \in \mathcal{D}_F$ akkor $\overline{a} \in \mathcal{D}_{\overline{F}})$, akkor S megoldja F-et (a *visszavezetés általánosításának tétele*).

Bizonyítás

$\mathcal{D}_F \subseteq \mathcal{D}_{p(S)}$ bizonyítása pontosan úgy történik, mint a *a változó bevezetésének tétele* bizonyítása esetén. A $\mathrm{pr}_B(p(\overline{S}) = p(S)$ és $\mathrm{pr}_B(\overline{F}) = F$ feltételek teljesülnek, valamint $\overline{S}$ megoldja az $\overline{F}$ feladatot, és a *a változó bevezetésének tétele* bizonyításának megfelelő részében csak ezeket a tulajdonságokat használtuk ki.

Az állítás igazolásához be kell még látni, hogy minden $a \in \mathcal{D}_F$-re: $p(S)(a) \subseteq F(a)$. Legyen $a \in \mathcal{D}_F$ tetszőleges. Az előzőek miatt $a \in \mathcal{D}_p(S)$ is teljesül. Legyen $b \in p(S)(a)$ tetszőleges. $\mathrm{pr}_B(p(\overline{S})) = p(S)$ miatt van olyan $\overline{a}, \overline{b} \in A$, amelyekre $(\overline{a}, \overline{b}) \in p(\overline{S})$ és $\mathrm{pr}_B(\overline{a}) = a$, valamint $\mathrm{pr}_B(\overline{b}) = b$. Ebből következik, hogy $\overline{a} \in \mathcal{D}_{p(\overline{S})}$. Kihasználva az állításban szereplő feltételt, $\overline{a} \in \mathcal{D}_{p(\overline{S})}$ és $\mathrm{pr}_B(\overline{a}) = a \in \mathcal{D}_F$-ből adódik, hogy $\overline{a} \in \mathcal{D}_{\overline{F}}$. Mivel $\overline{S}$ megoldja az $\overline{F}$ feladatot, ezért $(\overline{a}, \overline{b}) \in \overline{F}$. A $\mathrm{pr}_B(\overline{F}) = F$ feltétel miatt $(\mathrm{pr}_B(\overline{a}), \mathrm{pr}_B(\overline{b})) \in F$ is teljesül, ahonnan $(a, b) \in F$ következik. Mivel $b \in p(S)(a)$ tetszőleges volt, beláttuk, hogy tetszőleges $a \in \mathcal{D}_F$-re: $p(S)(a) \subseteq F(a)$. Amit bizonyítani kellett.

3. A típus

Definíció

1. Legyen

T tetszőleges halmaz

$I_S : T \to \mathbb{L}$ *specifikációs invariáns*, $T_S = [I_S]$

$\mathbb{F} = \{F_1, \ldots, F_n\}$ feladatok halmaza:

$$\forall i \in [1, n] : F_i \subseteq A^{F_i} \times A^{F_i} \ \ (A^{F_i} = A_1^{F_i} \times \ldots \times A_{n_i}^{F_i}) \quad \exists j \in [1..n_i] : A_j^{F_i} = T$$

A $\mathcal{T}_S = (T, I_S, \mathbb{F})$ hármast *típusspecifikációnak* nevezzük.

2. Legyen

E tetszőleges halmaz, az elemi típusértékek halmaza

$\varrho \subseteq E^* \times H$ *reprezentációs függvény,*

$I : E^* \to \mathbb{L}$ *típusinvariáns*

$\mathbb{S} = \{S_1, \ldots, S_m\}$ programok halmaza:

$$\forall i \in [1, m] : S_i \subseteq A^{S_i} \times A^{S_i^{**}} \ \ (A^{S_i} = A_1^{S_i} \times \ldots \times A_{m_i}^{S_i}) \quad \exists j \in [1..m_i] : A_j^{S_i} = E^*$$

A $\mathcal{T} = (\varrho, I, \mathbb{S})$ hármast *típusnak* nevezzük.

3. A $\mathcal{T} = (\varrho, I, \mathbb{S})$ típus *megfelel* a $\mathcal{T}_S = (T, I_S, \mathbb{F})$ típusspecifikációnak, ha

1. $\varrho([I]) = T_S$
2. $\forall F \in \mathbb{F} : \exists S \in \mathbb{S} :$ S *a* $\varrho_{|[I]}$*-n keresztül megoldja* F-et.

4. $A^S = A_1^S \times \ldots \times A_m^S$, $S \subseteq A^S \times (A^S)^{**}$ program,
$A^F = A_1^F \times \ldots \times A_n^F$, $F \subseteq A^F \times A^F$ $(m, n \in \mathbb{N})$.
Legyen $A^{F'} = A_1^{F'} \times \ldots \times A_m^{F'}$, ahol

$$A_i^{F'} := \begin{cases} T_S & \text{ha } A_i^S = E^* \\ A_i^S & \text{ha } A_i^S \neq E^* \end{cases} \qquad (i = 1, \ldots, m)$$

$\gamma \subseteq A^S \times A^{F'}$, ahol $\gamma = (\gamma_1, \ldots, \gamma_m)$, $\gamma_i \subseteq A_i^S \times A_i^{F'}$,

$$\gamma_i = \begin{cases} \varrho_{|[I]} & \text{ha } A_i^S = E^* \\ \mathrm{id}_{A_i^S} & \text{ha } A_i^S \neq E^* \end{cases} \qquad (i = 1, \ldots, m),$$

$$(\gamma_1, \ldots, \gamma_m) = \{((a_1^S, a_2^S, \ldots, a_m^S), (a_1^{F'}, a_2^{F'}, \ldots, a_m^{F'})) \mid \forall i \in [1..m] : (a_i^S, a_i^{F'}) \in \gamma_i\}$$

$S \subseteq A^S \times (A^S)^{**}$ a *a* $\varrho_{|[I]}$*-n keresztül megoldja* $F \subseteq A^F \times A^F$-et, ha

1. A^F altere $A^{F'}$-nek
2. $\mathcal{D}_{F'} \subseteq \mathcal{D}_{\gamma \odot p(S) \odot \gamma^{(-1)}}$
3. $\forall a \in \mathcal{D}_{F'} :$ $\gamma \odot p(S) \odot \gamma^{(-1)}(a) \subseteq F'(a)$

ahol F' az F kiterjesztése $A^{F'}$-re.

