Reguláris modellvizsgálat

Első rész

Kakuk Zsolt

kakukzs@inf.u-szeged.hu

Szegedi Tudományegyetem
Informatikai Tanszékcsoport
Számítástudomány Alapjai Tanszék
6701 Szeged Árpád tér 2.

2006. Március 27.

Tartalom

- Alapfogalmak
- Matematikai modell
- Példa
- A reguláris modellvizsgálat feladata
- Widening technikák
- Pontos widening
- Widening szituációk keresése

Alapfogalmak

Σ egy véges ábécé, Σ^* a Σ elemeiből képezhető szavak halmaza, ε jelöli az üres szót.

$R \subseteq \Sigma^* \times \Sigma^*$ hosszmegőrző, ha $\forall (w, w') \in R$-re $|w| = |w'|$.

Egy $R \subseteq \Sigma^* \times \Sigma^*$ hosszmegőrző reláció reguláris, ha az $\{(a_1, a'_1) \dots (a_n, a'_n) | (a_1 \dots a_n, a'_1 \dots a'_n) \in R\}$ halmaz reguláris $(\Sigma \times \Sigma)^*$ felett.

$R_{id} = \{(w, w) | w \in \Sigma^*\}$ az identikus reláció.

Ha R, R' reguláris relációk, akkor $R \cup R'$, $R \cap R'$ és $R \circ R'$ is azok.

R reflexív, tranzitív lezártja: $R^* = \bigcup_{i \geq 0} R^i$.

Alapfogalmak

Ha L egy tetszőleges reguláris nyelv, R pedig egy reguláris reláció, akkor

- $R(L)$ reguláris nyelv lesz, de
- $R^*(L)$ nem feltétlenül lesz az.

Például legyen $\Sigma = \{a, b\}$. Ekkor ha

- $L = (ab)^*$,
- $R = R_{id} \cdot (a, b) \cdot (b, a) \cdot R_{id} \cup R_{id} \cdot (b, a) \cdot (a, b) \cdot R_{id}$.

akkor L és R nyilván reguláris, de $R^*(L) = \{w \in \Sigma^* || w|_a = |w|_b\}$ nem az.

Matematikai modell [1]

A program egy $\mathcal{P} = \langle \Sigma, \phi_I, R \rangle$ rendszer, ahol

- Σ egy véges ábécé,
- ϕ_I egy reguláris nyelv Σ felett,
- R egy reguláris reláció Σ^* felett.

A $\mathcal{P}$ program egy konfigurációja egy $w \in \Sigma^*$ szó.

Egy $\mathcal{P} = \langle \Sigma, \phi_I, R \rangle$ programmal lehet például paraméterezett rendszereket modellezni.

Paraméterezett rendszerek tetszőleges számú folyamatból állnak, melyek lineáris elrendezésben kapcsolódnak egymáshoz. Ekkor

- Σ elemei a folyamatok lehetséges állapotai,
- ϕ_I a kezdőkonfigurációk halmaza,
- R a konfigurációk közötti váltás leírása.

Példa paraméterezett rendszerre [1]

Modellezzük a következő rendszert:

