6. előadás

Programozás-elmélet

Definíció

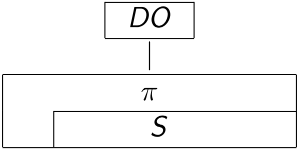
Legyen π feltétel és S program A-n. A $DO \subseteq A \times A^{**}$ relációt az S-ből a π feltétellel képezett ciklusnak nevezzük, és (π, S)-sel jelöljük, ha

1. $\forall a \notin [\pi] : \; DO(a) = \{\langle a \rangle\}$,
2. $\forall a \in [\pi] :$

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

1. Determinisztikus programból képezett ciklus is determinisztikus.
2. A ciklus értékkészlete tartalmazhat végtelen sorozatot akkor is, ha az S program csak véges sorozatokat generál (soha nem jutunk ki a π feltétel igazsághalmazából).

A $DO = (\pi, S)$ ciklus struktogramja:



Tétel

A szekvencia, az elágazás és a ciklus program.

Bizonyítás

Mindhárom program $A \times A^{**}$ tipusú reláció és mindhárom esetben $D_S = A$. A másik két tulajdonság igazolása a következő:
1. Szekvencia: $a \in A$, $\alpha \in S(a)$. Ha $\alpha \in S_1(a)$, akkor S_1 program volta miatt $\alpha_1 = a$ és $\alpha = red(\alpha)$. Ha $\alpha = \chi_2(\alpha^1, \alpha^2)$, ahol $\alpha^1 \in S_1(a)$ és $\alpha^2 \in S_2(\tau(\alpha^1))$, akkor χ_2 definíciója miatt α redukált és $\alpha_1 = \alpha_1^1 = a$.

Bizonyítás

2. Elágazás: $a \in A$, $\alpha \in IF(a)$. Ekkor

$$\alpha \in \cup_{i=0}^{m} w_i(a).$$

Ha $\alpha \in w_0(a)$, akkor $\alpha = \langle a, a, \ldots \rangle$ kielégíti a két kritériumot. Ha $\exists i \in [1..m] : \alpha \in w_i(a)$, akkor $\alpha \in S_i(a)$ és mivel S_i program, $\alpha_1 = a$ és $\alpha = red(\alpha)$.
3. Ciklus: $a \in A$, $\alpha \in DO(a)$. Ha $a \notin [\pi]$, akkor $\alpha = \langle a \rangle$, ami teljesíti a program követelményeit. Ha $a \in [\pi]$, akkor két eset lehetséges:
(a) Ha $\alpha \in A^{**}$ és $\exists n \in \mathbb{N} : \alpha = \chi_n(\alpha^1, \alpha^2, \ldots, \alpha^n)$, $\alpha^1 \in S(a)$, akkor χ_n definiciója miatt α redukált és $\alpha_1 = \alpha_1^1 = a$.
(b) Ha $\alpha \in A^{\infty}$ és $\alpha = \chi_{\infty}(\alpha^1, \alpha^2, \ldots)$, $\alpha^1 \in S(a)$, akkor χ_n definíciója miatt α redukált és $\alpha_1 = \alpha_1^1 = a$.

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.

Tétel

Legyen A állapottér, S_1, S_2 programok A-n, $S = (S_1; S_2)$ a belőlük képezett szekvencia. Ekkor

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

Bizonyítás

Emlékeztetünk arra, hogy a programfüggvény definíciója:

$$p(S) = \{(a, b) \mid S(a) \subseteq A^* \land \exists \alpha \in S(a) : \tau(\alpha) = b\} .$$

Esetünkben (feltéve, hogy minden sorozat véges):

$$\begin{gathered}
(a, a') \in p(S_2) \circ p(S_1) \iff \\
\exists b \in A : (a, b) \in p(S_1) \land (b, a') \in p(S_2) \iff \\
\exists \alpha \in S_1(a) : \tau(\alpha) = b \land \exists \beta \in S_2(b) : \tau(\beta) = a' \iff \\
\chi_2(\alpha, \beta) \in S(a) \land \tau(\chi_2(\alpha, \beta)) = a' \Leftrightarrow \\
(a, a') \in p(S) .
\end{gathered}$$

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.

