Modely konkurentných systémov
Formálne metódy tvorby softvéru

Damas Gruska

Katedra aplikovanej informatiky, I20, gruska@fmph.uniba.sk

Prednáška 11.

Verifikácia temporálnych vlastností

Chceme zistiť či systém P ma vlastnosť Φ.

Nepriama možnosť:

na to či $P \models \Phi$ využijeme $||\Phi||^{\mathcal{P}}$ t.j. množinu všetkých procesov z $\mathcal{P}$, ktoré spĺňajú Φ.

a overíme pre $P \in \mathcal{P}$ či $P \in ||\Phi||^{\mathcal{P}}$

Schodná cesta pre malé $\mathcal{P}$

Ďalšou možnosťou je využiť aproximácie tak ako bolo spomenuté v predchádzajúcom.

Hry

Hráč 1 a Hráč 2

Hráč 1 sa snaží ukázať, že $P \not\models \Phi$

Hráč 2 sa snaží ukázať, opak, t.j. že $P \models \Phi$

Ak existuje víťazná stratégia pre Hráča 2 (vie vyhrať každú hru) tak $P \models \Phi$.

Verifikácia temporálnych vlastností

Hra so začiatkom (P_0, Φ_0) je konečná alebo nekonečná postupnosť

$$(P_0, \Phi_0), (P_1, \Phi_1), \ldots, (P_n, \Phi_n), \ldots$$

V stave (P_j, Φ_j) ťahá Hráč 1 alebo Hráč 2 v závislosti od Φ_j.

Hráč 1 ťahá ak Φ_j má najvrchnejší operátor $\wedge, [K], \nu Z.\Psi$

Hráč 2 ťahá ak Φ_j má najvrchnejší operátor $\vee, < K >, \mu Z.\Psi$

Verifikácia temporálnych vlastností

Nech počiatočná časť hry je:

$$(P_0, \Phi_0), (P_1, \Phi_1), \ldots, (P_j, \Phi_j)$$

Ak $\Phi_j = \Psi_1 \wedge \Psi_2$ tak ťahá Hráč 1 a vyberie Ψ_i pre $i = 1$ alebo $i = 2$ a $P_{j+1} = P_j, \Phi_{j+1} = \Psi_i$.

Ak $\Phi_j = \Psi_1 \vee \Psi_2$ tak ťahá Hráč 2 a vyberie Ψ_i pre $i = 1$ alebo $i = 2$ a $P_{j+1} = P_j, \Phi_{j+1} = \Psi_i$.

Ak $\Phi_j = [K]\Psi$ tak ťahá Hráč 1 a vyberie prechod $P_j \xrightarrow{y} P', y \in K$ a zvolí $\Phi_{j+1} = \Psi, P_{j+1} = P'$.

Ak $\Phi_j =< K > \Psi$ tak ťahá Hráč 2 a vyberie prechod $P_j \xrightarrow{y} P', y \in K$ a zvolí $\Phi_{j+1} = \Psi, P_{j+1} = P'$.

Verifikácia temporálnych vlastností

Ak $\Phi_j = \nu Z.\Psi$ tak ťahá Hráč 1 a vyberie novú konštantu U, definuje $U \stackrel{def}{=} \nu Z.\Psi$ a $P_{j+1} = P_j, \Phi_{j+1} = U$.

Ak $\Phi_j = \mu Z.\Psi$ tak ťahá Hráč 2 a vyberie novú konštantu U, definuje $U \stackrel{def}{=} \mu Z.\Psi$ a $P_{j+1} = P_j, \Phi_{j+1} = U$.

Ak $\Phi_j = U$ a $U = \nu Z.\Psi$ a pre žiadne $k < j, P_k = P_j, \Phi_k = \Phi_j$ tak Hráč 1 rozvinie prevný bod t.j. $P_{j+1} = P_j, \Phi_{j+1} = \Psi[U/Z]$.

Ak $\Phi_j = U$ a $U = \mu Z.\Psi$ a pre žiadne $k < j, P_k = P_j, \Phi_k = \Phi_j$ tak Hráč 2 rozvinie prevný bod t.j. $P_{j+1} = P_j, \Phi_{j+1} = \Psi[U/Z]$.

Pravidlá sú spätne zdravé, t.j.:

ak Hráč 1 urobí ťah z j do $j+1$ tak ak $P_{j+1} \not\models \Phi_{j+1}$ potom $P_j \not\models \Phi_j$,

ak Hráč 2 urobí ťah z j do $j+1$ tak ak $P_{j+1} \models \Phi_{j+1}$ potom $P_j \models \Phi_j$.