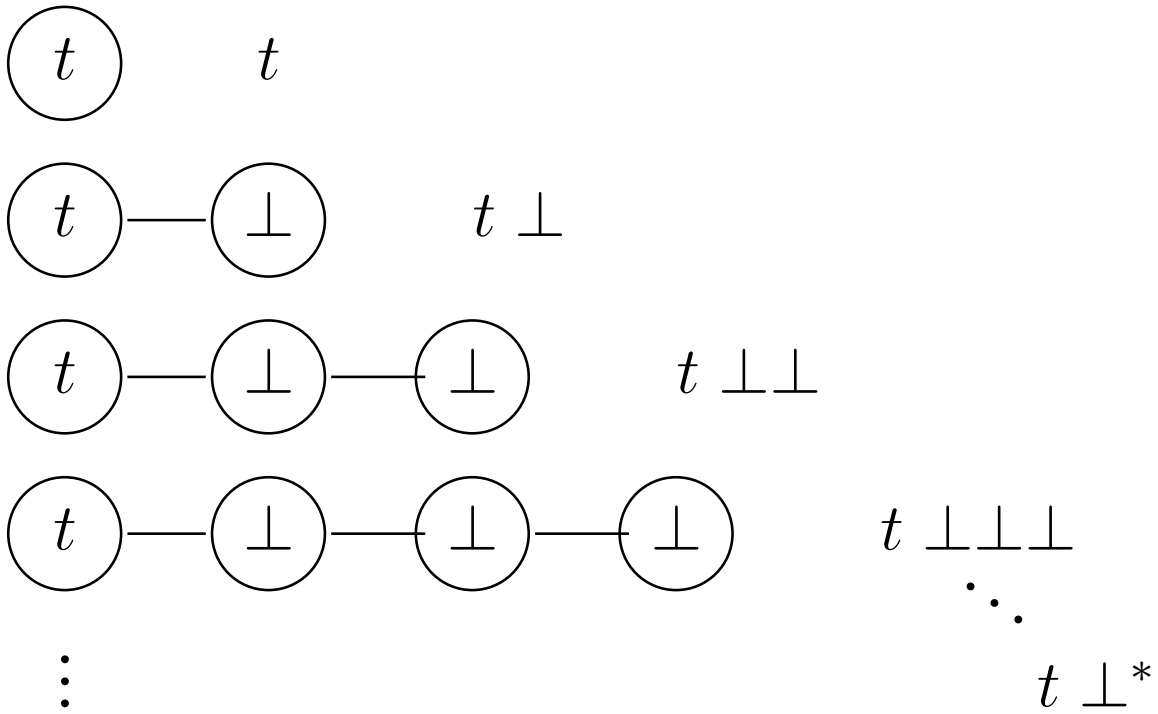
Tetszőleges számú folyamat kapcsolódhasson egymáshoz, melyek egy tokent adjanak át egymásnak balról jobbra. Kezdetben a legbaloldalibb folyamat birtokolja a tokent.

Legyen a $\mathcal{P} = \langle \Sigma, \phi_I, R \rangle$ program a következő

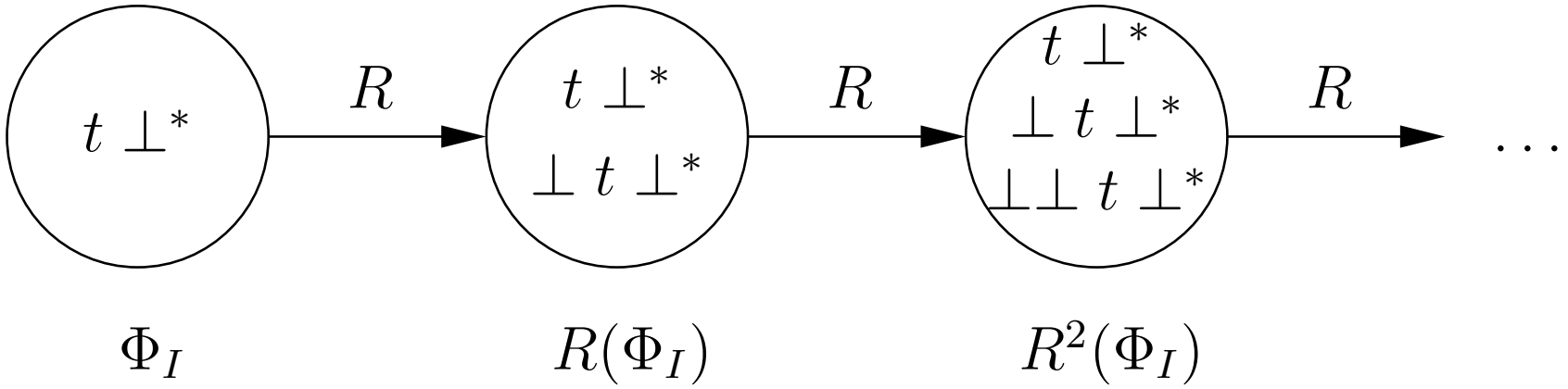
- $\Sigma = \{t, \bot\}$, ahol t jelentése, hogy a folyamat birtokolja a tokent, $\bot$ jelentése, hogy nem,
- $\phi_I = t \, \bot^*$,
- $R = (\bot, \bot)^* \cdot (t, \bot) \cdot (\bot, t) \cdot (\bot, \bot)^* \cup$ $(\bot, \bot)^* \cdot ((\bot, \bot) \cup (t, t)) \cdot (\bot, \bot)^*$.

