Programozási módszertan

2. Specifikáció, leggyengébb előfeltétel

Feldhoffer Gergely

2012

Ismétlés

Def (Állapottér)

Legyenek $A_1, A_2, \ldots, A_n$ tetszőleges véges, vagy megszámlálható nem üres halmazok. Ekkor az $A = A_1 \times A_2 \times \cdots \times A_n$ halmazt **állapottér***nek, az A_i halmazokat pedig* **típusértékhalmaz***oknak nevezzük.*

Def (Feladat)

Feladat*nak nevezzük az $F \subseteq A \times A$ relációt.*

Def (Program)

Program*nak nevezzük az $S \subseteq A \times A^{**}$ relációt, ha*

1. $\mathcal{D}_S = A$
2. $\forall a \in A : \forall \alpha \in S(a) : \alpha_1 = a$
3. $\forall \alpha \in \mathcal{R}_S : \alpha = red(\alpha)$

Ismétlés

Def (Programfüggvény)

A $p(S) \subseteq A \times A$ reláció az $S \subseteq A \times A^{**}$ program **programfüggvény***e, ha*

1. $\mathcal{D}_{p(S)} = \{a \in A | S(a) \subseteq A^*\}$
2. $p(S)(a) = \{b \in A | \exists \alpha \in S(a) : \tau(\alpha) = b\}$

Def (Megoldás)

Azt modjuk, hogy as S program megoldja az F feladatot, ha

1. $\mathcal{D}_F \subseteq \mathcal{D}_{p(S)}$,
2. $\forall a \in \mathcal{D}_F : p(S)(a) \subseteq F(a)$.

Példák

Legyen $A = \mathbb{Z} \times \mathbb{Z}$. Az F feladat a kétszerezés feladata, ha
$F = \{((a, b), (c, d))|d = 2a\}$
vagy
$F = \{((a, b), (c, d))|d = 2a \wedge c = a\}$

Legyen $A = \{0, 1, 2, 3, 4, 5\}$, ekkor a
`while(a > 0) a--;`
program esetén $S = \{0 \rightarrow < 0 >, 1 \rightarrow < 10 >, 2 \rightarrow < 210 >, 3 \rightarrow < 3210 >, 4 \rightarrow < 43210 >, 5 \rightarrow < 543210 >\}$

Kiterjesztési tételek

A diasorban ugyan nem részleteztük, a feladat és a program állapottere nem kell megegyezzen ahhoz, hogy értelmezni tudjuk a megoldás fogalmát közöttük.

A feladat például kiterjeszthető bővebb állapottérre, ahol az állapottér azon altereire, amiket eredetileg nem tartalmazott, nem tesz kikötéseket ($proj_B(F) = B$), ezért nincs akadálya a feladat megoldása kedvéért a programban segédváltozók bevezetésének, hiszen azok tetszőleges állapota megengedett.

Igazsághalmaz

Ha $R \subseteq A \times \mathbb{L}$, akkor

R igazsághalmaza:
$\lceil R \rceil = \{a \in A | R(a) = \{igaz\}\}$

R gyenge igazsághalmaza:
$\lfloor R \rfloor = \{a \in A | igaz \in R(a)\}$

Ha R függvény, akkor $\lceil R \rceil = \lfloor R \rfloor$

$Q \to R \Rightarrow \lceil Q \rceil \subseteq \lceil R \rceil$

Előfeltétel, utófeltétel

Ha $S \subseteq A \times A^{**}$ program, akkor minden $R \subseteq A \to \mathbb{L}$ függvény lehet S előfeltétele vagy utófeltétele.

Megvizsgálható, hogy milyen viszonyban áll egymással az S program programfüggvénye, és R igazsághalmaza.

Szeretnénk eljutni most odáig, hogy egy F feladatot meg tudjunk fogalmazni elő- és utófeltétellel.

Leggyengébb előfeltétel

Def (Leggyengébb előfeltétel)

If az S program **Leggyengébb előfeltétel***e egy R utófeltételre, ha* $\lceil If(S,R) \rceil = \{a \in \mathcal{D}_{p(S)} | p(S)(a) \subseteq \lceil R \rceil\}$

Az S program leggyengébb előfeltételének igazsághalmaza egy R utófeltételre tehát azon pontok az állapottérben, ahonnan indulva az R feltételt kielégítő pontokban terminál a program.

