Programozáselmélet - A leggyengébb előfeltétel

Készítette: Borsi Zsolt

1. Nevezetes logikai függvények

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

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

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

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

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

Jelölés (Igazsághalmaz)***:*** Legyen $R \in A \to \mathbb{L}$ logikai függvény. Ekkor $\lceil R \rceil$ jelöli az olyan állapottérbeli pontok halmazát ahol R igaz. Azaz

$$\lceil R \rceil = \{a \in A \mid R(a) = \{igaz\}\}$$

Az $\lceil R \rceil$ halmazt az R logikai függvény *igazsághalmazának* nevezzük.

Ne felejtsük el hogy $R \in A \to \mathbb{L}$ nem feltétlenül értelmezett az A minden pontjában. Amennyiben $R\colon A \to \mathbb{L}$, akkor már viszont igaz hogy egy $a \in A$ pontban ha R nem igaz, akkor hamis.

2. A „következik" reláció

Definíció: Legyenek $Q, R \in A \to \mathbb{L}$ 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-ból 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 $Q, R \in A \to \mathbb{L}$ 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 $Q, R \in A \to \mathbb{L}$ 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 $S \subseteq A \times (\bar{A} \cup \{\textbf{fail}\})^{**}$ program, $R \in A \to \mathbb{L}$ logikai függvény. Ekkor az S program R utófeltételhez tartozó leggyengébb előfeltétele az az $lf(S, R)\colon A \to \mathbb{L}$ 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 $S \subseteq A \times (\bar{A} \cup \{\textbf{fail}\})^{**}$ program, $Q, R \in A \to \mathbb{L}$ logikai függvények. Ekkor

1. $lf(S, HAMIS) = HAMIS$
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. $lf(S, Q) \vee lf(S, R) \implies lf(S, Q \vee R)$

Példa: Legyen $A = (x{:}\mathbb{N})$. $R\colon A \to \mathbb{L}$ 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 $< \{x{:}8\}, \{x{:}3\} >$ sorozatot, míg az $\{x{:}2\}$ állapothoz az $< \{x{:}2\}, fail >$ sorozatot rendeli. A program programfüggvénye olyan $\{x{:}a_1\}$ állapotokban van értelmezve, ahol $a_1 \geqslant 5$, 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:

$$\begin{aligned}\lceil lf(S, R) \rceil = \{a \in A \mid a \in D_{p(S)} \wedge p(S)(a) \subseteq \lceil R \rceil\} &= \\ \{a \in A \mid x(a) \geqslant 5 \wedge \{x(a) - 5\} \subseteq \lceil R \rceil\} &= \\ \{a \in A \mid x(a) \geqslant 5 \wedge x(a) - 5 \in \lceil R \rceil\} &= \\ \{a \in A \mid x(a) \geqslant 5 \wedge x(a) - 5 < 10\}\end{aligned}$$

Azaz azt kaptuk, hogy az $lf(S, R)$ pontosan akkor igaz ha $(5 \leqslant x < 15)$. 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. Továbbá az x értéke legalább 5 kell legyen, hogy az $x := x - 5$ értékadás hibátlanul működjön (ne ffeljtsük: az x típusa természetes szám).
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, méghozzá olyan állapotban ahol $x < 10$ teljesül. Mindez azért van, mert az $x \in [8..12]$ feltétel szigorúbb mint az a leggyengébb előfeltétel amit előbb 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”.