Tétel

Legyen A állapottér, $S_1, S_2, \ldots, S_m$ programok A-n, valamint $\pi_1, \pi_2, \ldots, \pi_m : A \to \mathbb{L}$ feltételek A-n, $IF = (\pi_1 : S_1, \ldots, \pi_m : S_m)$. Ekkor

1. $D_{p(IF)} =$
$\left\{ a \in A \mid a \in \cup_{i=1}^{m} [\pi_i] \land \forall j \in [1..m] : a \in [\pi_j] \Rightarrow a \in D_{p(S_j)} \right\}$
2. $\forall a \in D_{p(IF)}$:
$$p(IF)(a) = \cup_{i=1}^{m} pw_i(a),$$
ahol
$$pw_i(a) = \begin{cases} p(S_i)(a), & \text{ha } a \in [\pi_i] \\ \emptyset, & \text{különben} \end{cases}$$

Bizonyítás

$$a \in D_{p(IF)} \iff IF(a) \subseteq A^* \iff$$
$$\exists i \in [1..m] : a \in [\pi_i] \wedge \cup_{i=1}^{m} w_i(a) \subseteq A^* \iff$$
$$\exists i : a \in [\pi_i] \wedge \forall j \in [1..m] : a \in [\pi_j] \Rightarrow a \in D_{p(S_j)}.$$

Legyen $a \in D_{p(IF)}$. Ekkor

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

Ha az elágazásfeltételek lefedik az egész állapotteret, akkor mindig van olyan π_i állítás, amelyik igaz.

Definíció

A $p(S)$ reláció megszorítása a $[\pi]$ igazsághalmazra:

$$p(S)_{|[\pi]} = p(S) \cap ([\pi] \times A) .$$

Tétel

Legyen A tetszőleges állapottér, $S \subseteq A \times A^{**}$ program, π feltétel A-n, $DO = (\pi, S)$. Ekkor $D_{p(DO)} = [\neg\pi] \cup D^{*}_{p(S)_{|[\pi]}}$ és

$$p(DO)(a) = \overline{p(S)_{|[\pi]}}(a) \quad \left(a \in D_{p(DO)}\right) .$$

Ebben a részben 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.
Egy S program R utófeltételhez tartozó leggyengébb előfeltételének neveztük azt az $lf(S, R)$ állítást, amelyre

$$[lf(S, R)] = \{a \in D_{p(S)} \mid p(S)(a) \subseteq [R]\}.$$

Tétel (A szekvencia levezetési szabálya)

Legyen $S = (S_1; S_2)$ szekvencia, Q, R és Q' állítások 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 $q \in [Q]$. Ekkor (1) miatt $q \in D_{p(S_1)}$ és $p(S_1)(q) \subseteq [Q']$. A (2) feltétel miatt $[Q'] \subseteq D_{p(S_2)}$ és $\forall q' \in Q' : p(S_2)(q') \subseteq [R]$. Ezért $p(S_2) \circ p(S_1)(q) \subseteq [R]$, azaz $q \in [\mathit{lf}\,(S, R)]$.

Következmény

A szekvencia levezetési szabálya és a specifikáció tétele alapján a következőt mondhatjuk: ha S_1 és S_2 olyan programok, amelyekre a paramétertér minden pontjában $Q_b \Rightarrow \mathit{lf}\left(S_1, Q'_b\right)$ és $Q'_b \Rightarrow \mathit{lf}\,(S_2, R_b)$ teljesül, akkor $(S_1; S_2)$ megoldja a Q_b, R_b párokkal megadott feladatokat.

Tétel (A szekvencia levezetési szabályának megfordítása)

Legyen $S = (S_1; S_2)$ szekvencia, Q és R olyan állítások A-n, amelyekre $Q \Rightarrow lf(S, R)$. Ekkor $\exists Q' : A \to \mathbb{L}$ állítás, hogy

1. $Q \Rightarrow lf(S_1, Q')$ és
2. $Q' \Rightarrow lf(S_2, R)$.

