

1. Nevezetes logikai függvények

Definíció: Legyen A tetszőleges halmaz. $HAMIS$ jelöli azt a logikai függvényt, melyre

$$\forall a \in A: HAMIS(a) = \{hamis\}$$

Definíció: Legyen A tetszőleges halmaz. $IGAZ$ jelöli azt a logikai függvényt, melyre

$$\forall a \in A: IGAZ(a) = \{igaz\}$$

Azaz a $HAMIS$ logikai függvény egy adott A halmaz minden eleméhez a *hamis*, az $IGAZ$ az *igaz* értéket rendeli.

2. A „következik” reláció

Definíció: Legyenek $Q, R \in A \rightarrow \mathbb{L}$ tetszőleges logikai függvények. Amennyiben $\lceil Q \rceil \subseteq \lceil R \rceil$ teljesül, akkor azt mondjuk hogy Q maga után vonja R -t (vagy másképp: Q -ből következik R) és a következőképpen jelöljük: $Q \implies R$.

Vegyük észre, hogy ha $Q \implies R$, akkor ez azt jelenti, hogy minden olyan $a \in A$ pontra amire Q igaz, arra igaz R is.

Példa: Legyen $A = \{1, 2, 3, 4\}$ és $Q, R \in A \rightarrow \mathbb{L}$ logikai függvények úgy hogy $\lceil Q \rceil = \{1, 3, 4\}$ és $\lceil R \rceil = \{1, 3\}$. Ebben az esetben $Q \implies R$ nem teljesül (mert a 4-re igaz Q de R nem), de $R \implies Q$ igen.

Példa: Legyen $A = (a:\mathbb{N}, h:\mathbb{N})$ és $Q, R \in A \rightarrow \mathbb{L}$ logikai függvények úgy hogy $Q = (a = 10)$ és $R = (h = a^3)$. Ugyan van olyan A -beli pont (az A halmaz most speciálisan egy állapottér, tehát elemei állapotok) amihez Q és R is igazat rendel, méghozzá az $\{a:10, h:1000\}$ állapot, de az nem igaz hogy $Q \implies R$, hiszen például $\{a:10, h:82\} \in \lceil Q \rceil$, de az $\{a:10, h:82\}$ elemhez R hamisat rendel.

3. Leggyengébb előfeltétel

Definíció: Legyen $S \subseteq A \times (\bar{A} \cup \{\text{fail}\})^{**}$ program, $R \in A \rightarrow \mathbb{L}$ logikai függvény. Ekkor az S program R utófeltételhez tartozó leggyengébb előfeltétele az az $lf(S, R): A \rightarrow \mathbb{L}$ függvény, amelyre

$$\lceil lf(S, R) \rceil = \{a \in A \mid a \in D_{p(S)} \wedge p(S)(a) \subseteq \lceil R \rceil\}$$

A leggyengébb előfeltétel tehát pontosan azokban a pontokban igaz, ahonnan kiindulva az S program biztosan hibátlanul terminál, és az összes lehetséges végállapotban igaz R .

Tétel: Az lf tulajdonságai

Legyen $S \subseteq A \times (A \cup \{\text{fail}\})^{**}$ program, $Q, R \in A \rightarrow \mathbb{L}$ logikai függvények. Ekkor

1. $lf(S, \text{HAMIS}) = \text{HAMIS}$
2. ha $Q \implies R$ akkor $lf(S, Q) \implies lf(S, R)$
3. $lf(S, Q) \wedge lf(S, R) = lf(S, Q \wedge R)$
4. $lf(S, Q) \vee lf(S, R) \implies lf(S, Q \wedge R)$

Példa: Legyen $A = (x:\mathbb{N})$. $R: A \rightarrow \mathbb{L}$ logikai függvény adott, $R = (x < 10)$. Számoljuk ki az $x := x - 5$ értékadásnak az R utófeltételhez tartozó leggyengébb előfeltételét.

Először megvizsgáljuk hogyan viselkedik az $x := x - 5$ program az állapottér néhány pontjában: az $\{x:8\}$ ponthoz az $\langle \{x:8\}, \{x:3\} \rangle$ sorozatot, míg az $\{x:2\}$ állapothoz az $\langle \{x:2\}, \text{fail} \rangle$ sorozatot rendel. A program programfüggvénye olyan $\{x:a_1\}$ állapotokban van értelmezve, ahol $a_1 \geq 5$, innen indulva a program garantáltan olyan pontban terminál ahol x értéke $a_1 - 5$. Egyéb állapotból indulva a program a fail állapotban terminál.

