Eötvös Loránd Tudományegyetem

Informatikai Kar

Programozási Nyelvek és Fordítóprogramok Tanszék

Osztott rendszerek szintézise

IPM-08sztORSZE

Konzultációs segédanyag

Kopácsi László, Szabó Miklós

Utolsó módosítás: 2018. február 25.

Tartalomjegyzék

1. konzultáció **2**

1.1. Áttekintés 2

1.2. Étkező filozófusok 2

1.3. Moziterem 3

2. konzultáció **4**

2.1. Áttekintés 4

2.2. Program 6

2.3. Leggyengébb előfeltétel 7

3. Megoldások **10**

1. konzultáció

1.1. Áttekintés

Az előadás során több, temporális logikai relációval találkoztunk, nézzük ezeket át informálisan, kezdve a biztonsági tulajdonságokkal.

- Az első, melyet "háromszög"-ként említünk ($\rhd$), bizonyos állapot-átmeneteket megenged, másokat pedig megtilt. A $(P \rhd Q)$ azt jelenti, hogy a P állapotot **ha** elhagyjuk, akkor ezt csak a Q-n keresztül tehetjük meg. A háromszög azonban nem tesz semmiféle kikötést arról, hogy a P-t el kell hagynunk, csupán biztosít minket arról, hogy ha ez mégis megtörténik, akkor milyen irányba (nem) mozdulhatunk.

- Másik biztonsági tulajdonság az *invariáns*. Ha egy K állítás invariáns, akkor ennek minden állapot-átmenet előtt és után teljesülnie kell.

- A harmadik említett kikötés a *fixpont*. Ezzel leírhatjuk, hogy ha egy rendszerben már nem figyelhetünk meg további állapot-átmeneteket, akkor milyen tulajdonságoknak kell teljesülnie. $(FP \Rightarrow R)$ estén például egy R-el jelölt állítás igaz, amennyiben fixpontba jutottunk. Fixpontba azonban nem csak a kívánt befejezési állapot tartozhat, ha holtpont helyzet alakul ki, azt is tekinthetjük fixpontnak.

Természetesen nem csak biztonsági tulajdonságokra van szükségünk - azaz mit (ne) csinálhasson a rendszer -, hanem haladásira is (azért csináljon valamit).

- Az "egyenes nyíl" ($\mapsto$) néven nevezett reláció egy szigorú kikötés arra vonatkozóan, hogy egy állapotból milyen másik helyzetbe **kell** lépnünk. Míg $\rhd$ esetén csupán azt mondtuk, hogy *ha* elhagyunk egy állapotot, akkor azt milyen irányba tegyük, a $(P \mapsto Q)$ azt mondja, hogy a P állapotból a Q állapotba kell, hogy kerüljünk (véges időn belül).

- Ennél megengedőbb a "görbe nyíl"-ként ($\hookrightarrow$) ismert reláció. Ebben az esetben a $(A \hookrightarrow B)$ feltétel csupán annyit mond, hogy az A állapotot előbb-utóbb a B állapot fogja követni (azaz A-ból elkerülhetetlenül B-be fogunk érkezni), de itt nincs semmilyen megkötés arra, hogy a két állapot egymás után következzen be. Legális állapot-átmenet sorozat az $(A \hookrightarrow B)$-ra az $< A, G, F, D, F, E, C, D, B >$ is.

1.2. Étkező filozófusok

Tekintsük az előadáson is ismertetett *étkező filozófusok* feladatot (jegyzet[1] 1.1). Próbáljuk meg kiegészíteni a feltételeket további megkötések formalizálásával:

- Ha a rendszer nyugalmi állapotban van, akkor egy filozófus sem eszik.

- Mindegyik filozófusra igaz, hogy ha hazament, akkor utána már nem kerülhet más állapotba.

1.3. Moziterem

A következő példában egy mozira vonatkozó feladatot fogunk ismertetni, ahol a nézők tevékenységére szeretnénk megkötéseket tenni. A jelölést megkönnyítendő vezessük be az alábbiakat: $n(i)$ jelölje az i-ik nézőt. A moziba látogatók állapotait az alábbiak alapján jelöljük:

a) megérkezik a moziba - a

b) jegyet vesz - j

c) üdítőt és nasit vásárol - b

d) érvényes jeggyel rendelkezik - t

e) filmet néz - f

f) hazamegy - h

Próbáljuk formalizálni az alábbi feltételeket:

- A moziba érkező néző filmet fog nézni.
- Ha valaki érvényes jeggyel rendelkezik, akkor megnézi a filmet.
- Ha a moziban nincs mozgás, akkor minden néző már otthon van.
- A moziba érkező néző jegyet vásárol, vagy a büfébe megy.
- A film után a néző hazamegy.
- Senki nem nézhet filmet úgy, hogy nincs érvényes jegye. (Tipp: próbáljunk invariánst megfogalmazni.)
- Ha valaki hazament, akkor már nem csinál semmit a moziban.