Bizonyítás

Legyen $Q' = \mathit{If}\,(S_2, R)$. Ekkor (2) teljesül. Tfh. (1) nem teljesül. Ekkor $\exists q \in [Q] : q \notin [\mathit{If}\,(S_1, \mathit{If}\,(S_2, R))]$. Két eset lehetséges:

(a) $q \notin D_{p(S_1)}$, ami ellentmondás a $[Q] \subseteq D_{p(S)} \subseteq D_{p(S_1)}$ feltétellel;

(b) $p\,(S_1)\,(q) \nsubseteq [\mathit{If}\,(S_2, R)]$. Legyen $r \in p\,(S_1)\,(q) \setminus [\mathit{If}\,(S_2, R)]$. Két eset lehetséges:
- $r \notin D_{p(S_2)}$, ami ellentmond a $q \in D_{p(S_2) \circ p(S_1)}$ feltételnek.
- $p\,(S_2)\,(r) \nsubseteq [R]$: Legyen $s \in p\,(S_2)\,(r) \setminus [R]$. Ekkor $s \in p\,(S)\,(q)$ és $s \notin [R]$, ami ellentmond a $p\,(S)\,(q) \subseteq [R]$ feltételnek.

Tétel (Az elágazás levezetési szabálya)

Legyen $IF = (\pi_1 : S_1, \ldots, \pi_m : S_m)$ elágazás, Q és R állítások A-n.
Ha $\forall i \in [1..m] : Q \wedge \pi_i \Rightarrow lf(S_i, R)$, akkor

$$Q \wedge (\vee_{i=1}^{m} \pi_i) \Rightarrow lf(IF, R).$$

Bizonyítás

Legyen $q \in [Q]$ és tfh. $\exists i \in [1..m] : q \in [\pi_i]$. Ekkor $q \in D_{p(IF)}$, ui.

$$\forall j \in [1..m] : q \in [\pi_j] \Rightarrow lf(S_j, R) \Rightarrow q \in D_{p(S_j)}.$$

Mivel $\forall j \in [1..m] : q \in [\pi_j] \Rightarrow p(S_j)(q) \subseteq [R]$, azért

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

Tehát $q \in [lf(IF, R)]$.

Következmény

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

Tétel (Az elágazás levezetési szabályának megfordítása)

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

$$Q \wedge (\vee_{i=1}^{m} \pi_i) \Rightarrow lf\,(IF, R)\,.$$

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

Bizonyítás

Indirekt: tfh. $\exists i \in [1..m] : [Q \wedge \pi_i] \not\subseteq [\mathit{lf}(S_i, R)]$. Legyen $q \in [Q \wedge \pi_i] \setminus [\mathit{lf}(S_i, R)]$. Két eset lehetséges:

- $q \notin D_{p(S_i)}$, ami ellentmond a $q \in D_{p(IF)}$ feltevésnek.
- $p(S_i)(q) \not\subseteq [R]$. Ekkor $p(S_i)(q) \subseteq p(IF)(q) \subseteq [R]$ miatt ellentmondás.

A ciklus levezetési szabálya bonyolultabb. A cél:

$$DO \text{ véges lépésben termináljon.}$$

Olyan P feltételt keresünk, amely:

1. Igaz a ciklus/iteráció megkezdése előtt;
2. Igaz az iteráció alatt;
3. Igaz az iteráció befejezése után.

A ciklus befejezésekor $\urcorner\pi$, tehát $P \wedge \urcorner\pi$ igaz. Ha $P \wedge \urcorner\pi \Rightarrow R$, akkor a ciklus helyességét igazoltuk. A P feltétel elnevezése: *invariáns feltétel/tulajdonság*.

Bevezetünk továbbá egy $t : A \to \mathbb{Z}$ egész értékű függvényt, amely

1. A program változóitól függ;
2. Korlátot ad a szükséges iterációk számára;
3. Minden végrehajtott iteráció legalább 1-el csökkenti t értékét;
4. t alulról korlátos: $t > 0$ terminálás előtt.

A t függvény elnevezése: *korlátozó/termináló függvény*. A korlátozó függvény biztosítja, hogy a ciklusnak terminálnia kell.

Tétel (A ciklus levezetési szabálya)

Legyen P állítás A-n, $DO = (\pi, S)$ és $t : A \to \mathbb{Z}$. Ha

1. $P \wedge \pi \Rightarrow t > 0$,
2. $P \wedge \pi \Rightarrow lf\,(S, P)$,
3. $P \wedge \pi \wedge \forall t = t_0 \Rightarrow lf\,(S, t < t_0)$,

akkor $P \Rightarrow lf\,(DO, P \wedge \urcorner\pi)$.

Következmény

A ciklus levezetési szabályának és a specifikáció tételének felhasználásával elégséges feltételt adhatunk a megoldásra: ha adott az$F$ 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.