Példa folytatása

A kezdőkonfigurációk halmaza



Példa folytatása



A reguláris modellvizsgálat feladata

Ellenőrizni, hogy az elérhető állapotokban csak a rendszer követelményeinek megfelelő konfigurációk vannak-e.

Egy $\mathcal{P} = \langle \Sigma, \phi_I, R \rangle$ program esetén igaz lesz-e, hogy $R^*(\phi) \cap \phi_E = \emptyset$, ahol ϕ_E a rossz konfigurációk halmaza.

Feladat: $R^*(\phi)$ meghatározása.

$R^*(\phi_I)$ meghatározása

- Kétféle módszer van:
  - **Az elérhetőségi halmaz kiszámítása**: Egy adott ϕ reguláris nyelv és R reguláris reláció esetén $R^*(\phi)$ meghatározása.
  - **A tranzitív lezárt kiszámítása**: Adott R reguláris reláció esetén R^+ meghatározása.
- Alkalmazható technikák $R^*(\phi)$ és R^+ kiszámítására:
  - Automata konstruálása,
  - Widening technikák.

Widening technikák [2]

Egy $\mathcal{P} = \langle \Sigma, \phi_I, R \rangle$ program helyességének vizsgálata során a widening technikák lényege, hogy $R^*(\phi)$ helyett egy bővebb $R^*(\phi) \subseteq \phi_A$ reguláris nyelvet határozunk meg (az elérhetőségi halmazt) és azt ellenőrizzük, hogy $\phi_A \cap \phi_E = \emptyset$ teljesül-e.

Widening technikák [2]

1. Elemi widening.

Ellenőrizzük, hogy léteznek-e ϕ_1, ϕ_2, Λ reguláris nyelvek, melyekre

(1) $\phi = \phi_1 \cdot \phi_2$ és $R(\phi) = \phi_1 \cdot \Lambda \cdot \phi_2$,

(2) $\phi_1 \cdot \Lambda^* \cdot \phi_2 = R(\phi_1 \cdot \Lambda^* \cdot \phi_2) \cup \phi$

Az (1) feltétel jelentése, hogy R alkalmazásának hatása ϕ-re egy Λ beszúrása ϕ_1 és ϕ_2 közé.

A (2) jelentése, hogy $R^*(\phi) \subseteq \phi_1 \cdot \Lambda^* \cdot \phi_2$. Valójában (2) jelentése, hogy $\phi_1 \cdot \Lambda^* \cdot \phi_2$ egy fixpontja az $X = R(X) \cup \phi$ egyenletnek.

Ellenőrizzük, hogy $\phi_1 \cdot \Lambda^* \cdot \phi_2 = R(\phi_1 \cdot \Lambda^* \cdot \phi_2) \cup \phi$ teljesül-e. Ha igen, akkor megállunk, egyébként újra alkalmazzuk az eljárást $\phi_1 \cdot \Lambda^* \cdot \phi_2$-re.

Ha az eljárás terminál, akkor a kapott ϕ_A halmaz $R^*(\phi)$ felső becslése.