2. konzultáció

2.1. Áttekintés

Ahhoz, hogy a későbbiekben biztos módon számolhassunk programokkal , elkerülhetetlen a számunkra szükséges (alap)fogalmakat tisztázni a halmazelmélet és a relációk témakörében.

Legyenek A és B tetszőleges halmazok. A és B *direkt-*, vagy *Descartes*-szorzatán azt a halmazt értjük, melyben olyan párok találhatóak, melynek első eleme A-, második eleme pedig B-beli.

$$A \times B ::= \{(a,b) | a \in A \text{ és } b \in B\}$$

Jelölje $r \subseteq A \times B$ azt a bináris relációt, mely A elemeihez rendel értékeket a B halmazból (A és B tetszőleges halmazok). A reláció elemeit $(a,b) \in r$ módon fogjuk jelölni.

$$\text{Az } r \text{ reláció értelmezési tartománya: } \mathcal{D}_r ::= \{a \in A | \exists b \in B : (a,b) \in r\} \subseteq A$$

$$\text{Az } r \text{ reláció értékkészlete: } \mathcal{R}_r ::= \{b \in B | \exists a \in A : (a,b) \in r\} \subseteq B$$

$$r(a) \text{ jelölje azt a halmazt, melynek elemei: } \{b \in B | (a,b) \in r\}$$

Világos, hogy az értelmezési tartományban olyan elemek vannak, amikhez rendel valamit r, míg az értékkészletben olyanokat találhatunk, amik valamilyen elemhez hozzá lettek rendelve. Egy elem képe a hozzá rendelt elemek halmazából áll elő.

Egy g relációt *parciális függvény*nek (vagy determinisztikus relációnak) nevezhetünk, amennyiben az alábbi teljesül:

$$\forall a \in A : |g(a)| \leq 1,$$

azaz minden elemhez *legfeljebb* egy másikat társítunk. Jelölésünk ekkor: $g \in A \to B$. Ha minden elemhez pontosan egy értéket rendelünk, akkor az f reláció függvény, azaz:

$$\forall a \in A : |f(a)| = 1.$$

Jelölésünk ekkor: $f : A \to B$. Ebben az esetben általában $f(a)$ nem az egy elemű halmazt, hanem annak képét jelenti.

Ahhoz, hogy állításokat fogalmazhassunk meg a későbbiekben, szükségünk lesz logikai relációkra is.

$$\text{A } h \subseteq A \times \mathbb{L} \text{ logikai relációnak nevezzük, ahol } \mathbb{L} ::= \{igaz, hamis\}.$$

Ha h függvény, akkor *logikai függvény*nek nevezzük.

Egy reláció inverzét az alábbi módon definiálhatjuk:

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

A továbbiakban szükségünk lesz egy reláció adott halmazra vonatkozó inverz- és őskép definíciójára.
A $H \subseteq B$ halmaz R reláció szerinti *inverz*képe:

$$R^{(-1)}(H) ::= \{a \in A | R(a) \cap H \neq \varnothing\}$$

A $H \subseteq B$ halmaz R reláció szerinti *ős*képe:

$$R^{-1}(H) ::= \{a \in A | R(a) \subseteq H\}$$

Meggondolva látható, hogy az *inverzkép* megengedőbb, hisz csak annyit kér, hogy egy adott elemhez *létezzen* H-beli elem az R hozzárendelésben, az *őskép* viszont megköveteli, hogy *minden* ilyen elem a H halmazban legyen.
Legyen $R \subseteq A \times \mathbb{L}$ logikai reláció, R igazsághalmaza ekkor:

$$\lceil R \rceil ::= R^{-1}(\{igaz\}) \text{ azaz: } \lceil R \rceil = \{a \in \mathcal{D}_R | R(a) \subseteq \{igaz\}\}$$

Az igazsághalmazt tehát az $\{igaz\}$ halmazra vett őskép szerint definiáljuk.
Ha inverzképet számolunk, akkor juthatunk a *gyenge igazsághalmaz* fogalmához:

$$\lfloor R \rfloor ::= R^{(-1)}(\{igaz\}) \text{ azaz: } \lfloor R \rfloor = \{a \in \mathcal{D}_R | R(a) \cap \{igaz\} \neq \varnothing\}$$