Hráč vyhráva, ak oponent nemôže ťahať.

Hráč 1 nemôže ťahať ak v konfigurácií $\Phi_j = [K]\Psi$ neexistuje prechod $P_j \xrightarrow{y} P', y \in K$.

Hráč 2 nemôže ťahať ak v konfigurácií $\Phi_j =< K > \Psi$ neexistuje prechod $P_j \xrightarrow{y} P', y \in K$.

Verifikácia temporálnych vlastností

$$\vdots$$
$$U \stackrel{def}{=} \nu Z.\Psi$$
$$P_k$$
$$(P_k, U)$$
$$\vdots$$
$$(P_j, U)$$
$$P_k = P_j$$

Hráč 2 vyhráva

$$\vdots$$
$$U \stackrel{def}{=} \mu Z.\Psi$$
$$P_k$$
$$(P_k, U)$$
$$\vdots$$
$$(P_j, U)$$
$$P_k = P_j$$

Hráč 1 vyhráva

Verifikácia temporálnych vlastností

Prípad nekonečných hier:

$\vdots$	$\vdots$
$U \stackrel{def}{=} \nu Z.\Psi$	$U \stackrel{def}{=} \mu Z.\Psi$
P_k	P_k
(P_k, U)	(P_k, U)
$\vdots$	$\vdots$
(P_j, U)	(P_j, U)
$\vdots$	$\vdots$
(P_n, U)	(P_n, U)
Hráč 2 vyhráva	Hráč 1 vyhráva

Verifikácia temporálnych vlastností

Theorem

$P \models \Phi$ *iff Hráč 2 má víťaznú stratégiu v hre s počiatkom* (P, Φ).

Príklad.

$$Cl''' = tick.Cl''' + tick.Nil$$
$$\Phi = \nu Z. < tick > .Z$$

$$
\begin{array}{l}
(Cl''', \nu Z. < tick > .Z) \\
\qquad \downarrow 1 \\
(Cl''', U) \\
\qquad \downarrow 1 \\
(Cl''', < tick > .U) \\
\qquad \downarrow 2 \\
(Cl''', U)
\end{array}
$$

Hráč 2 vyhráva.

Príklad.

$$Cl''' = tick.Cl''' + tick.Nil$$
$$\Phi = \mu Z.[tick].Z$$

$$\begin{array}{l} (Cl''', \mu Z.[tick].Z) \\ \qquad \downarrow 2 \\ (Cl''', U) \\ \qquad \downarrow 2 \\ (Cl''', [tick].U) \\ \qquad \downarrow 1 \\ (Cl''', U) \end{array}$$

Hráč 1 vyhráva.

Tablový dokazovací systém

Dokazujeme, že Hráč 2 má víťaznú stratégiu.

$P \vdash \Phi$ synatktická obdoba $P \models \Phi$

Dokazovacie pravidlá:

$$\frac{P \vdash \Phi}{P_1 \vdash \Phi_1, \dots, P_n \vdash \Phi_n}$$

$P \vdash \Phi$ - cieľ
$P_i \vdash \Phi_i$ - podciele
môže to mať aj vedľajšie podmienky.

Tablový dokazovací systém

$$\frac{P \vdash \Phi \wedge \Psi}{P \vdash \Phi, P \vdash \Psi}$$

$$\frac{P \vdash \Phi \vee \Psi}{P \vdash \Phi}$$

$$\frac{P \vdash \Phi \vee \Psi}{P \vdash \Psi}$$

Tablový dokazovací systém

$$\frac{P \vdash [K]\Psi}{P_1 \vdash \Psi, \ldots, P_n \vdash \Psi} \quad \{P' | P \xrightarrow{y} P', y \in K\} = \{P_1, \ldots, P_n\}$$

$$\frac{P \vdash < K > \Psi}{P' \vdash \Psi} \quad P \xrightarrow{y} P', y \in K$$

Tablový dokazovací systém

$$\frac{P \vdash \sigma Z.\Psi}{P \vdash U} \quad U \stackrel{def}{=} \sigma Z.\Psi \text{ a } U \text{ je nová konštanta}$$

$$\frac{P \vdash U}{P \vdash \Psi[U/Z]} \quad U \stackrel{def}{=} \sigma Z.\Psi$$

Tablový dokazovací systém

Systém je spätne zdravý.