Widening technikák [2]

Az $X = R(X) \cup \phi$ egyenletnek $R^*(\phi)$ fixpontja, hiszen

$$R^*(\phi) = R(R^*(\phi)) \cup \phi$$

Tarski fixponttétele szerint pedig $R^*(\phi)$ az $X = R(X) \cup \phi$ egyenlet legkisebb fixpontja.

A másik irányú tartalmazás: $\phi_1 \cdot \Lambda^* \cdot \phi_2 \subseteq R^*(\phi)$ nem minden esetben teljesül.

Ha (2) nem teljesül, akkor $\phi = \phi_1 \cdot \Lambda^* \cdot \phi_2$-vel kezdjük előlről feltételek ellenőrzését.

Példa elemi wideningre [2]

A korábbi példában, ha $\phi = t\ \perp^*$ és $R(\phi) = \perp\ t\ \perp^*$, akkor $R^*(\phi) = \perp^*\ t\ \perp^*$ választást végezzük, ami most pontos becslést jelent.

Ezt elmetszve a rossz konfigurációk $(t+\ \perp)^* t (t+\ \perp)^* t (t+\ \perp)^*$ halmazával az üres halmazt kapjuk, azaz a rendszer helyes.

Widening technikák [2]

2. Unary (egyszeri) widening.

Akkor használható, ha

- ϕ felírható $\phi = \phi_1 \cdot \ldots \cdot \phi_n$ alakban és,
- R egyetlen pozíción alkalmazható, és
- $R(\phi) = \bigcup_i \phi_1 \cdot \ldots \cdot \phi_i \cdot \Lambda_i \cdot \phi_{i+1} \cdot \ldots \cdot \phi_n$

Legyen $\phi' = \phi_1 \cdot \Lambda_1^* \cdot \phi_2 \cdot \ldots \cdot \phi_{n-1} \cdot \Lambda_{n-1}^* \cdot \phi_n$.

Ellenőrizzük, hogy $\phi' = R(\phi') \cup \phi$ teljesül-e. Ha igen, akkor megállunk, egyébként újra alkalmazzuk az eljárást ϕ'-re.

Ha az eljárás terminál, akkor a kapott ϕ_A halmaz $R^*(\phi)$ felső becslése.

Példa unary (egyszeri) wideningre [2]

Például, ha $\phi = a^*ba^*$ és $R = R_{id} \cdot (a, c) \cdot R_{id}$ akkor

- ϕ felírható $\phi = \phi_1 \cdot \phi_2 \cdot \phi_3$ alakban, ahol $\phi_1 = a^*$, $\phi_2 = b$, $\phi_3 = a^*$,
- $R(\phi) = a^*\underline{ca^*}ba^* + a^*b\underline{a^*c}a^*$
- $R^*(\phi) = a^*(ca^*)^*ba^* + a^*b(a^*c)^*a^* = (a + c)^*b(a + c)^*$

Widening technikák [2]

3. Regular widening.

Akkor használható, ha

- ϕ felírható $\phi = \phi_1 \cdot \ldots \cdot \phi_n$ alakban és,
- $R(\phi) = \bigcup_i \phi_1 \cdot \Lambda_{1,i} \cdot \phi_2 \cdot \Lambda_{2,i} \cdot \phi_3 \cdot \ldots \cdot \phi_{n-1} \cdot \Lambda_{n-1,i} \cdot \phi_n$

Legyen
$\phi' = \phi_1 \cdot (\sum_i \Lambda_{1,i})^* \cdot \phi_2 \cdot (\sum_i \Lambda_{2,i})^* \cdot \phi_3 \cdot \ldots \cdot \phi_{n-1} \cdot (\sum_i \Lambda_{n-1,i})^* \cdot \phi_n$.

Ellenőrizzük, hogy $\phi' = R(\phi') \cup \phi$ teljesül-e. Ha igen, akkor megállunk, egyébként újra alkalmazzuk az eljárást ϕ'-re.