4. Specifikáció

Definíció

1. Az $R \subseteq A \times \mathbb{L}$ *utófeltétel* $S \subseteq A \times A^{**}$ programra vonatkozó *leggyengébb előfeltételének* nevezzük azt az $\mathrm{lf}(S, R)$ állítást, amelyre $[\mathrm{lf}(S, R)] = \{a \in \mathcal{D}_{p(S)} \mid p(S)(a) \subseteq [R]\}$.

2. B az $F \subseteq A \times A$ feladat *paramétertere*, ha $\exists F_1 \subseteq A \times B :$ $\exists F_2 \subseteq B \times A$ $F = F_2 \circ F_1$.

Állítás

1. $[\mathrm{lf}(S,R)] = p(S)^{-1}([R])$
2. $\mathrm{lf}(S, \mathrm{hamis}) = \mathrm{hamis}$ (A *csoda kizárásának elve.*)
3. $\mathrm{lf}(S, P \wedge Q) = \mathrm{lf}(S,P) \wedge \mathrm{lf}(S,Q)$
4. $\mathrm{lf}(S, P \vee Q) \Leftarrow \mathrm{lf}(S,P) \vee \mathrm{lf}(S,Q)$
5. $\mathrm{lf}(S, \neg Q) \Rightarrow \neg \mathrm{lf}(S,Q)$
6. Ha $Q \Rightarrow R$, akkor $\mathrm{lf}(S,Q) \Rightarrow \mathrm{lf}(S,R)$ (*monotonitás*)
7. S megoldja F-et $\Leftrightarrow \forall a \in \mathcal{D}_F : \; a \in [\mathrm{lf}(S, P(F(a)))]$
8. S megoldja F-et $\Leftrightarrow \forall H \subseteq A : \; \exists a \in \mathcal{D}_F : \; F(a) = H$ esetén: $F^{-1}(H) = [\mathrm{lf}(S, P(H))]$
9. *A specifikáció tétele:*
   Legyen A állapottér, $F \subseteq A \times A$ feladat, valamint $S \subseteq A \times A^{**}$ program A-n. Legyen B az F paramétertere:

   $$F = F_2 \circ F_1, \quad \text{ahol} \quad F_1 \subseteq A \times B \quad \text{és} \quad F_2 \subseteq B \times A.$$

   Tetszőleges $b \in B$-re legyen Q_b és R_b állítások A-n, amelyekre

   $$[Q_b] = F_1^{(-1)}(b) \quad \text{és} \quad [R_b] = F_2(b).$$

   Ha $\forall b \in B : \; Q_b \Rightarrow \mathrm{lf}(S, R_b)$, akkor S megoldja F-et.

Bizonyítás

Legyen $a \in D_F$ tetszőleges. Ekkor létezik olyan $a' \in A$, amelyre $(a, a') \in F$. $F = F_2 \circ F_1$ miatt létezik olyan $b \in B$, amelyre $(a,b) \in F_1$ és $(b, a') \in F_2$. Legyenek Q_b és R_b állítások A-n, amelyekre $[Q_b] = F_1^{(-1)}(b)$ és $[R_b] = F_2(b)$. Ebből következik, hogy $\forall a \in [Q_b] : \; [R_b] \subseteq F_2 \circ F_1(a)$. De $F = F_2 \circ F_1$ miatt $\forall a \in [Q_b] : \; [R_b] \subseteq F(a)$ is teljesül. A feltétel szerint $Q_b \Rightarrow \mathrm{lf}(S, R_b)$, ezért $[Q_b] \subseteq D_{P(S)}$. De $(a,b) \in F_1$ miatt $a \in [Q_b]$, ezért $a \in D_{P(S)}$. $Q_b \Rightarrow \mathrm{lf}(S, R_b)$ és $a \in [Q_b]$-ből következik, hogy $P(S)(a) \subseteq [R_b] \subseteq F(a)$. Tehát $P(S)(a) \subseteq F(a)$ is teljesül tetszőleges $a \in D_F$-re.

10. A specifikáció tétele nem megfordítható, azaz megadható olyan A állapottér, valamint F feladat és S program az A-n, továbbá olyan B paramétertér az F feladathoz, hogy bár S megoldja az F feladatot, mégis létezik olyan $b \in B$, amelyre $Q_b \not\Rightarrow \mathrm{lf}(S, R_b)$.
    Megjegyzés: ha F_1 determinisztikus, akkor a specifikáció tétele megfordítható.

5. Elemi programok

Definíció

1. *Elem*inek nevezünk egy A állapottéren egy S programot, ha
   $\forall a \in A : \; S(a) \subseteq \{<a>, <a,a,a,\ldots>, <a,b> \; | \; b \neq a\}$.
2. *Ü*resnek nevezzük, és SKIP-pel jelöljük azt a programot, amire
   $\forall a \in A : \; \mathrm{SKIP}(a) = \{<a>\}$.

3. *Törlődés*nek nevezzük, és ABORT-tal jelöljük azt a programot, amire $\forall a \in A:\ \text{ABORT}(a) = \{< a, a, a, \ldots >\}$.
4. Legyen $A = A_1 \times \ldots \times A_n$, $F = (F_1, \ldots, F_n)$, ahol $F_i \subseteq A \times A_i$. Az S program *általános értékadás*, ha

$$S = \{(a, \text{red}(a,b)) \mid a, b \in A \wedge a \in \bigcap_{i=1}^{n} \mathcal{D}_{F_i} \wedge b \in F(a)\} \cup$$
$$\{(a, < a, a, \ldots >) \mid a \in A \wedge a \notin \bigcap_{i=1}^{n} \mathcal{D}_{F_i}\}$$

Megjegyzés:

$\mathcal{D}_F = \bigcap_{i=1}^{n} \mathcal{D}_{F_i}, \quad F(a) = F_1(a) \times F_2(a) \times \ldots \times F_n(a)$

a) Ha F nem determinisztikus, akkor az S programot *értékkiválasztásnak* nevezzük és $a :\in F(a)$-val jelöljük, különben az S programot *értékadásnak* nevezzük és $a := F(a)$-val jelöljük.

b) Ha $\mathcal{D}_F \subset A$, akkor S *parciális* (értékkiválasztás vagy értékadás), különben *teljes*.

c) Ha

$$\exists i \in [1,n] : F_i(a_1, .., a_i, .., a_n) \neq a_i \wedge$$
$$\forall j \in [1,n] : i \neq j \rightarrow F_j(a_1, \ldots, a_j, \ldots, a_n) = a_j$$

akkor S *egyszerű* (értékadás vagy értékkiválasztás), különben *szimultán*.