Ak platí záver, tak platí i predpoklad.

Ak chceme zistiť či $P \models \Phi$ tak vytvoríme tablo pre cieľ $P \vdash \Phi$.

Vznikne strom s koreňom $P \vdash \Phi$. Ak je konečný a listy sú true, tak true je i cieľ.

Predchádzajúce pravidlá aplikujeme len na vrcholy, ktoré nie sú terminálne.

Tablový dokazovací systém

Vrchol $P \vdash \Psi$ je terminálny ak platí jedna z nasledujúcich podmienok:

Úspešná terminácia
1. $\Psi = [K]\Phi$ a $\{P' | P \xrightarrow{y} P', y \in K\} = \emptyset$
2. $\Psi = U$ a $U = \nu Z.\Phi$ a existuje vrchol vyššie $P \vdash \Psi$

Neúspešná terminácia
1'. $\Psi =< K > \Phi$ a $\{P' | P \xrightarrow{y} P', y \in K\} = \emptyset$
2'. $\Psi = U$ a $U = \mu Z.\Phi$ a existuje vrchol vyššie $P \vdash \Psi$

Tablový dokazovací systém

Definition

Úspešné tablo pre $P \vdash \Psi$ je konečný strom s koreňom $P \vdash \Psi$ a všetkými listami s úspešnou termináciou.

Theorem

Ak $P \vdash \Psi$ má úspešné tablo tak potom $P \models \Psi$.

Tablový dokazovací systém

Príklad.

$Cl = tick.Cl$
$\Phi = \nu Z. < tick > .Z$

$$\dfrac{Cl \vdash \nu Z. < tick > .Z}{Cl \vdash U} \quad U \stackrel{def}{=} \nu Z. < tick > Z \text{ a } U \text{ je nová konštanta}$$

$$\dfrac{}{Cl \vdash < tick > U}$$

$$\dfrac{}{Cl \vdash U}$$

Príklad.

$$Cl = tick.Cl$$
$$\Phi = \nu Z.(([-tick]ff \wedge < - > tt) \wedge [-].Z)$$

$$\dfrac{Cl \vdash \nu Z.(([-tick]ff \wedge < - > tt) \wedge [-].Z)}{Cl \vdash U} \quad U \stackrel{def}{=} \nu Z.(([-tick]ff \wedge < - > tt) \wedge [-].Z)$$

$$\dfrac{Cl \vdash U}{Cl \vdash ([-tick]ff \wedge < - > tt) \wedge [-].U}$$

$$\dfrac{Cl \vdash ([-tick]ff \wedge < - > tt) \wedge [-].U}{Cl \vdash [-tick]ff \wedge < - > tt \qquad Cl \vdash [-].U}$$

$$\dfrac{Cl \vdash [-tick]ff \wedge < - > tt}{Cl \vdash [-tick]ff \qquad Cl \vdash < - > tt} \qquad \dfrac{Cl \vdash [-].U}{Cl \vdash U}$$

$$\dfrac{Cl \vdash < - > tt}{Cl \vdash tt}$$

Tablový dokazovací systém

Theorem

Ak P má konečne veľa stavov a $P \models \Psi$ potom $P \vdash \Psi$ má úspešné tablo.

Parity game pre konečnostavové systémy

Parity game je orientovaný graf $G = (N, \rightarrow, L)$ kde

množina vrcholov N je konečná podmnožina množiny prirodzených čísel,

$\rightarrow$ reprezentuje hrany (budeme písať $i \rightarrow j$ miesto $(i, j) \in \rightarrow$)

Vrcholy sú pozície v hre.

$L(i)$ hovorí, ktorý hráč je na ťahu.

Predpokladáme, že z každého vrcholu vedie aspoň jedna hrana. (hra má nekonečnú dĺžku)

Hra začína v najmenšom vrchole.

Hráč, ktorý je na ťahu vyberie nasledujúcu "vychádzajúcu" pozíciu.

Hra je nekonečná, víťaz sa určí podľa najmenšieho vrcholu, ktorý sa vyskytuje nekonečne veľa krát v hre podľa L.

Parity game

Ideme ukázať $E \models_{\upsilon} \Phi$

Nech $\{E_1, \ldots, E_m\} = P(E)$ a $E_1 = E$.

Nech $Z_1, \ldots, Z_k$ sú všetky viazané premenné v Φ.

Nech $\Phi_1, \ldots, \Phi_l$ je množina podformúl Φ, okrem propozičných premenných, zoradených od najväčšej t.j. $\Phi = \Phi_1$.