Felhasználva a leggyengébb előfeltétel definícióját, és az $x := x - 5$ értékadást S -sel jelölve, felírhatjuk:

$$\begin{aligned} [lf(S, R)] &= \{a \in A \mid a \in D_p(S) \wedge p(S)(a) \subseteq [R]\} = \\ &= \{a \in A \mid x(a) \geq 5 \wedge \{x(a) - 5\} \subseteq [R]\} = \\ &= \{a \in A \mid x(a) \geq 5 \wedge x(a) - 5 \in [R]\} = \\ &= \{a \in A \mid x(a) \geq 5 \wedge x(a) - 5 < 10\} \end{aligned}$$

Azaz azt kaptuk, hogy $lf(S, R) = (5 \leq x < 15)$ (ne felejtsük el hogy az A állapottéren az egyetlen változónk neve x és most számoltuk ki azon állapotok halmazát ahol a leggyengébb előfeltétel igaz).

A leggyengébb előfeltétel fogalma nagyon fontos, ugyanakkor nagyon egyszerű. Vegyük észre hogy az előbbi példában azt számoltuk ki, hogy az x értéke 15-nél kisebb kell legyen, hogy az $x := x - 5$ értékadást végrehajtva olyan pontban termináljunk ahol x értéke 10-nél kisebb.

Természetesen igaz az is hogy $(x \in [8..12]) \implies lf(x := x - 5, x < 10)$, azaz hogy ha az x -hez tartozó érték a $[8..12]$ halmazból van, akkor az $x := x - 5$ biztos hogy hibátlanul terminál, még hozzá olyan állapotban ahol $x < 10$ teljesül. Mindez azért van, mert az $x \in [8..12]$ feltétel szigorúbb mint a leggyengébb előfeltétel amit kiszámoltunk. Általánosan: ha valamely P

logikai függvényre teljesül hogy $P \implies lf(S, R)$ (azaz P szigorúbb mint az $lf(S, R)$ feltétel) akkor a P tulajdonságú pontokból indulva az S program biztos hogy helyesen terminál és a végpontokban igaz R . A leggyengébb előfeltételt ezért hívják „leggyengébb előfeltételnek”.

4. Specifikáció tétele

Definíció: Azt mondjuk hogy a B halmaz az $F \subseteq A \times A$ feladat egy paramétertere, ha léteznek olyan $F_1 \subseteq A \times B$ és $F_2 \subseteq B \times A$ relációk, melyekre $F = F_2 \circ F_1$.

Megjegyzés: Bármely $F \subseteq A \times A$ feladatnak létezik paramétertere. Hiszen legyen $B = A$, és válasszuk az $F_1 \subseteq A \times B$ és $F_2 \subseteq B \times A$ relációkat úgy, hogy $F_1 = id$ (azaz a minden A -beli elemhez önmagát rendelő reláció) és $F_2 = F$. Ekkor nyilvánvalóan teljesül hogy $F \circ id = F$.

Definíció: Legyenek A és B tetszőleges nemüres halmazok és $R \subseteq A \times B$ tetszőleges reláció. Az R reláció inverze:

$$R^{(-1)} ::= \{(b, a) \in B \times A \mid (a, b) \in R\}$$

azaz olyan B -ről A -ra képező reláció, ami pontosan akkor tartalmaz egy $(b, a) \in B \times A$ párt, ha $(a, b) \in R$.

Tétel: Legyen $F \subseteq A \times A$ feladat, B az F egy paramétertere (azaz léteznek olyan $F_1 \subseteq A \times B$ és $F_2 \subseteq B \times A$ relációk úgy hogy $F = F_2 \circ F_1$). Legyen $b \in B$ tetszőleges paraméter, amihez definiáljuk a $Q_b: A \rightarrow \mathbb{L}$ és $R_b: A \rightarrow \mathbb{L}$ logikai függvényeket az igazsághalmazaik megadásával:

$$\lceil Q_b \rceil ::= F_1^{(-1)}(b)$$

$$\lceil R_b \rceil ::= F_2(b)$$

Ekkor ha $\forall b \in B : Q_b \implies lf(S, R_b)$ akkor az S program megoldja az F feladatot.

$\lceil Q_b \rceil = \{a \in A \mid (a, b) \in F_1\}$, azaz Q_b igazsághalmazában olyan $a \in A$ állapotok vannak, melyekhez az F_1 reláció hozzárendeli a $b \in B$ paramétert.

