ELTE PROG-MAT.
2000-2001

7.

Programkonstrukciók

Az előző fejezetben megismertünk bizonyos egyszerű programokat, a továbbiakban pedig bevezetünk néhány módszert, amellyel meglevő programjainkból új programokat készíthetünk. Természetesen sokféleképpen konstruálhatunk meglevő programjainkból új programokat, de mi csak háromféle konstrukciós műveletet fogunk megengedni: a szekvencia-, elágazás- és ciklusképzést. A *strukturált programozás alaptétele* [REF ??] kimondja, hogy ezzel a három konstrukciós művelettel minden programmal adható ekvivalens strukturált program, tehát ez a három konstrukciós művelet elegendő is.

7.1. Megengedett konstrukciók

Az első konstrukciós technika arra ad módot, hogy egy programot közvetlenül egy másik után végezzünk el. A definícióban használni fogjuk a következő jelölést: legyen $\alpha \in A^*$, $\beta \in A^{**}$. Ekkor

$$\chi_2(\alpha, \beta) = red(kon(\alpha, \beta)).$$

---

25. DEFINÍCIÓ: SZEKVENCIA

Legyenek $S_1, S_2 \subseteq A \times A^{**}$ programok. Az $S \subseteq A \times A^{**}$ relációt az S_1 és S_2 *szekvenciájának* nevezzük, és $(S_1; S_2)$-vel jelöljük, ha $\forall a \in A$:

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

Vegyük észre, hogy ha két olyan program szekvenciáját képezzük, amelyek értékkészlete csak véges sorozatokat tartalmaz, akkor a szekvencia is csak véges sorozatokat rendel az állapottér pontjaihoz.

Hasonlóan egyszerűen ellenőrizhető az is, hogy determinisztikus programok szekvenciája is determinisztikus reláció (függvény).

A programkonstrukciókat szerkezeti ábrákkal, úgynevezett **struktogramokkal** szoktuk ábrázolni.

Legyenek S_1, S_2 programok A-n. Ekkor az $S = (S_1; S_2)$ szekvencia struktogramja:

S
S_1
S_2

A második konstrukciós lehetőségünk az, hogy más-más meglevő programot hajtsunk végre bizonyos feltételektől függően.

26. DEFINÍCIÓ: ELÁGAZÁS

Legyenek $\pi_1, \dots, \pi_n : A \to \mathbb{L}$ feltételek, $S_1, \dots, S_n$ programok A-n. Ekkor az $IF \subseteq A \times A^{**}$ relációt az S_i-kből képzett π_i-k által meghatározott *elágazásnak* nevezzük és $(\pi_1 : S_1, \dots, \pi_n : S_n)$-nel jelöljük, ha $\forall a \in A$:

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

ahol $\forall i \in [1..n]$:

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

és

$$w_0(a) \quad = \quad \begin{cases} \langle a, a, a, \dots \rangle, & \text{ha } \forall i \in [1..n] : \neg\pi_i(a) \\ \emptyset, & \text{különben} \end{cases}$$

Ha a feltételek nem diszjunktak, akkor a determinisztikus programokból képzett elágazás lehet nem determinisztikus.

Ha csak olyan programokból képzünk elágazást, amik csak véges sorozatokat rendelnek az állapottér minden pontjához, az elágazás akkor is rendelhet (azonos elemekből álló) végtelen sorozatot, ha a feltételek igazsághalmazai nem fedik le az egész állapotteret.

Legyenek $S_1, S_2, \dots, S_n$ programok, $\pi_1, \pi_2, \dots, \pi_n$ feltételek A-n. Ekkor az $IF = (\pi_1 : S_1, \pi_2 : S_2, \dots, \pi_n : S_n)$ elágazás struktogramja:

IF			
\ π_1	\ π_2	\ $\dots$	\ π_n
S_1	S_2	$\dots$	S_n

A harmadik konstrukciós lehetőségünk az, hogy egy meglevő programot egy feltételtől függően valahányszor egymás után végrehajtsunk. A ciklus definálásához azonban szükségünk van további két jelölésre:

Legyenek $\alpha^1, \alpha^2, \dots, \alpha^{n-1} \in A^*$ és $\alpha^n \in A^{**}$. Ekkor

$$\chi_n(\alpha^1, \alpha^2, \dots, \alpha^n) = red(kon(\alpha^1, \alpha^2, \dots, \alpha^n)).$$