Ha az eljárás terminál, akkor a kapott ϕ_A halmaz $R^*(\phi)$ felső becslése.

Példa regular wideningre [2]

Legyen $\phi = a^*b^*$, és

- $R = R_{id} \cdot ((a, c) \cdot R_{id} \cdot (b, d) + (a, e) \cdot R_{id} \cdot (b, f)) \cdot R_{id}$
- ekkor $R(\phi) = \underline{a^*c}a^*b^*\underline{db^*} + \underline{a^*e}a^*b^*\underline{fb^*}$, és
- $R^*(\phi) = \{w \in (a^*c + a^*e)^*a^*b^*(db^* + fb^*)^* || w|_c = |w|_d$ és $|w|_e = |w|_f\}$,

Widening technikák [2]

Általánosabb eset az, ha ϕ felírható $\phi_1 \cdot \phi_2 \cdot \ldots \cdot \phi_n$ alakú nyelvek véges uniójaként.

Legyen ϕ és ϕ' két reguláris nyelv. Ekkor azt mondjuk, hogy $\phi \lhd \phi'$, ha létezik két sorozat, (ϕ_i^j) és $(\Lambda_{k,i,j})$ úgy, hogy

- $\phi = \bigcup_j \phi_1^j \cdot \phi_2^j \cdot \ldots \cdot \phi_n^j$ és,
- $\phi' = \bigcup_j \bigcup_i \phi_1^j \cdot \Lambda_{1,i,j} \cdot \phi_2^j \cdot \Lambda_{2,i,j} \cdot \phi_3^j \cdot \ldots \cdot \phi_{n-1}^j \cdot \Lambda_{n-1,i,j} \cdot \phi_n^j$.

Widening technikák [2]

Definiáljuk a ∇ operátort a következőképp:

Ha $\phi \lhd \phi'$, akkor $\nabla(\phi, \phi') =$
$\bigcup_j \phi_1^j \cdot (\sum_i \Lambda_{1,i,j})^* \cdot \phi_2^j \cdot (\sum_i \Lambda_{2,i,j})^* \cdot \phi_3^j \cdot \ldots \cdot \phi_{n-1}^j \cdot (\sum_i \Lambda_{n-1,i,j})^* \cdot \phi_n^j$.

Ekkor $R^*(\phi)$ becsléséhez hasonlítsuk össze ϕ és $R(\phi)$-t.

Ha $\phi \lhd R(\phi)$, akkor legyen $\phi' = \nabla(\phi, R(\phi))$ és ellenőrizzük, hogy $\phi' = R(\phi') \cup \phi$ teljesül-e. Ha igen, akkor megállunk, egyébként újra alkalmazzuk az eljárást ϕ'-re.

Ha az eljárás terminál, akkor a kapott ϕ_A halmaz $R^*(\phi)$ felső becslése.

Pontos widening [2]

Azt mondjuk, hogy az R reláció jól megalapozott, ha nincsen szavaknak olyan végtelen $w_0, w_1, \ldots$ sorozata, melyre $\forall i \geq 0, (w_{i+1}, w_i) \in R$.

Azaz nincs ilyen: $\ldots w_2 R w_1 R w_0$.

Például a természetes számokon értelmezett $<$ reláció jól megalapozott.

Tétel [4]. Ha R jól megalapozott, akkor bármely $\phi, \phi' \subseteq \Sigma^*$ esetén $\phi' = R^*(\phi)$ akkor és csak akkor, ha $\phi' = R(\phi') \cup \phi$.

Pontos widening [2]

Ha R jól megalapozott, akkor pontos becslést tudunk adni.

Ugyanis ekkor az előző tétel szerint $\phi' = R^*(\phi)$ akkor és csak akkor, ha $\phi' = R(\phi') \cup \phi$, ami pontosan azt jelenti, hogy $R^*(\phi)$ az egyetlen fixpontja az $X = R(X) \cup \phi$ egyenletnek.