A későbbiekben nagyban megkönnyíti a dolgunkat, ha bevezetjük az *azonosan igaz*, és az *azonosan hamis* logikai függvényeket.

$$Igaz : A \to \mathbb{L} : \forall a \in A : Igaz(a) = \{igaz\}$$

$$Hamis : A \to \mathbb{L} : \forall a \in A : Hamis(a) = \{hamis\}$$

Könnyű meggondolni, hogy ekkor $\lceil Igaz \rceil = A$ és $\lceil Hamis \rceil = \varnothing$.
Az igazsághalmazzal kapcsolatban fontos megemlíteni néhány tulajdonságot, melyeket a későbbiekben kihasználunk.

Legyenek P, $Q \subseteq A \times \mathbb{L}$, ekkor:

- $\lceil P \wedge Q \rceil = \lceil P \rceil \cap \lceil Q \rceil$
- $\lceil P \vee Q \rceil = \lceil P \rceil \cup \lceil Q \rceil$
- $\lceil \neg P \rceil = A \setminus \lceil P \rceil$

- $\lceil P \to Q \rceil = \lceil \neg P \vee Q \rceil = (A \setminus \lceil P \rceil) \cup \lceil Q \rceil$
- $P \Rightarrow Q = \lceil P \rceil \subseteq \lceil Q \rceil$

Egyszerűbben megfogalmazhatóak állítások, ha tudjuk, hogy $A \Rightarrow B$. Ekkor ugyanis:

- $A \vee B = B$
- $A \wedge B = A$

Nézzünk erre egy példát, legyenek A, $B : \mathbb{N} \times \mathbb{L}$ úgy, hogy:
$\lceil A \rceil$:={10-nél nagyobb szám} és
$\lceil B \rceil$:= {pozitív szám}.
Világos, hogy $A \Rightarrow B$, hiszen ha egy egész szám 10-nél nagyobb, akkor pozitív. Az $A \vee B$ állítást úgy fogalmazhatjuk meg, hogy azokat az egész számokat keressük, melyek 10-nél nagyobbak, **vagy** pozitívak. Érződik, hogy a *vagy* kapcsolat miatt a gyengébb feltétellel is megelégszünk, így a bővebb halmaz, azaz a pozitív számok halmazát kapjuk ($= B$). Ha azonban a 10-nél nagyobb **és** pozitív számokra vagyunk kíváncsiak, akkor a szigorítás miatt a szűkebb halmazt kapjuk, tehát a 10-nél nagyobb számokat kell vizsgálnunk ($= A$).

2.2. Program

Röviden tekintsük át, hogy a Fóthi[2]-Horváth - féle modellben hogyan is definiáltuk a programot és annak hatásrelációját.

Jelölje A^* az A elemeiből képzett véges, A^∞ pedig a végtelen sorozatokat. A későbbiekben A^{**} jelenti az $A^* \cup A^\infty$ halmazt, azaz a véges és végtelen sorozatok halmazát. Ha alaphalmaznak a természetes számokat választjuk, akkor az $< 1, 5, 3, 2 > \in A^*$ egy véges, míg az $< 1, 2, 3, 4, ... > \in A^\infty$ végtelen sorozatot jelöl.

Utasítás alatt egy olyan $s \subseteq A \times A^{**}$ relációt értünk, melyre:

1. $\mathcal{D}_s = A$
2. $\forall a \in A : \forall \alpha \in s(a) : |\alpha| \neq 0 \wedge \alpha_1 = a$
3. $(\alpha \in \mathcal{R}_s \wedge \alpha \in A^*) \Rightarrow (\forall i (1 \leq i < |\alpha|) : \alpha_i \neq \alpha_{i+1})$
4. $(\alpha \in \mathcal{R}_s \wedge \alpha \in A^\infty) \Rightarrow (\forall i \in \mathbb{N} : (\alpha_i = \alpha_{i+1} \to (\forall k \in \mathbb{N}^+ : \alpha_i = \alpha_{i+k}))$