Állítás

1. A SKIP, az ABORT és az értékadás program.
2. $p(\text{SKIP}) = id_A$
3. $p(\text{ABORT}) = \emptyset$
4. $p(a :\in F(a)) = F$
5. $\text{lf}(\text{SKIP}, R) = R$
6. $\text{lf}(\text{ABORT}, R) = \text{hamis}$
7. Ha S az F reláció által meghatározott általános értékadás, akkor $\text{lf}(S, R) = P(\mathcal{D}_F) \wedge R \circ F$

6. Programkonstrukciók

Definíció

1. Legyenek $S_1, S_2 \subseteq A \times A^{**}$ programok. Az $S \subseteq A \times A^{**}$ relációt, amelyre tetszőleges $a \in A$-ra

$$
\begin{aligned}
S(a) =&\{\chi_2(\alpha,\beta) \in A^* \mid \alpha \in S_1(a) \wedge \alpha \in A^* \wedge \beta \in S_2(\tau(\alpha)) \wedge \beta \in A^*\} \cup \\
&\{\alpha \in A^\infty \mid \alpha \in S_1(a)\} \cup \\
&\{\chi_2(\alpha,\beta) \in A^\infty \mid \alpha \in S_1(a) \wedge \alpha \in A^* \wedge \beta \in S_2(\tau(\alpha)) \wedge \beta \in A^\infty\}
\end{aligned}
$$

az S_1 és S_2 *szekvenciájának* nevezzük, és $(S_1; S_2)$-vel jelöljük.

2. Legyenek $\pi_1, \ldots, \pi_n$ feltételek (állítások), valamint $S_1, \ldots, S_n$ programok A-n. Az $IF \subseteq A \times A^{**}$ relációt, amelyre tetszőleges $a \in A$-ra

$$IF(a) = \bigcup_{i=1}^{n} w_i(a) \ \cup w_0(a),$$

ahol

$$w_i(a) = \begin{cases} S_i(a) & \text{, ha } a \in [\pi_i] \\ \emptyset & \text{, különben} \end{cases}$$

$$w_0(a) = \begin{cases} < a, a, \ldots > & \text{, ha } a \notin \bigcup\limits_{i=1}^{n} [\pi_i] \\ \emptyset & \text{, különben} \end{cases}$$

az $S_1, S_2, ..., S_n$ programokból, valamint a $\pi_1, \pi_2, ..., \pi_n$ feltételekből képzett *elágazásnak* nevezzük és $(\pi_1 : S_1, \ldots, \pi_n : S_n)$-nel jelöljük.

3. Legyen π feltétel és S_0 program A-n. A $DO \subseteq A \times A^{**}$ relációt, amelyre tetszőleges $a \in A$-ra

$$
\begin{aligned}
&a \in [\pi] \text{ esetén}: \ DO(a) = \\
&\{\alpha \in A^* \mid \exists \alpha_1, \ldots, \alpha_n \in A^* : (\alpha = \chi_n(\alpha_1, \ldots, \alpha_n) \wedge \alpha_1 \in S_0(a) \wedge \\
&\forall i \in [1, n-1] : \ (\alpha_{i+1} \in S_0(\tau(\alpha_i)) \wedge \tau(\alpha_i) \in [\pi]) \wedge \\
&(\tau(\alpha_n) \notin [\pi]))\} \cup \\
&\{\alpha \in A^\infty \mid \exists \alpha_1, \ldots, \alpha_n \in A^{**} : (\alpha = \chi_n(\alpha_1, \ldots, \alpha_n) \wedge \alpha_1 \in S_0(a) \wedge \\
&\forall i \in [1, n-1] : \ (\alpha_i \in A^* \wedge \alpha_{i+1} \in S_0(\tau(\alpha_i)) \wedge \tau(\alpha_i) \in [\pi]) \wedge \\
&\alpha_n \in A^\infty)\} \cup \\
&\{\alpha \in A^\infty \mid \exists \alpha_1, \ldots, \alpha_k, \ldots \in A^* : \ (\alpha = \chi_\infty(\alpha_1, \ldots, \alpha_k, \ldots) \wedge \alpha_1 \in S_0(a) \wedge \\
&\forall i \in \mathbb{N} : \ (\alpha_{i+1} \in S_0(\tau(\alpha_i)) \wedge \tau(\alpha_i) \in [\pi]))\}
\end{aligned}
$$

és

$$a \notin [\pi] \text{ esetén}: \ DO(a) = \mathrm{SKIP}(a)$$

az S_0-ból és π-ből képezett *ciklusnak* nevezzük, és (π, S_0)-lal jelöljük.

Állítás

1. A szekvencia, az elágazás és a ciklus program.

Bizonyítás

Az állítás közvetlen következik az egyes relációk definíciójából.

2. $p((S_1;S_2)) = p(S_2) \odot p(S_1)$.

Bizonyítás

Legyen $(a,a') \in p((S_1;S_2))$. Ebből következik, hogy

$$\{\alpha \in A^\infty \mid \alpha \in S_1(a)\} \;=\; \emptyset$$

és

$$\{\chi_2(\alpha,\beta) \in A^\infty \mid \alpha \in S_1(a) \wedge \alpha \in A^* \wedge \beta \in S_2(\tau(\alpha)) \wedge \beta \in A^\infty\} \;=\; \emptyset,$$

hiszen ebben az esetben $(S_1;S_2)(a)$ csak véges sorozatokat tartalmaz. Ebből következik, hogy $a \in D_{p(S_1)}$ és $p(S_1)(a) \subseteq D_{p(S_2)}$. A programfüggvény defníciójából közvetlen következik, hogy létezik olyan $\overline{\alpha} \in (S_1;S_2)(a)$, hogy $a' = \tau(\overline{\alpha})$. Ezért

$$S(a) = \{\chi_2(\alpha,\beta) \in A^* \mid \alpha \in S_1(a) \wedge \alpha \in A^* \wedge \beta \in S_2(\tau(\alpha)) \wedge \beta \in A^*\}$$

miatt létezik olyan $\chi_2(\alpha,\beta) \in A^*$, ahol $\alpha \in S_1(a) \wedge \alpha \in A^* \wedge \beta \in S_2(\tau(\alpha)) \wedge \beta \in A^*$, hogy $a' = \tau(\chi_2(\alpha,\beta))$. Ekkor viszont $(a,\tau(\alpha)) \in p(S_1)$ és $(\tau(\alpha),\tau(\beta)) \in p(S_2)$.
De $\tau(\beta) \;=\; \tau(\chi_2(\alpha,\beta))$, ezért $(a,a') \in p(S_2) \odot p(S_1)$.