Vagyis, ha a widening technikával meghatározunk egy ϕ' fixpontot, akkor az nyilván $R^*(\phi)$-vel lesz egyenlő.

Widening szituációk felismerése [2]

Célja: adott ϕ és ϕ' reguláris nyelvekről eldönteni, hogy azok felírhatóak-e az alábbi alakban.

- $\phi = \bigcup_j \phi_1^j \phi_2^j \dots \phi_n^j$ és,
- $\phi' = \bigcup_j \bigcup_i \phi_1^j \Lambda_{1,i,j} \phi_2^j \Lambda_{2,i,j} \phi_3^j \dots \phi_{n-1}^j \Lambda_{n-1,i,j} \phi_n^j$.

Ehhez vesszük a ϕ-t és ϕ'-t felismerő automatákat:

- $\mathcal{M} = (Q, \Sigma, \delta, q_0, F)$, $L(\mathcal{M}) = \phi$,
- $\mathcal{M}' = (Q', \Sigma, \delta', q_0', F')$, $L(\mathcal{M}') = \phi'$.

Widening szituációk felismerése [2]

Megkonstruálunk egy $\mathcal{P}$ automatát, amelynek állapothalmaza $Q \times Q'$. Kezdőállapota (q_0, q_0') és párhuzamosan szimuláljuk $\mathcal{M}$ és $\mathcal{M}'$ működését.

Minden elérhető (q, q') állapot esetén nemdeterminisztikusan döntünk, hogy folytatjuk a szimulációt $\mathcal{M}$-ben és $\mathcal{M}'$-ben is vagy $\mathcal{M}$-ben megállunk és csak $\mathcal{M}'$ haladunk tovább.

Mivel $\mathcal{P}$ nemdeterminisztikus ezért egy (w, w') bemenet esetén több felismerő futása is lehet, melyek az alábbi alakúak:

$$p = (q_0, q_0') \xrightarrow{*} (q_1, q_1') \xrightarrow{*} (q_1 = q_2, q_2') \xrightarrow{*} (q_3, q_3') \xrightarrow{*} (q_3 = q_4, q_4') \xrightarrow{*} \cdots \xrightarrow{*} (q_F, q_F')$$

ahol $q_F \in F$, $q_F' \in F'$

Widening szituációk felismerése [2]

Ekkor $k \geq 1$-re a $\mathcal{P}$ automata felismeri

- ϕ_k^j-t , ha a kezdőállapotának $(q_{2(k-1)}, q'_{2(k-1)})$-t, végállapotának (q_{2k-1}, q'_{2k-1})-t választjuk,
- $\Lambda_{k,i,j}$-t , ha a kezdőállapotának (q_{2k-1}, q'_{2k-1})-t, végállapotának (q_{2k-1}, q'_{2k})-t választjuk

Ezzel a módszerrel az összes lehetséges felbontását megkapjuk a ϕ és ϕ' nyelveknek.

Hivatkozások

[1] A. Bouajjani, B. Jonsson, M. Nilsson, T. Touili, Regular Model Checking, In *12th Intern. Conf. on Computer Aided Verification (CAV'00).*, LNCS vol. 1855, pages 403-418, Springer-Verlag, 2000.

[2] T. Touili, Regular Model Checking using Widening Techniques, *Electronic Notes in Theoretical Computer Science 50 No. 4*, pages 342-356, 2001.

[3] P. A. Abdulla, B. Jonsson, P. Mahata, J. d'Orso, Regular Tree Model Checking, *In Proc. 14th Int. Conf. on Computer Aided Verification*, LNCS vol. 2404, pages 555-568, 2002.

[4] L. Fribourg and H. Olsen, Reachability Sets of Parametrized Rings As Regular Languages, Pre-proceedings of Infinity'97, UPMAIL Technical Report 148, pages 115-138, July 1997.