Do tohoto zoznamu vložíme Z_i za $\sigma Z_i.\Psi_i$, takto dostaneme zoznam $\Phi_1, \ldots, \Phi_n$

Pozície v hre sú dvojice

$$(E_1, \Phi_1), \ldots, (E_m, \Phi_1), (E_1, \Phi_2), \ldots, (E_1, \Phi_n) \ldots, (E_m, \Phi_n)$$

Množina vrcholov je $\{1, \ldots, m \times n\}$
Každý vrchol $i = m \times (k-1) + j$ reprezentuje (E_j, Φ_k).

Parity game

Ideme teraz definovať $\rightarrow$ a L pre pozíciu (F, Ψ) reprezentujúcu i.

Ak Ψ je Z a Z je voľná v pôvodnej formule a $F \in \upsilon(Z)$ tak $L(i) = H2$ a existuje hrana $i \rightarrow i$. Ak $F \notin \upsilon(Z)$ tak $L(i) = H1$ a existuje hrana $i \rightarrow i$

Ak Ψ je tt tak $L(i) = H2$ a existuje hrana $i \rightarrow i$.

Ak Ψ je ff tak $L(i) = H1$ a existuje hrana $i \rightarrow i$.

Parity game

Ak Ψ je $\Psi_1 \wedge \Psi_2$ tak $L(i) = H1$ a existujú hrany $i \rightarrow j1$ a $i \rightarrow j2$ kde $j1$ reprezentuje (F, Ψ_1) a $j2$ reprezentuje (F, Ψ_2) .

Ak Ψ je $\Psi_1 \vee \Psi_2$ tak $L(i) = H2$ a existujú hrany $i \rightarrow j1$ a $i \rightarrow j2$ kde $j1$ reprezentuje (F, Ψ_1) a $j2$ reprezentuje (F, Ψ_2) .

Ak Ψ je $< K > \Psi'$ a $\{F' | F \xrightarrow{x} F', x \in K\} = \emptyset$ tak $L(i) = H1$ a existuje hrana $i \rightarrow i$

Ak Ψ je $< K > \Psi'$ a $\{F' | F \xrightarrow{x} F', x \in K\} \neq \emptyset$ tak $L(i) = H2$ a existuje hrana $i \rightarrow j$ pre každé j reprezentujúce pozíciu (F', Ψ') pre $F \xrightarrow{x} F'$ a $x \in K$.

Parity game

Ak Ψ je $[K]\Psi'$ a $\{F' | F \xrightarrow{x} F', x \in K\} = \emptyset$ tak $L(i) = H2$ a existuje hrana $i \rightarrow i$

Ak Ψ je $[K]\Psi'$ a $\{F' | F \xrightarrow{x} F', x \in K\} \neq \emptyset$ tak $L(i) = H1$ a existuje hrana $i \rightarrow j$ pre každé j reprezentujúce pozíciu (F', Ψ') pre $F \xrightarrow{x} F'$ a $x \in K$.

Ak Ψ je $\nu Z_j.\Psi_j$ tak $L(i) = H2$ a existuje hrana $i \rightarrow j'$ kde j' reprezentujúce pozíciu (F, Z_j).

Ak Ψ je $\mu Z_j.\Psi_j$ tak $L(i) = H1$ a existuje hrana $i \rightarrow j'$ kde j' reprezentujúce pozíciu (F, Z_j).

Parity game

Ak Ψ je Z_j a $\nu Z_j.\Psi_j$ je podformula Φ, tak $L(i) = H2$ a existuje hrana $i \rightarrow j'$ kde j' reprezentujúce pozíciu (F, Ψ_j).

Ak Ψ je Z_j a $\mu Z_j.\Psi_j$ je podformula Φ, tak $L(i) = H1$ a existuje hrana $i \rightarrow j'$ kde j' reprezentujúce pozíciu (F, Ψ_j).

Odstránime vrcholy, ktoré nie sú dosiahnuteľné z počiatočného vrcholu.

Parity game

Najmenší vrchol, ktorý sa vyskytne nekonečne veľa krát v hre, má jeden z tvarov:

(F, Z) kde Z je voľná.

(F, tt)

(F, ff)

$(F, [K]\Psi)$ a $\{F' | F \xrightarrow{x} F', x \in K\} = \emptyset$

$(F, < K > \Psi)$ a $\{F' | F \xrightarrow{x} F', x \in K\} = \emptyset$

(F, Z_j)