4. előadás

Programozás-elmélet

Definíciók:

- Logikai értékek halmaza: $\mathbb{L} = \{igaz, hamis\} = \{i, h\}$.
- Az A halmazon értelmezett (logikai) állítás egy $Q : A \to \mathbb{L}$ függvény.
- Legyen Q az A halmazon értelmezett állítás. A Q állítás igazsághalmaza:

$$[Q] = \{a \in A \mid Q(a) = igaz\}.$$

- Legyenek Q_1 és Q_2 az A halmazon értelmezett állítások. A Q_1 és Q_2 állítások ekvivalensek, ha $[Q_1] = [Q_2]$. Jelölés: $Q_1 \equiv Q_2$.
- Legyen $R \subseteq A$ tetszőleges részhalmaz. $P(R)$ olyan állítást jelöl, amelyre $[P(R)] = R$.

Következmény:

Tetszőleges Q állításra igaz, hogy $Q \equiv P([Q])$.

Definíció

Legyenek P és Q az A halmazon értelmezett állítások. A következő logikai műveleteket definiáljuk, un. igazságtáblával:

1. $P \wedge Q$ (konjunkció / és / logikai szorzás):

P	i	i	h	h
Q	i	h	i	h
$P \wedge Q$	i	h	h	h

   A $P \wedge Q$ állítás igaz $\Longleftrightarrow$ P és Q is igaz;

2. $P \vee Q$ (diszjunkció / vagy / logikai összeadás):

P	i	i	h	h
Q	i	h	i	h
$P \vee Q$	i	i	i	h

   A $P \vee Q$ állítás igaz $\Longleftrightarrow$ P és Q közül legalább az egyik igaz;

Definíció

Legyenek P és Q az A halmazon értelmezett állítások. A következő logikai műveleteket definiáljuk, un. igazságtáblával:

3 $\neg Q$ (negáció / tagadás):

Q	i	h
$\neg Q$	h	i

A $\neg Q$ állítás igaz $\iff$ Q hamis, az állítás hamis $\iff$ Q igaz;

4 $P \Rightarrow Q$ (implikáció / következés / ha P, akkor Q):

P	i	i	h	h
Q	i	h	i	h
$P \Rightarrow Q$	i	h	i	i

A $P \Rightarrow Q$ állítás hamis$\iff$ P igaz és Q hamis.

Állítás

Legyenek P és Q az A halmazon értelmezett állítások. Ekkor

(i) $[P \wedge Q] = [P] \cap [Q]$;

(ii) $[P \vee Q] = [P] \cup [Q]$;

(iii) $[\neg Q] = A \setminus [Q]$

(iv) Ha $P \Rightarrow Q$, akkor $[P] \subseteq [Q]$.

A megoldás definíciója közvetlenül elég nehézkesen használható a programok készítése során, hiszen az, hogy egy program megold-e egy feladatot az a megoldás eddigi definíciója alapján csak nehezen ellenőrizhető. Ezért bevezetünk néhány új fogalmat, majd ezek segítségével egy elégséges feltételt adunk a megoldásra.
A megoldás definíciójának közvetlen ellenőrzése helyett elégséges feltételt adunk meg a program helyességének ellenőrzésére. Ezt az eredményt a specifikáció tételének nevezzük. A tétel megfogalmazásához két fogalmat vezetünk be:

1. Leggyengébb előfeltétel
2. Paramétertér

Először a program futásának adjuk meg egy a programfüggvénynél kényelmesebben használható jellemzését.

Definíció

Legyen $S \subseteq A \times A^{**}$ program, R az A állapottéren értelmezett állítás. Az S program R utófeltételhez tartozó leggyengébb előfeltétele az $lf\,(S, R)$ állítás, amelyre

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

A leggyengébb előfeltétel tehát pontosan azokban a pontokban igaz, ahonnét kiindulva az S program biztosan terminál, és az összes lehetséges végállapotra igaz R.
Természetesen a leggyengébb előfeltétel igazsághalmazán kívül is lehetnek olyan pontok, amelyből a program egy futása eljut az utófeltétel igazsághalmazába, csak azokból a pontokból nem garantált, hogy oda jut.
Egy program működése úgy is jellemzhető, hogy megadjuk a program tetszőleges utófeltételhez tartozó leggyengébb előfeltételét.
A feladat megoldása során az a célunk, hogy olyan programot találjunk, amelyik bizonyos feltételeknek eleget tevő pontokban terminál. Ezért azt mondhatjuk, hogy ha a számunkra kedvező végállapotokra megadjuk a program leggyengébb előfeltételét, akkor a programfüggvény meghatározása nélkül jellemezzük a program működését.