Legyen $(a,a') \in p(S_2) \odot p(S_1)$. Ekkor $a \in D_{p(S_1)}$ és $p(S_1)(a) \subseteq D_{p(S_2)}$. Ezért

$$\{\alpha \in A^\infty \mid \alpha \in S_1(a)\} \;=\; \emptyset$$

és

$$\{\chi_2(\alpha,\beta) \in A^\infty \mid \alpha \in S_1(a) \wedge \alpha \in A^* \wedge \beta \in S_2(\tau(\alpha)) \wedge \beta \in A^\infty\} \;=\; \emptyset,$$

Tehát $a \in D_{p((S_1;S_2))}$. $(a,a') \in p(S_2) \odot p(S_1)$ feltételből következik, hogy létezik olyan $b \in A$, amelyre $(a,b) \in p(S_1)$ és $(b,a') \in p(S_2)$. Tekintettel a $p(S_1)$ és $p(S_2)$ definíciójára, következik, hogy létezik olyan $\alpha \in S_1(a)$ és $\beta \in S_2(b)$, hogy $\tau(\alpha) \;=\; b$ és $\tau(\beta) \;=\; a'$. Ekkor viszont $\chi_2(\alpha,\beta) \in (S_1;S_2)(a)$. Ebből következik, hogy $(a,\tau(\chi_2(\alpha,\beta))) \in p((S_1;S_2))(a)$, de $\tau(\chi_2(\alpha,\beta)) \;=\; \tau(\beta) \;=\; a'$ miatt $(a,a') \in p((S_1;S_2))$.

3. $\mathcal{D}_{p(IF)} = \{a \in A \mid a \in \bigcup\limits_{i=1}^{n} [\pi_i] \wedge \forall i \in [1,n]:\; a \in [\pi_i] \rightarrow a \in \mathcal{D}_{p(S_i)}\}$

$\forall a \in \mathcal{D}_{p(IF)}:\; p(IF)(a) = \bigcup\limits_{i=1}^{n} pw_i(a)$, ahol

$$pw_i(a) = \begin{cases} p(S_i)(a) & \text{, ha } a \in [\pi_i] \\ \emptyset & \text{, különben} \end{cases}$$

Bizonyítás

A tétel állítása közvetlen következik a program, illetve a programfüggvény definíciójából.

4. $p(DO(\pi;S_0)) = \overline{p(S_0)|_\pi}$

Bizonyítás

$$p(DO(\pi;S_0))|_{A\setminus[\pi]} = \overline{p(S_0)|_\pi}|_{A\setminus[\pi]}$$

nyilván teljesül.

Legyen $(a,a') \in p(DO(\pi;S_0))|_{[\pi]}$.Ebből következik, hogy $a \in [\pi]$, valamint

$$\begin{aligned}&\{\alpha \in A^\infty \mid \exists \alpha_1,\ldots,\alpha_n \in A^{**} : (\alpha = \chi_n(\alpha_1,\ldots,\alpha_n) \wedge \alpha_1 \in S_0(a) \wedge \\ &\forall i \in [1,n-1] :\ (\alpha_i \in A^* \wedge \alpha_{i+1} \in S_0(\tau(\alpha_i)) \wedge \tau(\alpha_i) \in [\pi]) \wedge \\ &\alpha_n \in A^\infty)\} \ = \ \emptyset\end{aligned}$$

és

$$\begin{aligned}&\{\alpha \in A^\infty \mid \exists \alpha_1,\ldots,\alpha_k,\ldots \in A^* :\ \ (\alpha = \chi_\infty(\alpha_1,\ldots,\alpha_k,\ldots) \wedge \alpha_1 \in S_0(a) \wedge \\ &\forall i \in \mathbb{N} :\ (\alpha_i \in A^* \wedge \alpha_{i+1} \in S_0(\tau(\alpha_i)) \wedge \tau(\alpha_i) \in [\pi]))\} \ = \ \emptyset\end{aligned}$$

Legyen $< a_0, a_1, \ldots > \in A^\infty$, ahol $\forall i \in \mathbb{N}_0 :\ \ a_{i+1} \in p(S_0)|_\pi(a_i)$ az $p(S_0)|_\pi$ reláció a_0 kezdőpontú végtelen pontlánca, ahol $a_0 \in [\pi]$. Ha $\forall i \in \mathbb{N}_0 : a_{i+1} \in p(S_0)|_{[\pi]}(a_i)$, akkor legyen $\alpha_i \in S_0(a_{i-1})$, amelyre $\tau(\alpha_i) = a_i,\ i = 1, 2, \ldots$. Ekkor

$$\begin{aligned}&\chi_\infty(\alpha_1,\ldots,\alpha_k,\ldots) \in \\ &\{\alpha \in A^\infty \mid \exists \alpha_1,\ldots,\alpha_k,\ldots \in A^* :\ \ (\alpha = \chi_\infty(\alpha_1,\ldots,\alpha_k,\ldots) \wedge \alpha_1 \in S_0(a_0) \wedge \\ &\forall i \in \mathbb{N}_0 :\ (\alpha_i \in A^* \wedge \alpha_{i+1} \in S_0(\tau(\alpha_i)) \wedge \tau(\alpha_i) \in [\pi]))\}\end{aligned}$$