Az *If* tulajdonságai

A csoda kizárásának elve: $\mathit{If}(S, \mathit{Hamis}) = \mathit{Hamis}$

Az *If* tulajdonságai

A csoda kizárásának elve: $\mathit{If}(S, \mathit{Hamis}) = \mathit{Hamis}$

Indirekt bizonyítás: tfh $\exists a \in \lceil \mathit{If}(S, \mathit{Hamis}) \rceil$. Mivel $\lceil \mathit{If}(S, R) \rceil = \{a \in \mathcal{D}_{p(S)} | p(S)(a) \subseteq \lceil R \rceil\}$ tehát $a \in \mathcal{D}_{p(S)}$ és $p(S)(a) \subseteq \lceil \mathit{Hamis} \rceil$, csakhogy $\lceil \mathit{Hamis} \rceil = \emptyset$

Az *If* tulajdonságai

Monotonitás: Ha $Q \Rightarrow R$ akkor $\mathit{If}(S, Q) \Rightarrow \mathit{If}(S, R)$

Az *If* tulajdonságai

Monotonitás: Ha $Q \Rightarrow R$ akkor $\mathit{If}(S, Q) \Rightarrow \mathit{If}(S, R)$

Indirekt bizonyítás: tfh $\exists a \in \lceil \mathit{If}(S, Q) \rceil \setminus \lceil \mathit{If}(S, R) \rceil$, azaz $a \in \mathcal{D}_{p(S)}$ és $p(S)(a) \subseteq \lceil Q \rceil \wedge p(S)(a) \not\subseteq \lceil R \rceil$. Ez ellentmondás, mivel abból indultunk ki, hogy $Q \Rightarrow R$

Az *If* tulajdonságai

$$If(S, Q) \wedge If(S, R) = If(S, Q \wedge R)$$

Az *If* tulajdonságai

$If(S, Q) \wedge If(S, R) = If(S, Q \wedge R)$

$If(S, Q) \wedge If(S, R) \Rightarrow If(S, Q \wedge R)$ mivel ha
$a \in \lceil If(S, Q) \wedge If(S, R) \rceil$ akkor $a \in \lceil If(S, Q) \rceil \wedge a \in \lceil If(S, R) \rceil$,
azaz $a \in \mathcal{D}_{p(S)} \wedge p(S)(a) \subseteq \lceil Q \rceil \wedge p(S)(a) \subseteq \lceil R \rceil$. Ekkor
$p(S)(a) \subseteq \lceil Q \rceil \cap \lceil R \rceil = \lceil Q \wedge R \rceil$, azaz $a \in \lceil If(S, Q \wedge R) \rceil$

$If(S, Q \wedge R) \Rightarrow If(S, Q) \wedge If(S, R)$, mivel ha $a \in \lceil If(S, Q \wedge R) \rceil$,
akkor, mivel az *If* definíciója szerint
$\lceil If(S, Q \wedge R) \rceil = \{a \in \mathcal{D}_{p(S)} | p(S)(a) \subseteq \lceil Q \wedge R \rceil\}$, tehát
$a \in \mathcal{D}_{p(S)} \wedge p(S)(a) \subseteq \lceil Q \wedge R \rceil$, vagyis
$p(S)(a) \subseteq \lceil Q \rceil \wedge p(S)(a) \subseteq \lceil R \rceil$, vagyis
$a \in \lceil If(S, Q) \rceil \wedge a \in \lceil If(S, R) \rceil$, vagyis $a \in \lceil If(S, Q) \wedge If(S, R) \rceil$

Az *If* tulajdonságai

$$If(S, Q) \vee If(S, R) \Rightarrow If(S, Q \vee R)$$

Az *If* tulajdonságai

$$If(S, Q) \vee If(S, R) \Rightarrow If(S, Q \vee R)$$

Bizonyítása házifeladat

Leggyengébb előfeltétel összefoglalás

A leggyengébb előfeltétel fogalma a program viselkedésének logikai formában való felírását teszi lehetővé.