A most következő tétel a leggyengébb előfeltétel néhány fontos tulajdonságát mondja ki.

Tétel (Dijkstra)

Legyen $S \subseteq A \times A^{**}$ program, R és Q az A halmazon értelmezett állítások, és *HAMIS* az azonosan hamis állítás. Ekkor

1. $lf\,(S, HAMIS) = HAMIS$,
2. Ha $Q \Rightarrow R$, akkor $lf\,(S, Q) \Rightarrow lf\,(S, R)$,
3. $lf\,(S, Q) \wedge lf\,(S, R) = lf\,(S, Q \wedge R)$,
4. $lf\,(S, Q) \vee lf\,(S, R) \Rightarrow lf\,(S, Q \vee R)$

Az első tulajdonságot a csoda kizárása elvének, a másodikat monotonitási tulajdonságnak nevezzük.

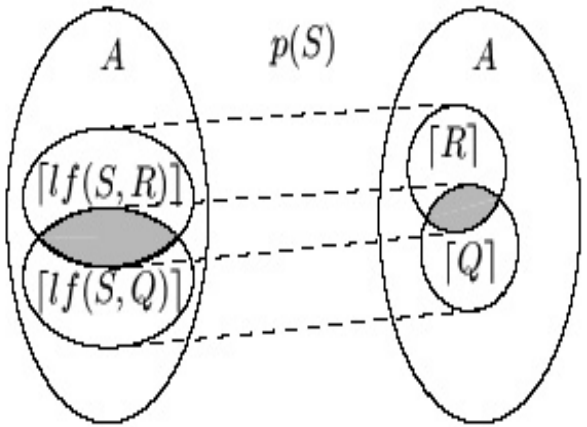
Bizonyítás

1. Indirekt tegyük fel, hogy létezik $a \in [\mathit{If}\,(S, \mathit{HAMIS})]$. Ekkor definíció szerint $a \in D_{p(S)}$ és $p\,(S)\,(a) \subseteq [\mathit{HAMIS}] = \emptyset$. Ez pedig ellentmondás.
2. Tegyük fel, hogy $a \in [\mathit{If}\,(S, Q)]$. Ekkor $p\,(S)\,(a) \subseteq [Q]$. Mivel $[Q] \subseteq [R]$, ezért $p\,(S)\,(a) \subseteq [R]$ és $a \in [\mathit{If}\,(S, R)]$.
3. $$\begin{aligned} [\mathit{If}\,(S, Q)] &= \left\{a \in D_{p(S)} \mid p\,(S)\,(a) \subseteq [Q]\right\} \\ [\mathit{If}\,(S, R)] &= \left\{a \in D_{p(S)} \mid p\,(S)\,(a) \subseteq [R]\right\} \end{aligned}$$

   miatt

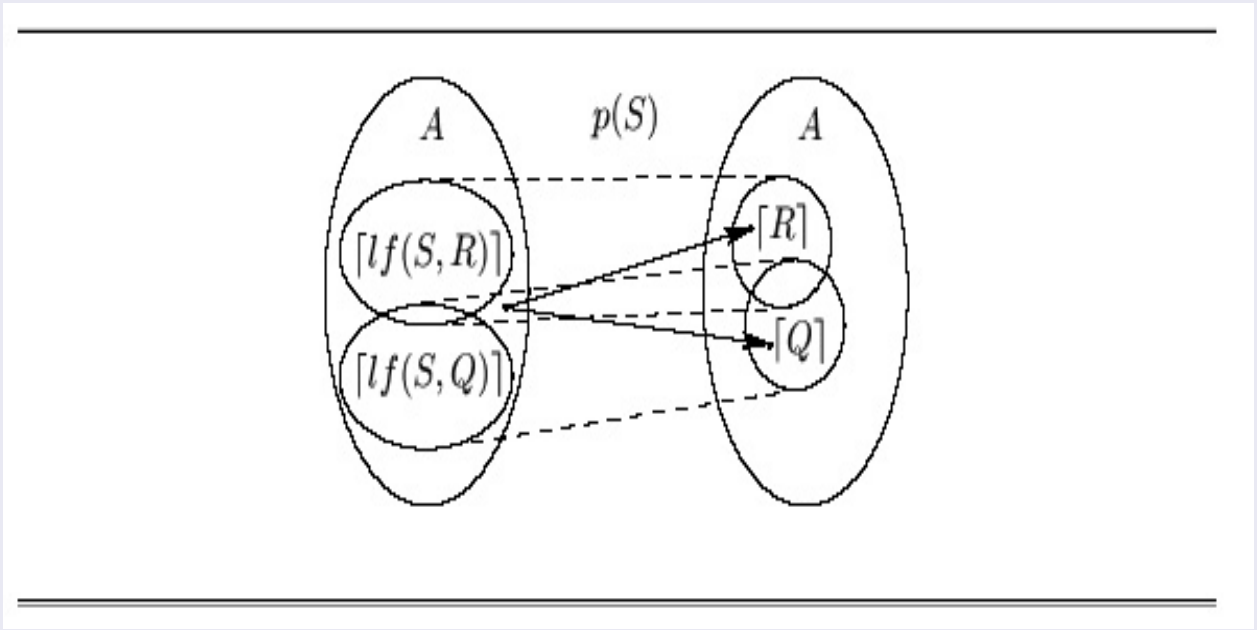
Bizonyítás (3)