Ha $\forall i \in \mathbb{N}_0 : a_{i+1} \in p(S_0)|_{[\pi]}(a_i)$ nem teljesül, akkor van olyan $i \in \mathbb{N}_0$, amelyre $a_{i+1} \in p(S_0)|_\pi(a_i)$ úgy, $a_i \notin D_{p(S_0)|_{[\pi]}} \wedge a_i \in [\pi]$. Ekkor szükségképpen $a_{i+1} = a_i$ a $p(S_0)|_{[\pi]}$ definíciója miatt. Legyen i_0 az ilyen tulajdonságú indexek közül a legkisebb. Az i_0 választása miatt $\forall j \in [0..i_0-1] : a_j \in D_{p(S_0)} \wedge \pi[a_j]$, $a_{i_0} \notin D_p(S_0) \wedge \pi(a_{i_0})$. Legyen $\alpha_{i+1} \in S_0(a_i)$, amelyre $\tau(\alpha_{i+1}) = a_{i+1},\ i = 0, 1, \ldots, i_0 - 1$ és $\alpha_{i_0+1} \in S(a_i) \cap A^\infty$. Ekkor

$$\begin{aligned}&\chi_n(\alpha_1,\ldots,\alpha_{i_0},\alpha_{i_0+1}) \in \\ &\{\alpha \in A^\infty \mid \exists \alpha_1,\ldots,\alpha_n \in A^{**} : (\alpha = \chi_n(\alpha_1,\ldots,\alpha_n) \wedge \alpha_1 \in S_0(a) \wedge \\ &\forall i \in [1,n-1] :\ (\alpha_i \in A^* \wedge \alpha_{i+1} \in S_0(\tau(\alpha_i)) \wedge \tau(\alpha_i) \in [\pi]) \wedge \\ &\alpha_n \in A^\infty)\}.\end{aligned}$$

Tehát $(a,a') \in p(DO(\pi;S_0))|_{[\pi]}$-ból következik, hogy $a \in D_{\overline{p(S_0)|_\pi}}$.
$(a,a') \in p(DO(\pi;S_0))|_{[\pi]}$-ből következik, hogy létezik olyan

$$\begin{aligned}&\alpha_1,\ldots,\alpha_n \in A^* : (\alpha_1 \in S_0(a) \wedge a \in [\pi] \wedge \\ &\forall i \in [1,n-1] :\ (\alpha_i \in A^* \wedge \alpha_{i+1} \in S_0(\tau(\alpha_i)) \wedge \tau(\alpha_i) \in [\pi]) \wedge \\ &(\alpha_n \in A^* \wedge \tau(\alpha_n) \notin [\pi])) \wedge a' \ = \ \tau(\chi_n(\alpha_1,\ldots,\alpha_n).\end{aligned}$$

$(a,a') \in p(DO(\pi;S_0))|_{[\pi]}$-ből ugyanakkor az is következik, hogy

$$S_0(a) \subseteq A^* \text{ és } \forall i \in [1, n-1] : S_0(\tau(\alpha_i)) \subseteq A^*$$

is teljesül, mert ellenkező esetben a

$$\{\alpha \in A^\infty \mid \exists \alpha_1, \ldots, \alpha_n \in A^{**} : (\alpha = \chi_n(\alpha_1, \ldots, \alpha_n) \wedge \alpha_1 \in S_0(a) \wedge$$
$$\forall i \in [1, n-1] : \ (\alpha_i \in A^* \wedge \alpha_{i+1} \in S_0(\tau(\alpha_i)) \wedge \tau(\alpha_i) \in [\pi]) \wedge$$
$$\alpha_n \in A^\infty)\} \ = \ \emptyset$$

nem teljesül. Legyen $a_0 = a, \ \forall i \in [1, n] : a_i = \tau(\alpha_i)$. Ekkor az $< a_0, a_1, ..., a_n >$ sorozatra

$$\forall i \in [1, n-1] : (a_{i+1} \in p(S_0)(a_i) \wedge \pi(a_i)) \wedge \neg\pi(a_n).$$

Mivel $\tau(\chi_n(\alpha_1, \ldots, \alpha_n) = \tau(\alpha_n)$, ezért $(a, a') \in \overline{p(S_0)|_\pi}|_{[\pi]}$.

Legyen $(a, a') \in \overline{p(S_0)|_\pi}|_{[\pi]}$. Ekkor $a \in [\pi]$. Ha

$$\{\alpha \in A^\infty \mid \exists \alpha_1, \ldots, \alpha_n \in A^{**} : (\alpha = \chi_n(\alpha_1, \ldots, \alpha_n) \wedge \alpha_1 \in S_0(a) \wedge$$
$$\forall i \in [1, n-1] : \ (\alpha_i \in A^* \wedge \alpha_{i+1} \in S_0(\tau(\alpha_i)) \wedge \tau(\alpha_i) \in [\pi]) \wedge$$
$$\alpha_n \in A^\infty)\} \ \neq \ \emptyset,$$

akkor legyen

$$\alpha_1, \ldots, \alpha_n \in A^{**} : (\alpha_1 \in S_0(a) \wedge$$
$$\forall i \in [1, n-1] : \ (\alpha_i \in A^* \wedge \alpha_{i+1} \in S_0(\tau(\alpha_i)) \wedge \tau(\alpha_i) \in [\pi]) \wedge$$
$$\alpha_n \in A^\infty).$$

Könnyen látható, hogy $n = 1$ esetén $a \notin D_{p(S_0)}$, valamint $n > 1$ esetén $\tau(\alpha_{n-1}) \notin D_{p(S_0)} \wedge \tau(\alpha_{n-1}) \in [\pi]$. Ebből következik, hogy $L^\infty_{p(S_0)|_\pi}(a) \neq \emptyset$, ami ellentmondáshoz vezet.
Ha viszont

$$\{\alpha \in A^\infty \mid \exists \alpha_1, \ldots, \alpha_k, \ldots \in A^* : \ (\alpha = \chi_\infty(\alpha_1, \ldots, \alpha_k, \ldots) \wedge \alpha_1 \in S_0(a) \wedge$$
$$\forall i \in \mathbb{N} : \ (\alpha_i \in A^* \wedge \alpha_{i+1} \in S_0(\tau(\alpha_i)) \wedge \tau(\alpha_i) \in [\pi]))\} \ \neq \ \emptyset,$$

akkor létezik olyan

$$\alpha_1, \ldots, \alpha_k, \ldots \in A^* : \ (\alpha_1 \in S_0(a) \wedge$$
$$\forall i \in \mathbb{N} : \ (\alpha_i \in A^* \wedge \alpha_{i+1} \in S_0(\tau(\alpha_i)) \wedge \tau(\alpha_i) \in [\pi])).$$