A leggyengébb előfeltétel intuitívebben viselkedik mint a programfüggvény, ezért hasznos lesz, hogy a programfüggvény kifejezése nélkül is van eszköz a program működésének bizonyos aspektusait megfogalmazni. Kérdés, hogy a gyakorlatban elegendő-e ez mindenre.

Feladat paramétertere

Def (Paramétertér)

Legyen $F \subseteq A \times A$ feladat. B halmazt a feladat **paramétertere**, *ha $\exists F_1, F_2$, hogy $F_1 \subseteq A \times B \wedge F_2 \subseteq B \times A \wedge F = F_2 \circ F_1$*

ahol $R_1 \circ R_2$ két reláció kompozíciója, vagyis ha $a \in (R_1 \circ R_2)(b)$ akkor $a \in R_1(R_2(b))$.

A paramétertér tehát lehet az az altere az állapottérnek, amit a feladat inputra használ, olyan kezdeti értékek, amiket a végállapotokra vonatkozó kikötéseiben említ. Lehetne akár a teljes állapottér is, de tipikusan a legszűkebb alteret érdemes használni.

Specifikáció tétele

Tétel (Specifikáció tétele)

Legyen $F \subseteq A \times A$ *feladat,* B *az* F *feladat egy paramétertere,* $F_1 \subseteq A \times B \wedge F_2 \subseteq B \times A \wedge F = F_2 \circ F_1$, *legyen* $b \in B$
$\lceil Q_b \rceil = \{a \in A | (a, b) \in F_1\} = inv(F_1)(b)$
$\lceil R_b \rceil = \{a \in A | (b, a) \in F_2\} = F_2(b)$
Ekkor ha $\forall b \in B : Q_b \Rightarrow If(S, R_b)$, *akkor az* S *program megoldja az* F *feladatot.*

A tétel szerint lehetséges elő- és utófeltétellel és a leggyengébb előfeltétel fogalmával kiváltani a feladat-program-programfüggvény-megoldás fogalmakat.

Specifikáció tétele

Legyen $F \subseteq A \times A$ feladat, B az F feladat egy paramétertere, $F_1 \subseteq A \times B \wedge F_2 \subseteq B \times A \wedge F = F_2 \circ F_1$, legyen $b \in B$
$\lceil Q_b \rceil = \{a \in A | (a, b) \in F_1\} = inv(F_1)(b)$
$\lceil R_b \rceil = \{a \in A | (b, a) \in F_2\} = F_2(b)$
Ekkor ha $\forall b \in B : Q_b \Rightarrow If(S, R_b)$, akkor az S program megoldja az F feladatot.

Bizonyítás: $\mathcal{D}_F \subseteq \mathcal{D}_{p(S)}$ mivel bármely $a \in \mathcal{D}_F : \exists b \in B : a \in \lceil Q_b \rceil$ ugye F_1 miatt. A tétel feltétele, hogy $Q_b \Rightarrow If(S, R_b)$, vagyis
$a \in \lceil Q_b \rceil \subseteq \lceil If(S, R_b) \rceil \subseteq \mathcal{D}_{p(S)}$

$\forall a \in \mathcal{D}_F : p(S)(a) \subseteq F(a)$, mivel ha $a \in \mathcal{D}_F$ és $b \in B$ amire $a \in \lceil Q_b \rceil$, akkor
$p(S)(a) \subseteq \lceil R_b \rceil = F_2(b) \subseteq F_2(F_1(a)) = F(a)$

Specifikáció tétele

Arrafelé haladunk, hogy a feladatot meg tudjuk adni halmaz alak helyett specifikáció alakban, az állapottér, paramétertér, előfeltétel és utófeltétel alakban. Azt már beláttuk, hogy ha választottunk egy megfelelő B paraméterteret, akkor a program utófeltételre vonatkozó leggyengébb előfeltételének felhasználásával el tudjuk dönteni, hogy a program a specifikált feladatnak megoldása-e.

Már csak egy kényelmes módszer hiányzik a paramétertér megadására, és így a specifikáció tömör, használható felírása elméletileg megalapozottá válik.

