Tartalomjegyzék

Tétel 3: Programtulajdonságok definíciói, a rájuk vonatkozó szabályok (pl. stabillal metszés) 1
Leggyengébb előfeltétel (lf, wp) . . . 1
Legszigorúbb utófeltétel (sp) . . . 1
Viselkedési reláció . . . 1
$P \rhd_S Q$, “P, feltéve, hogy nem Q”, unless . . . 1
$P \mapsto_S Q$, “P biztosítja Q”, ensures . . . 2
$P \hookrightarrow_S Q$, “P-ből elkerülhetetlen Q”, leads-to . . . 2
$P \in inv_S(Q)$, “Q-ból indulva P invariáns” . . . 2
$R \in FP_S$, “R teljesül fixpontban” . . . 3
$Q \in TERM_S$, “Q-ból a program biztosan fixpontba jut” . . . 3

Tétel 3: Programtulajdonságok definíciói, a rájuk vonatkozó szabályok (pl. stabillal metszés)

Leggyengébb előfeltétel (lf, wp)

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

R és $lf(s,R) : A \mapsto L$

Logikai függvény, amely megadja azon állapotokat, ahonnan indulva R biztosan teljesül.

Alaptulajdonságok:

- Csoda kizárásának elve: $lf(s, Hamis) = Hamis$
- $\lceil lf(s, Igaz) \rceil = D_{p(s)} = A$, azaz $lf(s, Igaz) = Igaz$
- Utófeltételbe helyettesítés módszere: $\lceil lf(s,R) \rceil = \lceil R \circ p(s) \rceil$
- Monotonitás: ha $P \Rightarrow Q$ akkor $lf(s,P) \Rightarrow lf(s,Q)$
- Gyenge additivitás: $lf(s,Q) \vee lf(s,R) \Rightarrow lf(s, Q \vee R)$
- Multiplikativitás: $lf(s,Q) \wedge lf(s,R) = lf(s, Q \wedge R)$

A leggyengébb előfeltétel általánosítható absztakt párhuzamos programokra. Az $lf(s,R)$-re belátott tulajdonságok teljesülnek $lf(S,R)$-re is.

Legszigorúbb utófeltétel (sp)

$\lceil sp(s,Q) \rceil = p(s)(\lceil Q \rceil)$

Q és $sp(s,Q) : A \mapsto L$

Logikai függvény, amely megadja azon állapotokat, ahova Q-ból s elvezet.

Viselkedési reláció

Reláció hatos: $\rhd_S$, $\mapsto_S$, $\hookrightarrow_S$, inv_S, FP_S, $TERM_S$

$INIT$ nem tartozik bele.

A viselkedési relációt és a feladat specifikációs feltételeit majd a megoldás fogalma fogja összekötni.

$P \rhd_S Q$, “P, feltéve, hogy nem Q”, unless

- Biztonsági tulajdonság

- $P \rhd_S Q \equiv P \land \neg Q \Rightarrow lf(S, P \lor Q)$
- Megjegyzés: csak a $P \land \neg Q$-beli állapotokra mond nekünk valamit
- Reflexív: $P \rhd_S P$
- Hogyha S mindenhol értelmezve van: $P \rhd_S \neg P$
- Jobbról gyengíthető: $(P \rhd_S Q) \land (Q \Rightarrow R)$ esetén $P \rhd_S R$
- Diszjunktív: $(P \rhd_S R) \land (Q \rhd_S R)$ esetén $P \lor Q \rhd_S R$

Stabil tulajdonság: $P \rhd_S Hamis$

- $P \rhd_S Hamis \equiv P \Rightarrow lf(S, P)$
- Minden invariáns egy stabil tulajdonság
- Azonban $P \rhd_S Hamis$ nem tud egy programmal szemben garanciákat biztosítani, hiszen semmi nem garantálja, hogy P valaha teljesülni fog. Ez a motiváció az invariáns tulajdonság mögött.
- Stabillal metszés: $(P \rhd_S Q) \land (K \rhd_S Hamis)$ esetén $(P \land K) \rhd_S (Q \land K)$

$P \mapsto_S Q$, "P biztosítja Q", ensures

- Haladási tulajdonság
- $P \mapsto_S Q \equiv (P \rhd_S Q) \land (\exists s \in S : P \land \neg Q \Rightarrow lf(s, Q))$
- Reflexív, jobbról gyengíthető, stabillal metszhető
- Nem diszjunktív
  - Ha P_1-ből s_1 utasítás visz Q-ba, P_2-ből viszont s_2, akkor a $\mapsto_S$ nem fog teljesülni, mert más állapot esetén más utasítást kéne végrehajtani
- Csoda kizárása: $P \mapsto_S Hamis$ esetén $P = Hamis$
- Implikációból következik: $P \Rightarrow R$ esetén $P \mapsto_S R$