Ha $a \in D_{p(S_0)} \wedge \forall i \in \mathbb{N} : \tau(\alpha_i) \in D_{p(S_0)}$, akkor Legyen $a_0 = a, a_1 = \tau(\alpha_1), a_2 = \tau(\alpha_2), \ldots, a_n = \tau(\alpha_n), \ldots$. Könnyen látható, hogy
$< a_0, a_1, \ldots, a_n, \ldots > \in L^\infty_{p(S_0)|_\pi}(a)$, ami ellentmond annak, hogy $(a, a') \in \overline{p(S_0)|_\pi}|_{[\pi]}$. Ha viszont $a \in D_{p(S_0)} \wedge \forall i \in \mathbb{N} : \tau(\alpha_i) \in D_{p(S_0)}$ nem teljesül, akkor vagy $a \notin D_{p(S_0)}$ vagy $\exists i \in \mathbb{N} : \tau(\alpha_i) \notin D_{p(S_0)}$. Mindkét esetben következik, hogy $L^\infty_{p(S_0)|_\pi}(a) \neq \emptyset$, ami szintén ellentmondáshoz vezet. Tehát $(a, a') \in \overline{p(S_0)|_\pi}|_{[\pi]}$-ból következik, hogy $a \in D_{p(DO(\pi;S_0))}$.
Ha $(a, a') \in \overline{p(S_0)|_\pi}|_{[\pi]}$, akkor létezik olyan

$$a_0 = a, a_1, \ldots, a_n : n \in \mathbb{N}_0 \wedge \forall i \in [1, n] : a_i \in p(S_0)|_\pi(a_{i-1}) \wedge a_n \notin D_{p(S_0)|_\pi} \wedge a' = a_n.$$

$a \in [\pi]$ miatt $n > 0$. Ekkor szükségképpen $\forall i \in [1,n] : a_{i-1} \in D(p(S_0)) \wedge \pi(a_{i-1})$, mivel ha lenne olyan
$i \in [1,n] : a_{i-1} \notin D(p(S_0)) \wedge \pi(a_{i-1})$, akkor a sorozat ezen i indextől
$a_{i-1}, a_{i-1}, \ldots, a_{i-1}, \ldots \in L^{\infty}_{p(S_0)|_\pi}(a_{i-1})$ sorozattal folytatható lenne, ebből viszont következne, hogy $L^{\infty}_{p(S_0)|_\pi}(a) \neq \emptyset$, ami ellentmondás. Tehát létezik olyan

$$a_0, a_1, \ldots, a_n : \forall i \in [1,n] : a_i \in p(S_0)(a_{i-1}) \wedge \pi(a_{i-1}) \wedge \neg\pi(a_n) \wedge a' = a_n.$$

Ekkor viszont létezik olyan

$$\begin{aligned}
&\alpha_1, \ldots, \alpha_n \in A^* : (\alpha_1 \in S_0(a) \wedge \\
&\forall i \in [1, n-1] : \ (\alpha_i \in A^* \wedge \alpha_{i+1} \in S_0(\tau(\alpha_i)) \wedge a_i = \tau(\alpha_i) \wedge \tau(\alpha_i) \in [\pi]) \wedge \\
&(\alpha_n \in A^* \wedge \tau(\alpha_n) \notin [\pi]) \wedge a_n = \tau(\alpha_n) \ ),
\end{aligned}$$

tehát $(a, \chi_n(\alpha_1, \ldots, \alpha_n))) \in p(DO(S_0, \pi))$.
$\tau(\chi_n(\alpha_1, \ldots, \alpha_n)) = \tau(\alpha_n) = a'$ miatt adódik, hogy $(a, a') = (a, \tau(\chi_n(\alpha_1, \ldots, \alpha_n)))$, tehát $(a, a') \in p(DO(S_0; \pi))|_{[\pi]}$ is teljesül.

5. Legyen $S = (S_1; S_2)$, és Q, R olyan állítások A-n, amelyekre $Q \Rightarrow \mathrm{lf}(S, R)$. Ekkor létezik olyan Q' állítás, amire $Q \Rightarrow \mathrm{lf}(S_1, Q')$ és $Q' \Rightarrow \mathrm{lf}(S_2, R)$.

Bizonyítás

Legyen

$$[Q'] = \bigcup_{a \in [Q]} p(S_1)(a).$$

Könnyen látható, hogy Q' kielegíti a tétel állítását.

6. Legyen $IF = (\pi_1 : S_1, \ldots, \pi_n : S_n)$, és Q, R olyan állítások A-n, amelyekre $Q \wedge \left(\bigvee_{i=1}^{n} \pi_i\right) \Rightarrow \mathrm{lf}(IF, R)$. Ekkor $\forall i \in [1,n] : \ Q \wedge \pi_i \Rightarrow \mathrm{lf}(S_i, R)$.

Bizonyítás

Legyen $a \in [Q \wedge \pi_i]$. Ekkor $a \in [Q \wedge (\bigvee_{j=1}^{n} \pi_j])$. Ebből következik, hogy $a \in D_{p(IF)}$, ezért $a \in [Q \wedge \pi_i]$ miatt $a \in D_{p(S_i)}$. $p(S_i)(a) \subseteq \bigcup_{j=1}^{n} pw_j(a) = IF(a)$ ahol,

$$pw_j(a) = \begin{cases} p(S_j)(a) & \text{, ha } a \in [\pi_j] \\ \emptyset & \text{, különben,} \end{cases}$$

mert $a \in [\pi_i]$ miatt $pw_i(a) = p(S_i)(a)$. Ezért $p(S_i)(a) \subseteq [R]$ is tejesül. Tehát tetszőleges i-re $Q \wedge \pi_i \Rightarrow \mathrm{lf}(S_i, R)$.

7. Legyen $DO = (\pi, S_0)$, és Q, R olyan állítások A-n, amelyekre $Q \Rightarrow \mathrm{lf}(DO, R)$, és tegyük fel, hogy $\forall a \in \mathcal{D}_{p(S_0)} \cap [\pi] : \ \exists k \in \mathbb{N} : \ p(S_0)^k(a) = \emptyset$. Ekkor létezik P állítás és $t : A \to \mathbb{Z}$ függvény, amelyekre

1. $Q \Rightarrow P$

2. $P \wedge \neg\pi \Rightarrow R$
3. $P \wedge \pi \Rightarrow t > 0$
4. $P \wedge \pi \Rightarrow \mathrm{lf}(S_0, P)$
5. $P \wedge \pi \wedge t = t' \Rightarrow \mathrm{lf}(S_0, t \leq t' - 1)$