Legyenek $\alpha^i \in A^*$ $(i \in \mathbb{N})$. Ekkor

$$\chi_\infty(\alpha^1, \alpha^2, \dots) = red(kon(\alpha^1, \alpha^2, \dots)).$$

27. DEFINÍCIÓ: CIKLUS

Legyen π feltétel és S_0 program A-n. A $DO \subseteq A \times A^{**}$ relációt az S_0-ból a π feltétellel képzett *ciklusnak* nevezzük, és (π, S_0)-lal jelöljük, ha

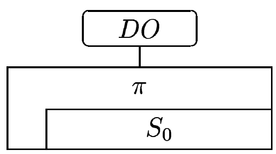
- $\forall a \notin \lceil \pi \rceil$:
$$DO(a) = \{\langle a \rangle\}$$
- $\forall a \in \lceil \pi \rceil$:

$$\begin{aligned}
DO(a) \;=\; & \{\alpha \in A^{**} \mid \exists \alpha^1, \dots, \alpha^n \in A^{**} : \alpha = \chi_n(\alpha^1, \dots, \alpha^n) \wedge \\
& \alpha^1 \in S_0(a) \wedge \forall i \in [1..n-1] :\ \alpha^i \in A^* \wedge \\
& \alpha^{i+1} \in S_0(\tau(\alpha^i)) \wedge \pi(\tau(\alpha^i))) \wedge (\alpha^n \in A^\infty \vee \\
& (\alpha^n \in A^* \wedge \neg\pi(\tau(\alpha^n))))\} \;\cup \\
\cup \;\; & \{\alpha \in A^\infty \mid \forall i \in \mathbb{N} : \exists \alpha^i \in A^* : \alpha = \chi_\infty(\alpha^1, \alpha^2, \dots) \wedge \\
& \alpha^1 \in S_0(a) \ \wedge \forall i \in \mathbb{N} :\ \alpha^i \in A^* \wedge \alpha^{i+1} \in S_0(\tau(\alpha^i)) \wedge \\
& \pi(\tau(\alpha^i))\}.
\end{aligned}$$

Vegyük észre, hogy a determinisztikus programból képzett ciklus is determinisztikus lesz.

Ezzel ellentétben, ha egy csak véges sorozatokat rendelő programot foglalunk ciklusba, akkor a ciklus értékkészlete még tartalmazhat végtelen sorozatot (ha soha nem jutunk ki a feltétel igazsághalmazából).

Legyen S_0 program, π feltétel A-n. Ekkor a $DO = (\pi, S_0)$ ciklus struktogramja:



A fentiekben leírt konstrukciókat programokra lehet alkalmazni. De vajon programokat hoznak-e létre? Az alábbi tétel kimondja, hogy az előzőkben definiált három konstrukciós művelet meglevő programokból valóban programokat hoz létre.

7. TÉTEL: A SZEKVENCIA, AZ ELÁGAZÁS ÉS A CIKLUS PROGRAM.

Legyen A tetszőleges állapottér, $S_0, S_1, S_2, \dots, S_n \subseteq A \times A^{**}$ programok, valamint $\pi, \pi_1, \pi_2, \dots, \pi_n : A \to \mathbb{L}$ feltételek A-n. Ekkor

1. $S = (S_1; S_2)$,
2. $IF = (\pi_1 : S_1, \pi_2 : S_2, \dots, \pi_n : S_n)$,
3. $DO = (\pi, S_0)$

programok A-n.

Bizonyítás: Mindhárom konstrukció definíciójában explicit szerepel, hogy reláció $A \times A^{**}$-on, és $\mathcal{D}_S = A$, azaz teljesül a program definíciójának első pontja. A továbbiakban esetekre bontva megvizsgáljuk a másik két kritérium teljesülését.