$P \hookrightarrow_S Q$, "P-ből elkerülhetetlen Q", leads-to

- Haladási tulajdonság
- A $\mapsto_S$ reláció tranzitív diszjunktív lezártja
- Azaz a legkisebb reláció, amelyre teljesül:
  - $(P \mapsto_S R) \Rightarrow (P \hookrightarrow_S R)$
  - $(P \hookrightarrow_S Q) \land (Q \hookrightarrow_S R) \Rightarrow (P \hookrightarrow_S R)$
  - $(P \hookrightarrow_S R) \land (Q \hookrightarrow_S R) \Rightarrow (P \lor Q \hookrightarrow_S R)$
- Reflexív, csoda kizárása teljesül rá, implikációból következik, jobbról gyengíthető, stabillal metszhető
- Általánosan diszjunktív: $(P_1 \hookrightarrow_S Q_2) \land (P_2 \hookrightarrow_S Q_2) \Rightarrow (P_1 \lor P_2 \hookrightarrow_S Q_1 \lor Q_2)$
- PSP, Progress-Safety-Progress: a stabillal metszés általánosítása
  - $(P \hookrightarrow_S Q) \land (K \rhd_S B) \Rightarrow (P \land K \hookrightarrow_S (Q \land K) \lor B)$
- Bal oldal erősíthető: $(Q \hookrightarrow_S R) \Rightarrow (P \land Q \hookrightarrow_S R)$

$\rightsquigarrow_S$, elkerülhetetlen feltétlenül pártatlan ütemezés mellett

- $\rightsquigarrow_S \equiv \hookrightarrow_S$
  - Helyes és relatívan teljes
- Definíció: $P \rightsquigarrow_S Q$ akkor és csak akkor, ha $\forall a \in P$ az S által a-hoz rendelt fákban mindegyik feltétlenül pártatlan ütemezésnek megfelelő végrehajtási úton véges távolságon belül van Q-beli csúcs
- A $\rightsquigarrow$_S a $\hookrightarrow_S$ tulajdonságok cáfolatára hasznos

$P \in inv_S(Q)$, "Q-ból indulva P invariáns"

Invariáns tulajdonság: egy meglévő program tulajdonságát vizsgáljuk. Ezzel szemben létezik invariáns kikötés is, amely egy programmal szembeni elvárás. Az invariáns tulajdonság egy biztonsági tulajdonság.

Definíció: $inv_S(\lceil Q \rceil) \subseteq \mathcal{P}(A)$: azon logikai függvények igazsághalmazainak halmaza, amelyek S-re nézve invariánsok.

A továbbiakban $inv_S(\lceil Q \rceil)$ helyett $inv_S(Q)$ jelölés lesz alkalmazva.

Alternatív definíció: $P \in inv_S(Q) \equiv Q \Rightarrow lf(s_0, P) \wedge P \Rightarrow lf(S, P)$

Ha egy állapot egy tetszőleges $P \in inv_S(Q)$ invariánson kívül van, akkor az az állapot Q-ból nem érhető el.

Megjegyzés: $inv_S(Q)$ sosem üres: $Igaz \in inv_S(Q)$

Invariánsok konjukciója: $inv_S(Q)$ zárt a $\wedge$ műveletre. Tehát $P, K \in inv_S(Q)$ esetén $(P \wedge K) \in inv_s(Q)$

Mindig igaz állítás Definíció: $P \in true_S(Q) \equiv INV_S(Q) \implies P$

Azaz $true_S(Q)$ azon halmazok, amelyek tartalmazzák a legszigorúbb invariánst.

Lemma: $inv_S(Q) \subseteq true_S(Q)$, azaz egy invariáns egyben mindig igaz állítás is.

Az invariáns alkalmas programkomponensek összeillesztésére, a mindig igaz állítások viszont nem. Ez azért van, mert a programok komponálásakor olyan állapotok elérhetővé válhatnak, amelyek korábban elérhetetlenek voltak. A mindig igaz állítások csak az (erdetileg) elérhető állapotokat vizsgálják, de az invariánsok a nem elérhető állapotokban is igazak maradnak.

Invariáns mindig igazzal elmetszve invariánst eredményez.

Legszigorúbb invariáns $INV_S(Q)$ az $inv_S(Q)$ halmaz legkisebb eleme, a legszigorúbb invariáns.

Az alábbiak megegyeznek, ekvivalensek:

- Legszigorúbb invariáns
- Legszigorúbb mindig igaz állítás
- Elérhető állapotok halmaza

Minden invariáns tartalmazza az összes elérhető állapotot, de a legszűkebb invariáns kivételével az invariánsok ezen felül további állapotokat is tartalmaznak.

$R \in FP_S$, "R teljesül fixpontban"

- $R \in FP_S \equiv \varphi_S \Rightarrow R$
- Gyengíthető: $R \Rightarrow Q \wedge R \in FP_S$ esetén $Q \in FP_S$

φ_S, fixpontok halmaza

- Egy program fixpontba jutott, ha az utasításai nem okoznak állapotátmenetet
- Elégséges feltétel determinisztikus, feltételes értékadásokból álló program esetén: $\varphi_S = \wedge_{s_i \in S} : \pi_i \to a = F_i(a)$
  - π_i a feltételes értékadás feltétele
  - a az eredeti állapot
  - $F_i(a)$ az értékadás jobb oldalán található értékek által meghatározott állapot

$Q \in TERM_S$, "Q-ból a program biztosan fixpontba jut"

- $Q \in TERM_S \equiv Q \hookrightarrow_S \varphi_S$
- Egy program biztosan fixpontba jut, ha egy alkalmas variáns függvény értéke bármely állapot elérése után elkerülhetetlenül csökken