Bizonyítás

Ismeretes, hogy $p(DO(\pi; S_0)) = \overline{p(S_0)|_\pi}$. A $\forall a \in \mathcal{D}_{p(S_0)} \cap [\pi] : \exists k \in \mathbb{N} : \; p(S_0)^k(a) = \emptyset$ feltételből következik, hogy A $\forall a \in \mathcal{D}_{\overline{p(S_0)|_\pi}} : \;\; \exists k \in \mathbb{N} : \;\; p(S_0)|_\pi{}^k(a) = \emptyset$, ugyanis ha $a \notin [\pi]$, akkor $k = 1$ már alkalmas választás. Legyen $a \in [\pi] \wedge a \in \mathcal{D}_{\overline{p(S_0)|_\pi}}$.
Ha $< a_0 = a, a_1, \ldots, a_n > \in L_{\overline{p(S_0)|_\pi}}(a)$, akkor $\forall i \in [0, n-1] : a \in [\pi]$. Ekkor viszont $\forall i \in [0, n-1] : a \in \mathcal{D}_{p(S_0)}$ is teljesül $L^\infty_{p(S_0)|_\pi} = \emptyset$ miatt. Ezért, ha $p(S_0)^k(a) = \emptyset$, akkor az $L_{\overline{p(S_0)|_\pi}}(a)$ minden lánca k-nál rövidebb, tehát $p(S_0)|_\pi{}^k(a) = \emptyset$. Legyen

$$t(a) = \begin{cases} \min\limits_{k \in \mathbb{N}} p(S_0)|_\pi{}^k(a) = \emptyset & \text{, ha } a \in \mathcal{D}_{\overline{p(S_0)|_\pi}} \\ 0 & \text{, különben} \end{cases}$$

és legyen P olyan állítás, amelyre $[P] = \bigcup\limits_{k=0}^{\infty} p(S_0)|_\pi{}^k[Q]$.

1. $Q \Rightarrow P$ nyilván teljesül.
2. $P \wedge \neg\pi \Rightarrow R$ teljesül, mert $Q \Rightarrow \mathrm{lf}(DO, R)$ és $P \wedge \neg\pi$ a Q-ból $p(S_0)|_\pi$-szerint kiinduló láncok végei.
3. $P \wedge \pi \Rightarrow t > 0$ teljesül, hiszen az ilyen pontokban az $p(S_0)|_\pi$-szerinti láncok nem érnek véget és ezért $Q \Rightarrow \mathrm{lf}(DO, R)$ miatt $[P \wedge \pi] \subseteq \mathcal{D}_{\overline{p(S_0)|_\pi}}$.
4. $P \wedge \pi \Rightarrow \mathrm{lf}(S_0, P)$ P definíciójából közvetlen következik.
5. $P \wedge \pi \wedge t = t' \Rightarrow \mathrm{lf}(S_0, t \leq t' - 1)$ teljesül, mert ha egy pontból indul ki $p(S_0)|_\pi$ szerint lánc és e láncok hosszának van felső határa, akkor ha valamely láncon egy lépést előre megyünk $p(S_0)|_\pi$ szerint, akkor az abból $p(S_0)|_\pi$ szerint kiinduló láncok hosszának felső határa eggyel biztosan csökken.

7. Levezetési szabályok

Állítás

1. *A szekvencia levezetési szabálya:*
Legyen $S = (S_1; S_2)$, és adott Q, R és Q' állítás A-n.
Ha $Q \Rightarrow \mathrm{lf}(S_1, Q')$ és $Q' \Rightarrow \mathrm{lf}(S_2, R)$ akkor $Q \Rightarrow \mathrm{lf}(S, R)$.

Bizonyítás

Legyen $a \in [Q]$. A feltétel szerint, $a \in D_{p(S_1)}$ és $p(S_1)(a) \subseteq [Q']$. $Q' \Rightarrow \mathrm{lf}(S_2, R)$ miatt $[Q'] \subseteq D_{p(S_2)}$. Tehát $p(S_1)(a) \subseteq D_{p(S_2)}$, ezért $a \in D_{p(S_2) \odot p(S_1)}$.

Legyen $b \in p(S_2) \odot p(S_1)(a)$. Ekkor van olyan a', amelyre $a' \in p(S_1)(a) \wedge b \in p(S_2)(a')$. Ebből adódik, hogy $a' \in [Q']$, ezért $b \in [R]$. Tehát $p(S_2) \odot p(S_1)(a) \subseteq [R]$. Mivel $a \in [Q]$ tetszőleges volt, adódik, hogy $Q \Rightarrow \mathrm{lf}(S, R)$.

2. *Az elágazás levezetési szabálya:*
Legyen $IF = (\pi_1 : S_1, \dots, \pi_n : S_n)$, és adott Q, R állítás A-n.
Ha $\forall i \in [1, n] :\ Q \wedge \pi_i \Rightarrow \mathrm{lf}(S_i, R)$, akkor $Q \wedge \left(\bigvee_{i=1}^{n} \pi_i\right) \Rightarrow \mathrm{lf}(IF, R)$.

Bizonyítás

Legyen $a \in [Q \wedge (\bigvee_{j=1}^{n} \pi_j)]$. Ha $a \in [\pi_i]$, akkor $a \in [Q \wedge \pi_i]$, amiből következik $a \in D_{p(S_i)}$ a feltételek miatt. Az i tetszőleges választása miatt következik, hogy ha $a \in [Q \wedge (\bigvee_{j=1}^{n} \pi_j)]$, akkor $a \in D_{p(IF)}$ is teljesül. Definíció szerint $\forall a \in \mathcal{D}_{p(IF)} :\ p(IF)(a) = \bigcup_{i=1}^{n} pw_i(a)$, ahol

$$pw_i(a) = \begin{cases} p(S_i)(a) & \text{, ha } a \in [\pi_i] \\ \emptyset & \text{, különben} \end{cases}$$

Ugyanakkor a feltételek miatt $pw_i(a) \subseteq [R]$, $i = 1, 2, \dots, n$, tehát $p(IF)(a) \subseteq [R]$ is teljesül. Mivel $a \in [Q \wedge (\bigvee_{j=1}^{n} \pi_j)]$ tetszőleges volt, adódik, hogy $Q \wedge \left(\bigvee_{i=1}^{n} \pi_i\right) \Rightarrow \mathrm{lf}(IF, R)$.

