Reguláris modellvizsgálat
Kakuk Zsolt

A modellvizsgálat célja nagy, folyamatosan működő rendszerek, protokollok helyességének vizsgálata. A helyességvizsgálat során ezúttal egy olyan program helyességét ellenőrizzük, amellyel lineáris topológiában egymáshoz kapcsolódó folyamatok (processzek) működését lehet leírni. Programnak egy $\mathcal{P} = \langle \Sigma, \phi_I, R \rangle$ rendszert nevezünk, ahol Σ egy véges ábécé, ami tartalmazza a folyamatok lehetséges állapotait. Egy $w \in \Sigma^*$ szó a rendszer egy konfigurációjának felel meg, ahol w i-edik betűje az i-edik folyamat állapotát adja meg. Továbbá, $\phi_I \subseteq \Sigma^*$ nyelv a kezdő konfigurációk halmaza, $R \subseteq \Sigma^* \times \Sigma^*$ pedig egy reláció, amely a vizsgált rendszer átmeneteit írja le. Mivel a $\mathcal{P}$ program által modellezett rendszerben lévő processzek száma nincs korlátozva, ezért ϕ_I általában végtelen nyelv lesz. A reguláris modellvizsgálat elnevezés onnan származik, hogy feltételezzük, hogy ϕ_I reguláris nyelv, R pedig reguláris reláció. 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.

A vizsgált rendszer működését az $R(\phi_I)$, $R^2(\phi_I), R^3(\phi_I), \dots$ reguláris nyelvekből álló sorozat írja le. A rendszer akkor működik helyesen, ha az elérhető konfigurációk $R^*(\phi_I)$ halmaza nem tartalmaz "rossz" konfigurációt, azaz $R^*(\phi_I) \cap \phi_E = \emptyset$, ahol $R^* = \bigcup_{i \geq 0} R^i$ és ϕ_E a rossz konfigurációk halmaza.

A probléma az, hogy már akár egész egyszerű esetben sem lesz $R^*(\phi_I)$ reguláris nyelv, és ezért az $R(\phi_I), R^2(\phi_I), \dots$ sorozat nem konvergál. Ezért olyan technikát alkalmazunk, amely egy olyan reguláris ϕ_A nyelvet határoz meg, amely az $R^*(\phi_I)$ nyelv felső becslése. Így, amennyiben $\phi_A \cap \phi_E$ is üres, a rendszer helyesen működik.

Ezt a technikát widening technikának hívjuk, amelynek lényege, hogy a ϕ és $R(\phi)$ nyelveket összehasonlítjuk egy adott ϕ reguláris nyelv esetén. Ezzel azt próbáljuk megsejteni, hogy R alkalmazása hogyan változtatja meg a ϕ nyelvet. Például, ha ϕ felírható $\phi = \phi_1 \cdot \phi_2$ alakban és $R(\phi) = \phi_1 \cdot \Lambda \cdot \phi_2$, akkor feltételezzük, hogy R mindig egy Λ nyelvet szúr be ϕ_1 és ϕ_2 közé. Ezért a ϕ_A halmazhoz hozzávesszük $\phi_1 \cdot \Lambda^* \cdot \phi_2$-t, majd ellenőrizzük, hogy ϕ_A fixpont-e, azaz megegyezik-e $R(\phi_A) \cup \phi$-vel. Ha igen megállunk, ha nem akkor további lépéseket teszünk.

Bizonyos esetekben ez a becslés pontos lesz, azaz $\phi_A = R^*(\phi_I)$. Az előbbi példán kívűl még számos esetet megvizsgálunk. Szó lesz arról is, hogy mely esetben kapjuk meg pontosan az $R^*(\phi_I)$ nyelvet. Megvizsgáljuk, hogyan lehet eldönteni, hogy alkalmazható-e valamely widening technika.

Egy másik módszer az elérhető állapotok $R^*(\phi_I)$ halmazának meghatározására, ha adunk egy automatát, amely R^+-t számolja ki. A folyamatok lineáris topológiájának általánosításaként fastruktúrában elrendezett processzeket is modellezhetünk így fákra is kiterjeszthetünk néhány eredményt. Ezekről az előadás második részében lesz szó.

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.