A fenti definíció a *működés* fogalmát próbálja absztrakt módon szemléltetni. A négy pont jól jellemzi az utasítást: elsőként szeretnénk, ha az utasítás minden állapottér-beli pontban értelmezve lenne (azaz az utasítás mindenhonnan el tud indulni).
Második pontban azt fogalmazzuk meg, hogy egy sorozat a működése teljes történetét írja le, kezdve a kiindulási állapottal.
A harmadik pontunk a *redukáltságra* vonatkozik: ha véges hosszú sorozattal dolgozunk,

akkor egymás után kétszer ne szerepelhessen ugyanaz az elem (hiszen az nem egy jó véges utasítás, amelyik úgy lép egy következő állapotba, hogy nem történt állapotváltozás - ez a megfogalmazáson is érződik).
A negyedik pont a végtelen utasításra utal: ha egy utasítás futása nem fejeződik be (végtelen ciklus, stb.), akkor ezt a hozzárendelt sorozatban úgy jelzi, hogy egy adott ponttól kezdve nem történik állapotváltozás, folyton ugyan abban az állapotban ragad (pl. $s(4) =< 4, 3, 2, 1, 0, 0, 0, 0, 0, 0, ... >$)

Egy $s \subseteq A \times A^{**}$ utasítás *hatásreláció*ja az a $p(s) \subseteq A \times A$ reláció, melyre:

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

ahol $\tau : A^* \to A; \tau(\alpha) ::= \alpha_{|\alpha|}$, azaz a *tau* függvény egy véges sorozathoz annak utolsó tagját rendeli.

A hatásrelációt tehát csak olyan pontokban definiáljuk, ahol a program *megáll*, azaz véges sorozatot rendel, a hozzárendelési szabály pedig az, ahová az utasítás eljut, tehát az adott sorozatok utolsó eleme.

Az előzőek alapján meg tudjuk az *absztrakt program*ot egy $S = (s_0, \{s_1, s_2, \ldots, s_n\})$ párként. Ez egy párhuzamos programot jelöl, melynek első tagja (s_0) a kezdeti utasítás, ami a program indulásakor hajtódik végre. A második tagja ($\{s_1, s_2, \ldots, s_n\}$) *atomi* (vagyis párhuzamos futás során nem akadnak össze, szekvenciális futás eredményét adó) utasítások halmaza, amelyeket valamilyen *feltétlenül pártatlan ütemezés* (kiéheztetés nélkül, azaz egy végrehajtás során minden utasítás végtelen sokszor kerül kiértékelésre) szerint végtelen sokáig értékelünk ki. A programra pedig akkor mondjuk, hogy terminált (befejeződött), ha fixpontba jut, azaz már nem történik állapotváltozás.

Az egyszerűség kedvéért nézzük erre egy példát:
Legyen $S = (x := 0, \{x := 2 \cdot x, x := x + 1\})$. Ekkor az alábbi sorozatot ennek egy lehetséges kiértékelésének tekintjük:

$$\begin{array}{ccccccc} x := 0, & x := x+1, & x := 2*x, & x := 2*x, & x := x+1, & x := x+1, & \ldots \\ 0, & 1, & 2, & 4, & 5, & 6, & \ldots \end{array}$$

2.3. Leggyengébb előfeltétel

Érezhető, hogy a fenti definíciókkal történő számolások nagyon nehézzé fogják tenni a későbbiekben a feladatok és az azt megoldó programok közötti kapcsolat megteremtését, ezért bevezetünk egy új fogalmat, a *leggyengébb előfeltétel*t.

Legyen $s \subseteq A \times A^{**}$ utasítás, $R : A \to \mathbb{L}$ állítás. Az s utasítás R utófeltételhez tartozó *leggyengébb előfeltétele* az az $lf(s, R) : A \to \mathbb{L}$ **függvény**, melyre:

$$\lceil lf(s, R) \rceil = \{A \in \mathcal{D}_{p(s)} | p(s)(a) \subseteq \lceil R \rceil\}.$$

Az *lf* tehát egy olyan függvény, mely pontosan azokhoz a pontokhoz rendel igazat, melyből elindítva az s utasítást az biztosan megáll, és az összes ilyen állapotban az R tulajdonság teljesül. Magának a függvénynek a definícióját legtöbbször nehéz megadni, de az igazsághalmazát könnyedén kifejezhetjük. Az igazsághalmaz definícióját, a kompozíció és az őskép tulajdonságait felhasználva kapjuk, hogy:

$$\lceil lf(s, R) \rceil = \lceil R \circ p(s) \rceil.$$

Az *lf*-et tehát az utófeltételbe helyettesítés módszerével tudjuk kifejezni (ennek bizonyítása megtalálható a *tankönyv*[2] 44-ik oldalán, a 3.1-es definíciónál).