3. *A ciklus levezetési szabálya:*
Adott P, Q, R állítás A-n, $t : A \to \mathbb{Z}$ függvény és legyen $DO = (\pi, S_0)$. Ha

1. $Q \Rightarrow P$
2. $P \wedge \neg\pi \Rightarrow R$
3. $P \wedge \pi \Rightarrow t > 0$
4. $P \wedge \pi \Rightarrow \mathrm{lf}(S_0, P)$
5. $P \wedge \pi \wedge t = t' \Rightarrow \mathrm{lf}(S_0, t \leq t' - 1)$

akkor $Q \Rightarrow \mathrm{lf}(DO, R)$.

Bizonyítás

Ismeretes, hogy $p(DO(\pi; S_0)) = \overline{p(S_0)|_\pi}$. Legyen $a \in [P]$. Ha $a \notin [\pi]$, akkor 2. miatt $a \in [R]$. De $\overline{p(S_0)|_\pi}(a) = \{a\}$ $a \notin [\pi]$ miatt, ezért $\overline{p(S_0)|_\pi}(a) \subseteq [R]$.

Legyen $a \in [P]$ és $a \in [\pi]$. Ekkor $a \in D_{\overline{p(S_0)|_\pi}}$ és 3. miatt $t(a) > 0$.
Legyen $< a_0 = a, a_1, \dots, a_n, \dots > \in L^{\infty}_{\overline{p(S_0)|_\pi}}(a)$. $\forall i \in \mathbb{N}_0 : a_i \in [\pi]$ nyilván teljesül, mivel $D_{\overline{p(S_0)|_\pi}} = [\pi]$. A 4. feltétel miatt teljes indukcióval könnyen belátható, hogy

$$\forall i \in \mathbb{N}_0 : a_i \in [P]$$

is teljesül. Ugyanakkor 5. és 3. miatt

$$\forall i \in \mathbb{N}_0 : t(a_{i+1}) < t(a_i) \wedge t(a_i) > 0,$$

ami lehetetlen. Tehát $L^{\infty}_{\overline{p(S_0)|_\pi}}(a) = \emptyset$. Legyen $< a_0 = a, a_1, \ldots, a_n > \in L_{\overline{p(S_0)|_\pi}}(a)$. Ebből következik, hogy $\forall i \in [0, n-1] : a_i \in [\pi]$ és $a_n \notin [\pi]$. Hasonlóan az előzőekhez belátható, hogy $\forall i \in [0, n] : a_i \in [P]$, tehát adódott $a_n \in \overline{p(S_0)|_\pi}(a)$-ra, hogy $a_n \in [P] \wedge a_n \notin [\pi]$. Ebből 2. miatt következik, hogy $a_n \in [R]$. Mivel $< a_0 = a, a_1, \ldots, a_n > \in L_{\overline{p(S_0)|_\pi}}(a)$ tetszőleges volt, adódik, hogy $\overline{p(S_0)|_\pi}(a) \subseteq [R]$. Összegezve a kapott eredményeket, kapjuk, hogy $P \Rightarrow \mathrm{lf}(DO, R)$. Ugyanakkor az 1. feltétel miatt $Q \Rightarrow \mathrm{lf}(DO, R)$ is nyilván teljesül.

8. Típuskonstrukciók

Legyenek $T_0, T_1, \ldots, T_n$ típusértékhalmazok, $E_1, \ldots, E_n$ nem üres, véges vagy megszámlálható halmazok, $E = \bigcup_{i=1}^{n} E_i$, $\varrho_i \subset E^* \times T_i$ $(i = 1, \ldots, n)$ reprezentációs függvények, $\mathcal{T}_i = (\varrho_i, I_i, \mathcal{S}_i)(i = 0, \ldots, n)$ típusok.

Definíció

1. *Direktszorzat*
$\varrho = \psi_D \circ \varphi_D$, ahol $\psi_D \subset B \times T, B = T_1 \times \ldots \times T_n$,
$\varphi_D = \{(\varepsilon, b) \in E^* \times B \mid \exists \varepsilon_1, \ldots, \varepsilon_n \in E^* \ \forall i \in [1, n] : \ (\varepsilon_i, b_i) \in \varrho_i \wedge \varepsilon = \mathrm{kon}(\varepsilon_1, \ldots, \varepsilon_n)\}$
Jelölés: $\mathcal{T} = (\mathcal{T}_1, \ldots, \mathcal{T}_n)$.
Ha ψ_D kölcsönösen egyértelmű, akkor $\mathcal{T}$ rekord típus.

2. *Unió*
$\varrho = \psi_U \circ \varphi_U$, ahol $\psi_U \subset B \times T, B = T_1 \cup \ldots \cup T_n$,
$\varphi_U = \{(\varepsilon, b) \in E^* \times B \mid \exists i \in [1, n] : \ (\varepsilon, b) \in \varrho_i\}$
Jelölés: $\mathcal{T} = (\mathcal{T}_1; \ldots; \mathcal{T}_n)$.
Ha ψ_U kölcsönösen egyértelmű, akkor $\mathcal{T}$ egyesítés.

3. *Iterált*
$\varrho = \psi_I \circ \varphi_I$, ahol $\psi_I \subset T_0^* \times T$, $\varphi_I = \{(\varepsilon, \beta) \in E^* \times T_0^* \mid \exists \alpha \in (E^*)^* : \ |\alpha| = |\beta| \wedge \forall i \in [1, |\alpha|] : \ (\alpha_i, \beta_i) \in \varrho_0 \wedge \varepsilon = \mathrm{kon}(\alpha_1, \ldots, \alpha_{|\alpha|}\}$
Jelölés: $\mathcal{T} = it(\mathcal{T}_0)$.
Ha ψ_I kölcsönösen egyértelmű, akkor $\mathcal{T}$ sorozat típus.
Jelölés: $\mathcal{T} = seq(\mathcal{T}_0)$.
Ha $\mathcal{D}_{\psi_I} = T_0^*$ és $(\alpha, t), (\beta, t) \in \psi_I \Leftrightarrow \alpha \in \mathrm{perm}(\beta)$, akkor $\mathcal{T}$ kombináció típus.
Jelölés: $\mathcal{T} = com(\mathcal{T}_0)$.
Ha $\mathcal{D}_{\psi_I} = T_0^*$ és $(\alpha, t), (\beta, t) \in \psi_I \Leftrightarrow \bigcup_{i=1}^{|\alpha|} \{\alpha_i\} = \bigcup_{i=1}^{|\beta|} \{\beta_i\}$, akkor $\mathcal{T}$ halmaz típus.
Jelölés: $\mathcal{T} = set(\mathcal{T}_0)$.