1. Legyen $a \in A$ tetszőleges, és $\alpha \in S(a)$. Ekkor két eset lehetséges:
   - Ha $\alpha \in S_1(a)$ és ebben az esetben $\alpha_1 = a$ és $\alpha = red(\alpha)$ triviálisan teljesül, hiszen S_1 program.
   - Ha $\alpha = \chi_2(\alpha^1, \alpha^2)$ úgy, hogy $\alpha^1 \in S_1(a)$ és $\alpha^2 \in S_2(\tau(\alpha^1))$. Ekkor a χ_2 definíciója miatt α redukált. Másrészt $\alpha_1 = \alpha_1^1$, tehát $\alpha_1 = a$.
2. Legyen $a \in A$ tetszőleges, és $\alpha \in IF(a)$. Ekkor
   $$\alpha \in \bigcup_{i=0}^{n} w_i(a).$$
   - Tegyük fel, hogy $\alpha \in w_0(a)$. Ekkor $\alpha = \langle a, a, \ldots \rangle$, tehát teljesíti a program definíciójának kritériumait.
   - Tegyük fel, hogy $\exists i \in [1..n] : \alpha \in w_i(a)$. Ekkor $\alpha \in S_i(a)$, így mivel S_i program, α teljesíti a definícióban megkívánt tulajdonságokat.
3. Legyen $a \in A$ tetszőleges, és $\alpha \in DO(a)$.
   - Tegyük fel, hogy $\neg\pi(a)$. Ekkor $\alpha = \langle a \rangle$, így az előírt tulajdonságok triviálisan teljesülnek.
   - Tegyük fel, hogy $\pi(a)$. Ekkor három eset lehetséges:
     (a) $\alpha \in A^*$:
     Ekkor $\exists n \in \mathbb{N} : \alpha = \chi_n(\alpha^1, \ldots, \alpha^n)$, így – χ_n definíciója miatt – α redukált. Másrészt felhasználva, hogy $\alpha^1 \in S_0(a)$ és $\alpha_1 = \alpha_1^1$, $\alpha_1 = a$ is teljesül.
     (b) $\exists n \in \mathbb{N} : \alpha = \chi_n(\alpha^1, \ldots, \alpha^n) \wedge \forall i \in [1..n-1] : \alpha^i \in A^* \wedge \alpha_n \in A^\infty$: Ekkor a kritériumok teljesülése az előző ponttal analóg módon ellenőrizhető.
     (c) $\alpha = \chi_\infty(\alpha^1, \alpha^2, \ldots)$:
     Ekkor α a χ_∞ definíciója alapján redukált sorozat, és $\alpha_1 = \alpha_1^1 = a$ is teljesül.

□

7.2. A programkonstrukciók programfüggvénye

Miután beláttuk, hogy meglevő programokból a programkonstrukciók segítségével új programokat készíthetünk, vizsgáljuk meg, hogy milyen kapcsolat van a konstruált programok programfüggvénye és az eredeti programok programfüggvénye között.

A szekvencia a legegyszerűbb programkonstrukció, ennek megfelelően a programfüggvénye is egyszerűen felírható a két komponensprogram programfüggvényének segítségével. Mivel a szekvencia két program egymás utáni elvégzését jelenti, várható, hogy a programfüggvénye a két komponensprogram programfüggvényének kompozíciója. Azonban mint látni fogjuk kompozíció helyett szigorú kompozíciót kell alkalmazni.

8. TÉTEL: A SZEKVENCIA PROGRAMFÜGGVÉNYE

Legyen A tetszőleges állapottér, S_1, S_2 programok A-n, $S = (S_1; S_2)$. Ekkor

$$p(S) = p(S_2) \odot p(S_1).$$

Bizonyítás: Legyen $a \in A$ tetszőleges. Ekkor

$$\begin{gathered} a \in \mathcal{D}_{p(S)} \iff S(a) \subseteq A^* \iff \\ S_1(a) \subseteq A^* \wedge \forall \alpha \in S_1(a) : S_2(\tau(\alpha)) \subseteq A^* \iff \\ a \in \mathcal{D}_{p(S_1)} \wedge p(S_1)(a) \subseteq \mathcal{D}_{p(S_2)} \iff \\ a \in \mathcal{D}_{p(S_2) \odot p(S_1)} \end{gathered}$$

tehát:

$$\mathcal{D}_{p(S)} = \mathcal{D}_{p(S_2) \odot p(S_1)}.$$

Legyen $a \in \mathcal{D}_{p(S)}$. Ekkor

$$\begin{gathered} (a, a') \in p(S_2) \odot p(S_1) \iff \\ \exists b \in A : (a, b) \in p(S_1) \wedge (b, a') \in p(S_2) \iff \\ \exists \alpha \in S_1(a), \beta \in S_2(b) : \tau(\alpha) = b \wedge \tau(\beta) = a' \iff \\ (a, a') \in p(S). \end{gathered}$$

□

Vegyük észre, hogy a nem szigorú kompozíció értelmezési tartományában olyan pont is lehet, amelyhez a szekvencia rendel végtelen sorozatot is. Nézzünk erre egy egyszerű példát: Legyen $A = \{1, 2\}$,

$$\begin{aligned} S_1 &= \{(1, \langle 1 \rangle), (1, \langle 1, 2 \rangle), (2, \langle 2 \rangle)\}, \\ S_2 &= \{(1, \langle 1, 2 \rangle), (2, \langle 2, 2, \dots \rangle)\}. \end{aligned}$$

Ekkor $1 \in \mathcal{D}_{p(S_2) \circ p(S_1)}$, de $\langle 1, 2, 2, 2, \dots \rangle \in S(1)$.