$\lceil R_b \rceil = \{a \in A \mid (b, a) \in F_2\}$, azaz R_b igazsághalmazában olyan $a \in A$ állapotok vannak, melyeket az F_2 reláció a $b \in B$ paraméterhez rendel.

5. Feladat specifikációja

Tekintsük azt a feladatot, amikor egy adott pozitív egész egy osztóját kell megadnunk. A feladat állapottere $A = (n: \mathbb{N}^+, d: \mathbb{N}^+)$. Ezt a feladatot le tudjuk formálisan írni, mint olyan $(u, v) \in A \times A$ párok halmaza ahol u és v állapotok n változó szerinti értékei megegyeznek és

v célállapot d változóhoz tartozó értéke osztója az u kiindulási állapot n változóhoz tartozó értéknek:

$$\{(u, v) \in A \times A \mid n(u) = n(v) \wedge d(v) \mid n(u)\}$$

Felhasználva a specifikáció tételének jelöléseit, írjuk fel más módon - de formálisan - a feladat specifikációját. Azt vesszük észre, hogy minden $a \in A$ állapothoz melyekre $n(a)$ megegyezik, a feladat ugyanazt rendeli; nem függ a kiindulási állapot d változó szerinti értéktől. Írjuk fel az F feladatot a F_1 és F_2 relációk kompozíciójaként, úgy hogy azokhoz az állapotokhoz melyeknek F szerinti képe azonos, F_1 ugyanazt a paramétert rendelje. Mivel ezek az állapotok megegyeznek az n változóhoz tartozó értékükben, célszerű hozzájuk ugyanazt a (címkézett) értéket rendelni, F_1 reláció szerint. Azaz, a feladat egy paramétertere legyen a pozitív egész számok halmaza, ahol az értékre az n' változó segítségével (egy komponens lévén, nem lenne szükség változóra, de általános esetben kell) hivatkozhatunk: $B = (n':\mathbb{N}^+)$.

Azt, hogy F_1 pontosan akkor rendel egy $a \in A$ állapothoz egy $b \in B$ értéket, a specifikáció tételében szereplő Q_b logikai függvénnyel adhatjuk meg. Legyen $b \in B$ tetszőleges, ekkor $\forall a \in A : Q_b(a) = (n(a) = n'(b))$.

Természetesen úgy kapjuk meg F feladatot az F_1 és F_2 relációk kompozíciójaként, ha F_2 a $b \in B$ paraméterhez olyan állapotterbeli a pontot rendel, melynek d változóhoz tartozó értéke osztója a kiindulási állapot n változóhoz tartozó értékének. Épp ezért tetszőleges $b \in B$ esetén legyen R_b olyan logikai függvény, melyre

$$\forall a \in A : R_b(a) = (n(a) = n'(b) \wedge d(a) \mid n(a)).$$

Vegyük észre hogy a $n(a) = n'(b)$ kikötésre szükségünk van, anélkül csak annyit mondanánk hogy a célállapotban a d változóhoz tartozó érték osztója kell legyen az n változóhoz tartozó aktuális értéknek, nem fogalmaznánk meg szorosabb kapcsolatot a kiindulási állapot és a célállapot között. A feladat specifikációja tehát

$$A = (n:\mathbb{N}^+, d:\mathbb{N}^+)$$

$$B = (n':\mathbb{N}^+)$$

$$\forall b \in B : Q_b(a) = (n(a) = n'(b)) \text{ (ahol } a \in A \text{ tetszőleges állapot)}$$

$$\forall b \in B : R_b(a) = (n(a) = n'(b) \wedge d(a) \mid n(a)) \text{ (ahol } a \in A \text{ tetszőleges állapot)}$$

A továbbiakban a feladatnak ezen leírását (tehát ami tartalmazza a feladat állapotterét és a feladat egy paraméterterének megadását; minden $b \in B$ paraméterre a hozzá tartozó Q_b és R_b logikai függvények definícióját) a feladat specifikációjának nevezzük. Mivel d az A állapotteréről \mathbb{N} -re képező függvény (azaz argumentumába egy $a \in A$ elemet írhatunk), hasonlóan Q_b egy $b \in B$ paraméterhez definiált, $a \in A$ állapotokhoz logikai értéket rendelő függvény; az egyértelmű jelöléseket elhagyva a következőket kapjuk:

$$A = (n:\mathbb{N}^+, d:\mathbb{N}^+)$$

$$B = (n':\mathbb{N}^+)$$

$$Q = (n = n')$$

$$R = (Q \wedge d \mid n)$$