Mivel a leggyengébb előfeltételt nem csak utasításokra, hanem programokra is ki szeretnénk tudni számolni, a fenti definíciót picit általánosítani kell. Tehát legyen $S = (s_0, \{s_1, s_2, \ldots, s_n\})$ program, $R : A \to \mathbb{L}$ állítás. Ekkor az S program R utófeltélhez tartozó *leggyengébb előfeltétele* az egyes utasításai által adott leggyengébb előfeltételek konjugáltja lesz:

$$lf(S, R) = \bigwedge_{i=1}^{n} lf(s_i, R).$$

A későbbiekben több alaptulajdonságra is szükségünk lesz, ha az *lf*-fel akarunk számolni. Nézzük ezeket:

Legyen $S = (s_0, \{s_1, s_2, \ldots, s_n\})$ program, $Q, R : A \to \mathbb{L}$ állítások. Ekkor:

1. $lf(S, Hamis) = Hamis$ (csoda kizárásának elve),
2. Ha $Q \Rightarrow R$, akkor $lf(S, Q) \Rightarrow lf(S, R)$ (monotonitás),
3. $lf(S, Q) \vee lf(S, R) \Rightarrow lf(S, Q \vee R)$ (gyenge additivitás),
4. $lf(S, Q) \wedge lf(S, R) = lf(S, Q \wedge R)$ (multiplikativitás)

A bizonyításokat szintén a jegyzetben lehet olvasni.

Kiszámítása: Az *lf* kiszámolását a már fentebb említett utófeltételbe helyettesítés módszerével tudjuk megtenni.

Az **egyszerű értékadás**ok során ez a következőt jelenti:

$$lf(x := y, R) = R^{x \leftarrow y}$$

Például az $S = \{x := 3\}, R = (1 \leq x \leq 5)$ esetben:
$lf(S, R) = lf(\{x := 3\}, (1 \leq x \leq 5)) = R^{x \leftarrow y} = (1 \leq x \leq 5)^{x \leftarrow 3} = (1 \leq 3 \leq 5)$. Az S programot tehát olyan állapotokból tudjuk elindítani biztonságosan úgy, hogy R-be érkezzen, melyre teljesül az, hogy $1 \leq 3 \leq 5 \equiv igaz$, azaz tetszőleges pontból indítva helyesen működő programot kaphatunk.

Feltételes értékadás esetén figyelembe kell venni a feltételt is, hiszen ha ez nem teljesül, abban az esetben nem kell az értékadást végrehajtanunk.

$$lf(\{x := y, \text{ha } \pi\}, R) = (\pi \rightarrow R^{x \leftarrow y}) \wedge (\neg\pi \rightarrow R^{SKIP})$$

Szimultán értékadás során egyszerre hajtjuk végre az adott értékadásokat:

$$lf(\{x_1, ..., x_n := y_1, ..., y_n\}, R) = lf(\{\mathop{\Big\|}_{i=1}^{n} x_i := y_i\}, R) = R^{\substack{x_1 \leftarrow y_1 \\ \cdots \\ x_n \leftarrow y_n}}$$

A **feltételes szimultán értékadás** kiszámításának módja ezek után egyértelműen megállapítható az előzőek alapján:

$$lf(\{x_1, ..., x_n := y_1, ..., y_n, \text{ha } \pi\}, R) = lf(\{\mathop{\Big\|}_{i=1}^{n} x_i := y_i, \text{ha } \pi\}, R) =$$

$$= (\pi \rightarrow R^{\substack{x_1 \leftarrow y_1 \\ \cdots \\ x_n \leftarrow y_n}}) \wedge (\neg\pi \rightarrow R^{SKIP})$$

3. Megoldások

1.2 - Étkező filozófusok

- $FP \Rightarrow (\forall i : \neg f(i).e)$
- $f(i).o \rhd \perp$

1.3 - Moziterem

- $n(i).a \hookrightarrow n(i).f$
- $n(i).t \hookrightarrow n(i).f$
- $FP \Rightarrow \forall i : n(i).h$
- $n(i).a \rhd (n(i).j \vee n(i).b)$
- $n(i).f \mapsto n(i).h$
- $(\forall i : n(i).f \Rightarrow n(i).t) \in inv$
- $n(i).h \rhd \perp$

Hivatkozások

[1] dr. Horváth Zoltán: Párhuzamos és elosztott programozás (http://people.inf.elte.hu/hz/parh/jegyzet.ps)

[2] Fóthi Ákos: Bevezetés a programozáshoz (http://bzsr.web.elte.hu/progmod2/konyv.pdf)