Mivel az elágazást több programból képezzük, a programfüggvényét is csak kissé körülményesebben tudjuk megfogalmazni. Hiszen az, hogy egy ponthoz az elágazás rendel-e végtelen sorozatot attól is függ, hogy mely feltételek igazak az adott pontban. Sőt, ha egy pontban egyetlen feltétel sem igaz, akkor a komponensprogramok programfüggvényétől függetlenül abban a pontban az elágazás programfüggvénye nem lesz értelmezve. Az elágazás programfüggvényének formális megfogalmazását adja meg a következő tétel.

9. TÉTEL: AZ ELÁGAZÁS PROGRAMFÜGGVÉNYE

Legyen A tetszőleges állapottér, $S_1, S_2, \dots, S_n \subseteq A \times A^{**}$ programok, valamint $\pi_1, \pi_2, \dots, \pi_n : A \to \mathbb{L}$ feltételek A-n, $IF = (\pi_1 : S_1, \dots, \pi_n : S_n)$. Ekkor

- $\mathcal{D}_{p(IF)} = \{a \in A \mid \bigvee_{i=1}^{n} \pi_i(a) \wedge \forall i \in [1, n] : \ \pi_i(a) \Rightarrow a \in \mathcal{D}_{p(S_i)}\}$
- $\forall a \in \mathcal{D}_{p(IF)}$:

$$p(IF)(a) = \bigcup_{i=1}^{n} pw_i(a),$$

ahol

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

Bizonyítás: Legyen $a \in A$ tetszőleges. Ekkor

$$\begin{gathered} a \in \mathcal{D}_{p(IF)} \iff IF(a) \subseteq A^* \iff \\ \exists i \in [1..n] : \pi_i(a) \wedge \bigcup_{i=1}^{n} w_i(a) \subseteq A^* \iff \\ \exists i \in [1..n] : \pi_i(a) \wedge \forall i \in [1..n] : \pi_i(a) \Rightarrow a \in \mathcal{D}_{p(S_i)}. \end{gathered}$$

Legyen továbbá $a \in \mathcal{D}_{p(IF)}$. Ekkor

$$p(IF)(a) = \tau\left(\bigcup_{i=1}^{n} w_i(a)\right) = \bigcup_{i=1}^{n} pw_i(a).$$

□

Természetesen, ha az elágazás-feltételek lefedik az egész állapotteret, akkor az a feltétel, hogy valamelyik π_i-nek igaznak kell lennie, triviálisan teljesül.

10. TÉTEL: A CIKLUS PROGRAMFÜGGVÉNYE

Legyen A tetszőleges állapottér, S program, π feltétel A-n, $DO = (\pi, S)$. Ekkor

$$p(DO) = \overline{p(S)|_\pi}.$$

Bizonyítás: Legyen $a \in A$ tetszőleges. Ekkor

$$a \in \mathcal{D}_{p(DO)} \iff DO(a) \subseteq A^*$$
$$\Updownarrow$$
$$DO(a) = \begin{cases} \{\langle a \rangle\}, & \text{ha } \neg\pi(a) \\ \{\alpha \in A^* \mid \exists n \in \mathbb{N} : \alpha = \chi_n(\alpha^1, \dots, \alpha^n) \land & \\ \quad \alpha^1 \in S(a) \land \forall i \in [1..n-1] : & \\ \quad \alpha^{i+1} \in S(\tau(\alpha^i)) \land \pi(\tau(\alpha^i)) \land & \\ \quad \neg\pi(\tau(\alpha^n))\}, & \text{ha } \pi(a) \end{cases}$$
$$\Updownarrow$$
$$\neg\pi(a) \lor (\nexists \beta \in A^\infty : \beta_1 = a \land \forall i \in \mathbb{N} : \beta_{i+1} \in p(S)(\beta_i) \land \pi(\beta_i))$$
$$\Updownarrow$$
$$a \in \mathcal{D}_{\overline{p(S)|_\pi}}$$

tehát $\mathcal{D}_{p(DO)} = \mathcal{D}_{\overline{p(S)|_\pi}}$. Másrészt legyen $a \in \mathcal{D}_{p(DO)}$. Ekkor