$$
\begin{aligned}
[\mathit{If}\,(S,Q)] \quad \cap \quad & [\mathit{If}\,(S,R)] = \left\{a \in D_{p(S)} \mid p\,(S)\,(a) \subseteq [Q]\right. \\
\text{és} \quad & \left. p\,(S)\,(a) \subseteq [R]\right\} \\
= \quad & \left\{a \in D_{p(S)} \mid p\,(S)\,(a) \subseteq [Q \wedge R]\right\} \\
= \quad & [\mathit{If}\,(S, Q \wedge R)]\,.
\end{aligned}
$$



Bizonyítás (4)

Legyen $a \in [\mathit{lf}\,(S, Q) \vee \mathit{lf}\,(S, R)]$. Ekkor $a \in [\mathit{lf}\,(S, Q)]$, vagy $a \in [\mathit{lf}\,(S, R)]$. Felhasználjuk, hogy $Q \Rightarrow Q \vee R$ és $R \Rightarrow Q \vee R$. Ha $a \in [\mathit{lf}\,(S, Q)]$, akkor a 2. állítás alapján $a \in [\mathit{lf}\,(S, Q \vee R)]$. Ha $a \in [\mathit{lf}\,(S, R)]$, akkor a 2. állítás alapján ismét $a \in [\mathit{lf}\,(S, Q \vee R)]$.



Példa

Legyen $A = \mathbb{Z}, F = \left\{(x, y) \mid y = \left(x^2 - 1\right)^2 + 1\right\}$ és $S = \left\{(x, \alpha) \mid \alpha = \left\langle x, x^2 - 1, \left(x^2 - 1\right)^2 + 1\right\rangle\right\}$. Ekkor $D_{p(S)} = A$ és

$$p(S)(a) = \left\{\left(a^2 - 1\right)^2 + 1\right\}.$$

Legyen az S program utófeltétele $R : 1 \leq y \leq 17$, ahol y a program eredménye. Az R utófeltétel igazsághalmaza: $[R] = \{1, 2, \ldots, 17\} = [1..17]$. A

$$p(S)(a) = \left\{\left(a^2 - 1\right)^2 + 1\right\} \subseteq [R] = [1..17]$$

feltételből $-2 \leq a \leq 2$ adódik. Tehát $[\mathit{lf}\,(S, R)] = [-2..2]$, amelyhez választhatjuk az $\mathit{lf}\,(S, R) : -2 \leq a \leq 2$ állítást, mint leggyengébb előfeltételt.

Példa (folytatás)

Legyen az S program új utófeltétele: $R : y = 18 \vee y = 19$. Az $\left\{ \left(a^2 - 1\right)^2 + 1 \right\} \subseteq [R] = \{18, 19\}$ tartalmazási feltételnek egész a-ra nincs megoldása. Tehát csak $[\mathit{lf}\,(S, R)] = \emptyset$ és $\mathit{lf}\,(S, R) \equiv h$ lehetséges. Ha viszont az $R : y \in \mathbb{N}$ feltételt választjuk, akkor $[R] = \mathbb{N},\ [\mathit{lf}\,(S, R)] = \mathbb{Z} = A$ és $\mathit{lf}\,(S, R) \equiv i$.

A következőkben bevezetjük a feladat megadásának egy másik módját, és kimondunk egy gyakorlati szempontból fontos tételt. Általában a feladat nem függ az állapottér összes komponensétől, azaz az állapottér több pontjához is ugyanazt rendeli. Ezeket a pontokat fogjuk össze egy ponttá a paramétertér segítségével.

Definíció

Legyen $F \subseteq A \times A$ feladat. A B halmazt a feladat paraméterterének nevezzük, ha van olyan $F_1 \subseteq A \times B$ és $F_2 \subseteq B \times A$ reláció, hogy $F = F_2 \circ F_1$.