Változók

Def (Változó)

Az $A = A_1 \times A_2 \times \cdots \times A_n$ állapottér $v_i : A \to A_i$ projekciós függvényeit **változó***knak nevezzük.*

A változó tehát nem a projektált halmaz (mivel az a típusértékhalmaz) hanem a vetítő függvény. Így értelmezhető lesz a program pillanatnyi állapotában a változó értéke, és értelmezhető lesz a feladat megfogalmazásakor felírt összefüggés az adott dimenzió mindenkori értékeire.

Feladat specifikációja változókkal

Példa: két szám összege

$A = \underset{x}{\mathbb{Z}} \times \underset{y}{\mathbb{Z}} \times \underset{z}{\mathbb{Z}}$

$B = \underset{x'}{\mathbb{Z}} \times \underset{y'}{\mathbb{Z}}$

$Q_{x'(b),y'(b)}(a) = (x(a) = x'(b) \wedge y(a) = y'(b))$

$R_{x'(b),y'(b)}(a) = (z(a) = x'(b) + y'(b) \wedge x(a) = x'(b) \wedge y(a) = y'(b))$

ahol a vesszős tagok a kezdeti állapotok megkülönböztetését szolgálják az állapottér végállapotaival összevetendő

Feladat specifikációja változókkal

Példa: két szám összege
$A = \underset{x}{\mathbb{Z}} \times \underset{y}{\mathbb{Z}} \times \underset{z}{\mathbb{Z}}$
$B = \underset{x'}{\mathbb{Z}} \times \underset{y'}{\mathbb{Z}}$
$Q_{x'(b),y'(b)}(a) = (x(a) = x'(b) \wedge y(a) = y'(b))$
$R_{x'(b),y'(b)}(a) = (z(a) = x'(b) + y'(b) \wedge x(a) = x'(b) \wedge y(a) = y'(b))$

ahol a vesszős tagok a kezdeti állapotok megkülönböztetését szolgálják az állapottér végállapotaival összevetendő

vegyük észre, hogy a változók paraméterei, tehát a program kezdeti állapotai és végállapotai, itt az a és b mindig a megfelelő helyen vannak: az előfeltételben a paraméterek rögzítésekor, a paramétertérre való hivatkozáskor b, az állapottérre való hivatkozáskor a. Ez tehát a jelölés általánosságának megtartásával elhagyható

Feladat specifikációja változókkal

Példa: két szám összege

$A = \underset{x}{\mathbb{Z}} \times \underset{y}{\mathbb{Z}} \times \underset{z}{\mathbb{Z}}$

$B = \underset{x'}{\mathbb{Z}} \times \underset{y'}{\mathbb{Z}}$

$Q_{x',y'}(a) = (x = x' \wedge y = y')$

$R_{x',y'}(a) = (z = x' + y' \wedge x = x' \wedge y = y')$

Feladat specifikációja változókkal

Példa: két szám összege
$A = \underset{x}{\mathbb{Z}} \times \underset{y}{\mathbb{Z}} \times \underset{z}{\mathbb{Z}}$
$B = \underset{x'}{\mathbb{Z}} \times \underset{y'}{\mathbb{Z}}$
$Q_{x',y'}(a) = (x = x' \wedge y = y')$
$R_{x',y'}(a) = (z = x' + y' \wedge x = x' \wedge y = y')$

Ez tovább egyszerűsíthető, mivel mindig a paramétertér minden pontjára vonatkozik a feltétel

Feladat specifikációja változókkal

Példa: két szám összege

$A = \underset{x}{\mathbb{Z}} \times \underset{y}{\mathbb{Z}} \times \underset{z}{\mathbb{Z}}$

$B = \underset{x'}{\mathbb{Z}} \times \underset{y'}{\mathbb{Z}}$

$Q : x = x' \wedge y = y'$

$R : z = x' + y' \wedge x = x' \wedge y = y'$

Feladat specifikációja változókkal

Példa: két szám összege

$A = \underset{x}{\mathbb{Z}} \times \underset{y}{\mathbb{Z}} \times \underset{z}{\mathbb{Z}}$

$B = \underset{x'}{\mathbb{Z}} \times \underset{y'}{\mathbb{Z}}$

$Q : x = x' \wedge y = y'$

$R : Q \wedge z = x' + y'$