- Ha $\neg\pi(a)$ akkor
$$p(DO)(a) = a = \overline{p(S)|_\pi}(a).$$
- Ha $\pi(a)$ akkor $p(DO)(a) =$

$$\begin{aligned} &= \tau(\{\alpha \in A^* \mid \exists n \in \mathbb{N} : \alpha = \chi_n(\alpha^1, \dots, \alpha^n) \land \alpha^1 \in S(a) \land \\ &\qquad \forall i \in [1..n-1] : \alpha^{i+1} \in S(\tau(\alpha^i)) \land \pi(\tau(\alpha^i)) \land \neg\pi(\tau(\alpha^n))\}) = \\ &= \tau(\{\beta \in A^* \mid \beta_1 = a \land \forall i \in [1..|\beta|-1] : \beta_{i+1} \in p(S)(\beta_i) \land \\ &\qquad \pi(\beta_i) \land \neg\pi(\tau(\beta))\}) = \\ &= \{b \in A \mid \exists k \in \mathbb{N} : b \in (p(S)|_\pi)^k(a) \land \neg\pi(b)\} \\ &= \overline{p(S)|_\pi}(a). \end{aligned}$$

□

7.3. Levezetési szabályok

Ebben az alfejezetben megvizsgáljuk a programkonstrukciók és a specifikáció kapcsolatát.

Először azt fogjuk megvizsgálni, hogy a szekvencia adott utófeltételhez tartozó leggyengébb előfeltétele milyen kapcsolatban van az őt alkotó programok leggyengébb előfeltételével.

11. TÉTEL: A SZEKVENCIA LEVEZETÉSI SZABÁLYA
Legyen $S = (S_1; S_2)$, és adott Q, R és Q' állítás A-n. Ha

(1) $Q \Rightarrow lf(S_1, Q')$ és

(2) $Q' \Rightarrow lf(S_2, R)$

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

Bizonyítás: Legyen $q \in \lceil Q \rceil$. Ekkor (1) miatt $q \in \mathcal{D}_{p(S_1)}$ és $p(S_1)(q) \subseteq \lceil Q' \rceil$. Mivel (2) miatt $\lceil Q' \rceil \subseteq \mathcal{D}_{p(S_2)}$: $q \in \mathcal{D}_{p(S_2) \odot p(S_1)} = \mathcal{D}_{p(S)}$.
Továbbá (2) miatt $p(S_2)\big(p(S_1)(q)\big) \subseteq \lceil R \rceil$, tehát $q \in lf(S, R)$.
□

A szekvencia levezetési szabálya és a specifikáció tétele alapján a következőt mondhatjuk: ha S_1 és S_2 olyan programok, amelyekre a paramétertér minden b pontjában $Q_b \Rightarrow lf(S_1, Q'_b)$ és $Q'_b \Rightarrow lf(S_2, R_b)$ teljesül, akkor $(S_1; S_2)$ megoldja a Q_b, R_b párokkal adott feladatot.

12. TÉTEL: A SZEKVENCIA LEVEZETÉSI SZABÁLYÁNAK MEGFORDÍTÁSA
Legyen $S = (S_1; S_2)$, és Q, R olyan állítások A-n, amelyekre $Q \Rightarrow lf(S, R)$. Ekkor $\exists Q' : A \to \mathbb{L}$ állítás, amire

(1) $Q \Rightarrow lf(S_1, Q')$ és

(2) $Q' \Rightarrow lf(S_2, R)$.