Fontos észrevenni, hogy paraméterteret mindig lehet találni. Például maga a feladat állapottere minden esetben választható paramétertérnek úgy, hogy a definícióban szereplő F_1 relációnak az identikus leképezést, F_2-nek pedig magát az F feladatot választjuk. Ám az, hogy egy konkrét esetben mit is választunk paramétertérnek a feladattól függ.

Specifikáció tétele

Legyen $F \subseteq A \times A$ feladat, B az F egy paramétertere, $F_1 \subseteq A \times B$, $F_2 \subseteq B \times A$ és $F = F_2 \circ F_1$. Legyen $b \in B$ és legyenek Q_b és R_b olyan állítások, amelyek igazsághalmazai

$$[Q_b] = \{a \in A \mid (a, b) \in F_1\} = F_1^{(-1)}(b),$$

$$[R_b] = \{a \in A \mid (b, a) \in F_2\} = F_2(b).$$

Ha minden $b \in B$ esetén $Q_b \Rightarrow \mathit{If}(S, R_b)$, akkor az S program megoldja az F feladatot.

Bizonyítás

Két tulajdonságot kell belátnunk:

1. $D_F \subseteq D_{p(S)}$
2. minden $a \in D_F$ esetén $p(S)(a) \subseteq F(a)$.

1. Legyen $a \in D_F$ tetszőleges. Ekkor létezik $b \in B$ úgy hogy $a \in [Q_b]$. A tétel feltevése miatt $[Q_b] \subseteq [lf\,(S, R_b)] = \left\{a \in D_{p(S)} \mid p\,(S)\,(a) \subseteq [R_b]\right\} \subseteq D_{p(S)}$. Tehát $D_F \subseteq D_{p(S)}$.
2. A $b \in F_1(a)$ tartalmazási feltétel miatt $F_2(b) \subseteq F_2\,(F_1(a))$ és

$$p(S)(a) \subseteq [R_b] = F_2(b) \subseteq F_2\,(F_1(a)) = F\,(a)\,.$$

Példa

Legyen $A = \mathbb{Z}$, $F = \left\{ \left(x, \left(x^2+1\right)^2 - 1 \right) \mid x \in A \right\}$ és

$$S = \left\{ (x, \alpha) \mid \alpha = \left\langle x, x^2+1, \left(x^2+1\right)^2 - 1 \right\rangle \right\} \subseteq A \times A^{**}.$$

Ekkor S program és megoldja az F feladatot.
Alkalmazzuk azonban a specifikáció tételét! Legyen $B = \mathbb{N}$, $F_1 = \left\{ \left(x, x^2+1\right) \mid x \in A \right\}$ és $F_2 = \left\{ \left(u, u^2-1\right) \mid u \in \mathbb{N} \right\}$. Ekkor $F = F_2 \circ F_1$ és B paramétertér. Legyen $b \in \mathbb{N} = B$ rögzített. Definíció szerint kapjuk, hogy

$$[Q_b] = \{a \in \mathbb{Z} \mid (a, b) \in F_1\} = \left\{a \in \mathbb{Z} \mid a^2 + 1 = b\right\}$$

és $Q_b : a^2 + 1 = b$.

Példa

Hasonlóképpen adódik, hogy

$$[R_b] = \{a \in \mathbb{Z} \mid (b, a) \in F_2\} = \left\{a \in \mathbb{Z} \mid a = b^2 - 1\right\}$$

és $R_b : a = b^2 - 1$.
Ugyancsak definíció szerint kapjuk, hogy
$p(S)(a) = \left\{(a^2 + 1)^2 - 1\right\}$,

$$[\mathit{If}\,(S, R_b)] = \left\{a \in A \mid \left\{\left(a^2 + 1\right)^2 - 1\right\}\right.$$
$$\left.\subseteq \left\{b^2 - 1\right\}\right\} = \left\{a \in A \mid a^2 + 1 = b\right\}$$

és $\mathit{If}\,(S, R_b) : a^2 + 1 = b$. Ha $b \in B$ olyan, hogy $Q_b = i$, akkor $a^2 + 1 = b$ és $\mathit{If}\,(S, R_b) = i$. Ha $Q_b = h$, akkor $a^2 + 1 \neq b$ és $\mathit{If}\,(S, R_b) = h$. Tehát minden $b \in B$ esetén $Q_b \Rightarrow \mathit{If}\,(S, R_b)$ (tkp. $Q_b \equiv \mathit{If}\,(S, R_b)$). A specifikáció tétele miatt az S program megoldja az F feladatot (azaz S helyes program).