Bizonyítás: Legyen $Q' = lf(S_2, R)$. Ekkor (2) automatikusan teljesül. Csak (1) fennállását kell belátnunk. Ehhez indirekt feltesszük, hogy

$$\exists q \in \lceil Q \rceil : q \notin \lceil lf(S_1, lf(S_2, R)) \rceil.$$

Ez kétféleképpen fordulhat elő:

- $q \notin \mathcal{D}_{p(S_1)}$, de ez ellentmond annak a feltételnek, mely szerint $\lceil Q \rceil \subseteq \mathcal{D}_{p(S)} \subseteq \mathcal{D}_{p(S_1)}$.
- $p(S_1)(q) \nsubseteq \lceil lf(S_2, R) \rceil$. Ekkor legyen $r \in p(S_1)(q) \setminus \lceil lf(S_2, R)$. Ekkor két eset lehetséges:
  - $r \notin \mathcal{D}_{p(S_2)}$. Ez ellentmond annak, hogy $q \in \mathcal{D}_{p(S_2) \odot p(S_1)}$.
  - $p(S_2)(r) \nsubseteq \lceil R \rceil$: Legyen $s \in p(S_2)(r) \setminus \lceil R \rceil$. Ekkor $s \in p(S)(q)$ és $s \notin \lceil R \rceil$, és ez ellentmond a $p(S)(q) \subseteq \lceil R \rceil$ feltételnek.

□

Vizsgáljuk meg, mi a kapcsolat az elágazás és az őt alkotó programok adott utófeltételhez tartozó leggyengébb előfeltétele között.

13. TÉTEL: AZ ELÁGAZÁS LEVEZETÉSI SZABÁLYA
Legyen $IF = (\pi_1 : S_1, \ldots, \pi_n : S_n)$, és adott Q, R állítás A-n. Ha

(1) $Q \Rightarrow \left(\bigvee_{i=1}^{n} \pi_i \right)$ és

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

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

Bizonyítás: Legyen $q \in \lceil Q \rceil$, ekkor (1) miatt valamelyik feltétel igaz q-ra, azaz $\exists i \in [1..n] : \pi_i(q)$ és (2) miatt

$$\forall j \in [1..n] : q \in \pi_j \Rightarrow q \in \lceil lf(S_j, R) \rceil \Rightarrow q \in \mathcal{D}_{p(S_j)}$$

vagyis $q \in \mathcal{D}_{p(IF)}$.

Másrészt mivel $\forall j \in [1..n] : \pi_j(q) \Rightarrow p(S_j)(q) \subseteq \lceil R \rceil$:

$$p(IF)(q) = \bigcup_{\substack{j \in [1..n] \\ \pi_j(q)}} p(S_j)(q) \subseteq \lceil R \rceil,$$

azaz $q \in \lceil lf(IF, R) \rceil$.

$\square$

Felhasználva a specifikáció tételét és az elágazás levezetési szabályát azt mondhatjuk: Legyen adott az F feladat specifikációja (A, B, Q, R). Ekkor ha minden $b \in B$ paraméterre és minden S_i programra $Q_b \wedge \pi_i \Rightarrow lf(S_i, R_b)$, és minden b paraméterhez van olyan π_i feltétel, amelyre $Q_b \Rightarrow \pi_i$, akkor az elágazás megoldja a Q_b, R_b párokkal specifikált feladatot.

Hasonlóan a szekvencia levezetési szabályához az elágazás levezetési szabálya is megfordítható, tehát ha egy elágazás megold egy specifikált feladatot, akkor le is lehet vezetni.

14. TÉTEL: AZ ELÁGAZÁS LEVEZETÉSI SZABÁLYÁNAK MEGFORDÍTÁSA

Legyen $IF = (\pi_1 : S_1, \ldots, \pi_n : S_n)$, és Q, R olyan állítások A-n, amelyekre

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

Ekkor

(1) $Q \Rightarrow \left(\bigvee_{i=1}^{n} \pi_i \right)$ és

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

Bizonyítás: Tetszőleges $q \in \lceil Q \rceil$ esetén, mivel $\lceil Q \rceil \subseteq \mathcal{D}_{p(IF)}$ létezik $i \in [1..n] : q \in \lceil \pi_i \rceil$ ezért $q \in \lceil \bigvee_{i=1} \pi_i \rceil$ azaz (1) teljesül és ha $q \in \mathcal{D}_{p(IF)}$ és $q \in \lceil \pi_i \rceil$ akkor $q \in \mathcal{D}_{p(S_i)}$ és $p(S_i)(q) \subseteq p(IF)(q) \subseteq R$, tehát (2) is teljesül.

$\square$

Az előző két konstrukcióhoz hasonlóan most megvizsgáljuk, hogy milyen kapcsolat van a ciklus és a ciklusmag leggyengébb előfeltétele között.

15. TÉTEL: 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) $P \wedge \pi \Rightarrow lf(S_0, P)$

(5) $P \wedge \pi \wedge t = t_0 \Rightarrow lf(S_0, t < t_0)$

akkor

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

Jelölje a továbbiakban g a ciklusmag programfüggvényének a ciklusfeltételre vonatkozó leszűkítését, azaz $g = p(S_0)|_{\lceil \pi \rceil}$. Mielőtt magát a levezetési szabályt bizonyítanánk, ennek a g relációnak látjuk be két tulajdonságát:
1. állítás: Legyen $q \in \lceil P \wedge \pi \rceil$. Ekkor

$$\forall k \in \mathbb{N}_0 : g^k(q) \subseteq \lceil P \rceil.$$

Bizonyítás: k szerinti teljes indukcióval:

- $k = 0$: $g^0(q) = q \in \lceil P \rceil$
- Tegyük fel, hogy $g^k(q) \subseteq \lceil P \rceil$. Legyen $r \in g^k(q)$ tetszőleges. Ekkor két eset lehetséges:
  - $r \in \lceil P \wedge \neg\pi \rceil$. Ekkor $g(r) = r \in \lceil P \rceil$.
  - $r \in \lceil P \wedge \pi \rceil$. Ekkor (4) miatt $r \in \mathcal{D}_{p(S_0)} \wedge g(r) = p(S_0)(r) \subseteq \lceil P \rceil$.

  Tehát: $g^{k+1}(q) \subseteq \lceil P \rceil$.

□
2. állítás: Legyen $q \in \lceil P \wedge \pi \rceil$. Ekkor

$$\exists n \leq t(q) : g^n(q) \subseteq \lceil \neg\pi \rceil.$$

Bizonyítás: Indirekt: tegyük fel, hogy $\forall n \in \mathbb{N} : g^n(q) \subseteq \lceil \pi \rceil$. Tekintsünk egy tetszőleges $b \in p(S_0)(q)$ pontot. Ekkor $t(b) < t(q)$, ugyanis (5)-ben t_0 helyére $t(q)$-t írva: $t(b) < t(q)$ teljesül. Ekkor viszont

$$\max_{b \in g^{t(q)+1}(q)} t(b) < \max_{b \in g^{t(q)}(q)} t(b) < \cdots < \max_{b \in g(q)} t(b) < t(q),$$

azaz

$$\max_{b \in g^{t(q)+1}(q)} t(b) < 0.$$

Ez viszont ellentmond (3)-nak.
□
Bizonyítás: *(Ciklus levezetési szabálya)* Legyen $q \in \lceil Q \rceil$ tetszőleges. Mivel (1) miatt $\lceil Q \rceil \subseteq \lceil P \rceil$, ezért $q \in \lceil P \wedge \neg\pi \rceil$ vagy $q \in \lceil P \wedge \pi \rceil$ teljesül.

- Tegyük fel, hogy $q \in \lceil P \wedge \neg\pi \rceil$. Ekkor a ciklus definíciója alapján $p(DO)(q) = \{q\}$, másrészt (2) miatt $q \in \lceil R \rceil$, tehát $q \in \lceil lf(DO, R) \rceil$.
- Tekintsük most azt az esetet, amikor $q \in \lceil P \wedge \pi \rceil$ teljesül. Ekkor a 2. állítás alapján

  $$\exists n \in \mathbb{N}_0 : (p(S_0)|_\pi)^n(q) = \emptyset,$$

  azaz

  $$q \in \mathcal{D}_{p(DO)}.$$

Ekkor a feltételre vonatkozó lezárt definíciója alapján:

$$p(DO)(q) \subseteq \lceil \neg\pi \rceil .$$

Másrészt az 1. állítás miatt

$$p(DO)(q) \subseteq \lceil P \rceil ,$$

és ekkor (2) miatt

$$p(DO)(q) \subseteq \lceil P \wedge \neg\pi \rceil \subseteq \lceil R \rceil ,$$

tehát

$$q \in \lceil lf(DO, R) \rceil .$$

□

A levezetési szabályban szereplő P állítást a ciklus invariáns tulajdonságának, a t függvényt terminálófüggvénynek nevezzük. A P invarianciáját az (1) és (4) feltételek biztosítják: garantálják, hogy az invariáns tulajdonság a ciklusmag minden lefutása előtt és után teljesül. A terminálófüggvény a ciklus befejeződését biztosítja: az (5) pont alapján a ciklusmag minden lefutása legalább eggyel csökkenti a terminálófüggvényt, másrészt a (3) miatt a terminálófüggvénynek pozitívnak kell lennie. A (2) feltétel garantálja, hogy ha a ciklus befejeződik, akkor az utófeltétel igazsághalmazába jut.

A ciklus levezetési szabályának és a specifikáció tételének felhasználásával elégséges feltételt adhatunk a megoldásra: ha adott a feladat specifikációja (A, B, Q, R), és találunk olyan invariáns állítást és terminálófüggvényt, hogy a paramétertér minden elemére teljesül a ciklus levezetési szabályának öt feltétele, akkor a ciklus megoldja a (Q_b, R_b) párokkal definiált feladatot.

A ciklus levezetési szabálya visszafelé nem igaz, azaz van olyan ciklus, amit nem lehet levezetni. Ennek az az oka, hogy egy levezetett ciklus programfüggvénye mindig korlátos lezárt, hiszen az állapottér minden pontjában a terminálófüggvény értéke korlátozza a ciklusmag lefutásainak számát.

Az is könnyen látható, hogy ha a ciklus programfüggvénye nem korlátos lezárt, akkor nem tudunk a ciklushoz terminálófüggvényt adni. Ám ha egy ciklus programfüggvénye megegyezik a ciklusmag ciklusfeltételre vonatkozó korlátos lezártjával, akkor a ciklus levezethető.

16. TÉTEL: A CIKLUS LEVEZETÉSI SZABÁLYÁNAK MEGFORDÍTÁSA

Legyen $DO = (\pi, S_0)$, és Q, R olyan állítások A-n, amelyekre $Q \Rightarrow lf(DO, R)$, és tegyük fel, hogy $p(DO) = \overline{\overline{p(S_0)}}|_\pi$. 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) $P \wedge \pi \Rightarrow lf(S_0, P)$

(5) $P \wedge \pi \wedge t = t_0 \Rightarrow lf(S_0, t < t_0)$

Bizonyítás: Legyen $P = lf(DO, R)$ és válasszuk t-t úgy, hogy $\forall a \in A$:

$$t(a) = \begin{cases} 0, & \text{ha } a \notin \mathcal{D}_{p(DO)} \cap \lceil \pi \rceil \\ max\{i \in \mathbb{N} \mid p(S_0)^i(a) \cap \lceil \pi \rceil \neq \emptyset\}, & \text{ha } a \in \mathcal{D}_{p(DO)} \cap \lceil \pi \rceil \end{cases}$$

Ekkor

(1) $Q \Rightarrow lf(DO, R)$ triviálisan teljesül.

(2) Legyen $a \in \lceil P \wedge \neg\pi \rceil$. Ekkor mivel $a \in \lceil lf(DO, R) \rceil$, $p(DO)(a) \subseteq \lceil R \rceil$. Másrészt mivel $a \in \lceil \neg\pi \rceil$, $p(DO)(a) = a$. Tehát $a \in \lceil R \rceil$, azaz $\lceil P \wedge \neg\pi \rceil \subseteq \lceil R \rceil$.

(3) t definíciója miatt nyilvánvaló.

(4) Felhasználva a lezárt azon egyszerű tulajdonságát, hogy

$$a \in \mathcal{D}_{\overline{R}} \Longrightarrow R(a) \subseteq \mathcal{D}_{\overline{R}}$$

a következő eredményt kapjuk: Legyen $a \in \lceil lf(DO, R) \wedge \pi \rceil$. Ekkor

$$a \in \mathcal{D}_{p(S_0)}, \quad \text{és} \quad p(S_0)(a) \subseteq \lceil lf(DO, R) \rceil,$$

tehát

$$a \in lf(S_0, P).$$

(5) A t definíciójából leolvasható, hogy a ciklusmag egyszeri végrehajtása csökkenti a terminálófüggvény értékét:

Legyen $a \in \lceil P \wedge \pi \rceil$, $t_0 = t(a)$, $b \in p(S_0)(a)$. Ekkor ha

$$t(a) = max\{i \in \mathbb{N} \mid p(S_0)^i(a) \cap \lceil \pi \rceil \neq \emptyset\}$$

akkor

$$t(b) < t(a)$$

azaz

$$t(b) < t_0.$$

□

Azt, hogy a lezárt és a korlátos lezárt megegyezik, a t definíciójában használtuk ki: ez a feltétel garantálja, hogy a definícióban szereplő maximum véges.