Modely konkurentných systémov
Formálne metódy tvorby softvéru

Damas Gruska

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

Prednáška 9.

Modálna logika: Hennessy - Milner logika

$$\Phi ::= true|false|\Phi_1 \wedge \Phi_2|\Phi_1 \vee \Phi_2|[K]\Phi| < K > \Phi$$

kde $K \subseteq Act$ a Act je množina akcií.

skratky: *tt* za *true* a *ff* za *false*

$P \models tt$
$P \not\models ff$
$P \models \Phi_1 \vee \Phi_2$ iff $P \models \Phi_1$ alebo $P \models \Phi_2$
$P \models \Phi_1 \wedge \Phi_2$ iff $P \models \Phi_1$ a $P \models \Phi_2$
$P \models [K]\Phi$ iff $\forall R \in \{P'|P \xrightarrow{x} P', x \in K\}$ platí $R \models \Phi$
$P \models < K > \Phi$ iff $\exists R \in \{P'|P \xrightarrow{x} P', x \in K\}$ také, že $R \models \Phi$

Hennessy - Milner logika

Skratky:

$-K$ miesto $Act \setminus K$
$-a_1, \ldots, a_n$ miesto $-\{a_1, \ldots, a_n\}$
$-$ miesto $-\emptyset$

$[-]ff$ - deadlock

$Nil \models [-]ff$

P môže vykonať a a len a:
$P \models < - > tt \wedge [-a]ff$

$(K)\Phi \stackrel{def}{=} < K > tt \wedge [-K]ff \wedge [-]\Phi$
len K akcie sa môžu vykonať a po vykonaní K akcie výsledok spĺňa Φ

Ako ďalšia akcia sa musí vykonať a:

$(a)tt$

$P \models (a)tt$ iff $\exists R \in \{P' | P \xrightarrow{a} P'\}$ a $\{P' | P \xrightarrow{b} P', a \neq b\} = \emptyset$

Hennessy - Milner logika

Rozšírenie:

$P \models [|\ \ |]\Phi$ iff $\forall R \in \{P' | P \Rightarrow P'\}\ \ R \models \Phi$

$P \models << \ \ >> \Phi$ iff $\exists R \in \{P' | P \Rightarrow P'\}\ \ R \models \Phi$

$[|\ \ |]$ a $<< \ \ >>$ sa nedajú nahradiť pomocou $[\ \ ]$ a $< \ \ >$.

Hennessy - Milner logika

Nech

$$\begin{aligned} D_0 &\stackrel{def}{=} \tau.Nil \\ D_{i+1} &\stackrel{def}{=} \tau.D_i \\ D_0^a &\stackrel{def}{=} a.Nil \\ D_{i+1}^a &\stackrel{def}{=} \tau.D_i^a \end{aligned}$$

Nech veľkosť formuly ψ ($|\psi|$) je počet výskytov $\vee, \wedge, [K], < K >$.

Theorem

Nech $|\psi| = n$ (ψ neobsahuje $[| \ \ |]$ a $<< \ \ >>$). Potom pre každé m, $m \geq n$

$$D_m \models \psi \text{ iff } D_m^a \models \psi$$

Modálna logika

Definujme nové modálne operátory

$K, K \subseteq A \; (Act = A \cup \{\tau\})$

$[|K|]\Phi \stackrel{def}{=} [| \;\; |][K][| \;\; |]\Phi$

$<< K >> \Phi \stackrel{def}{=} << \;\; >>< K ><< \;\; >> \Phi$

$P \models [|K|]\Phi \text{ iff } \forall R \in \{P' | P \stackrel{a}{\Rightarrow} P', a \in K\} \;\; R \models \Phi$

$P \models << K >> \Phi \text{ iff } \exists R \in \{P' | P \stackrel{a}{\Rightarrow} P', a \in K\} \;\; R \models \Phi$

Modálna logika

P môže vykonať a a len a:
$P \models < - > tt \wedge [-a]ff$
obdoba $<< - >> tt \wedge [| - a|]ff$

Nech:
$Cl = tick.Cl$
$Cl' = tick.Cl' + \tau.Nil$

$Cl' \models << - >> tt \wedge [| - tick|]ff$
ale Cl' sa môže dostať do deadlocku, t.j.

$Cl' \not\models [| \; |] << - >> tt$

Vylepšíme to formulou $\Phi = [| \; |] << - >> tt \wedge [| - tick|]ff$

$Cl \models \Phi$
$Cl' \not\models \Phi$

Modálna logika

Nech:
$Cl'' = tick.Cl'' + \tau.Cl''$

$Cl'' \models \Phi$

ale Cl'' nemusí nikdy vykonať *tick*.

Proces diverguje ak môže stále vykonávať interné τ akcie ($P \uparrow$).
Proces konverguje ak nediverguje ($P \downarrow$).

$Cl' \downarrow$ a $Cl'' \uparrow$

Zatiaľ toto nevieme vyjadriť modálnou logikou.

Modálna logika

Zavedieme nové operátory.

$P \models [| \downarrow |]\Phi$ iff $P \downarrow$ a $\forall R \in \{P' | P \stackrel{\tau}{\Rightarrow} P'\}\ \ R \models \Phi$

$P \models [| \downarrow K|]\Phi$ iff $P \downarrow$ a $\forall R \in \{P' | P \stackrel{a}{\Rightarrow} P', a \in K\}\ \ R \models \Phi$

Modálna logika

kombinácie:

$[|K \downarrow|]$ $\ldots$ $[|\ \ |][K][|\downarrow|]$

$[|\downarrow K \downarrow|]$ $\ldots$ $[|\downarrow|][K][|\downarrow|]$

To čo sme chceli pôvodne vyjadriť je teda:

$\Phi' = [|\downarrow|] << - >> tt \wedge [|-tick|]ff$

$Cl \models \Phi'$ a $Cl'' \not\models \Phi'$

Modálna logika

Nech

$$\begin{aligned} Cl^0 &\stackrel{def}{=} Nil \\ Cl^{i+1} &\stackrel{def}{=} tick.Cl^i \end{aligned}$$

a
$P \stackrel{def}{=} \sum_{i \geq 0} Cl^i$ a $R \stackrel{def}{=} P + Cl$

Potom $P \not\sim R$ ale nedajú sa rozlíšiť žiadnou formulou, t.j. $\forall \Phi$ platí $P \models \Phi$ iff $R \models \Phi$.

Definition

Proces P voláme bezprostredne image finite ak množina $\{P'|P \xrightarrow{x} P', x \in Act\}$ je konečná.
Proces voláme image finite ak každý proces z $\{P'|P \xrightarrow{s} P', s \in Act^*\}$ je bezprostredne image finite.

Theorem

Ak P, Q sú image finite a $\forall\Phi$ platí $P \models \Phi$ iff $R \models \Phi$ potom $P \sim R$.

Temporálne vlastnosti

Pomocou predchádzajúcich modálnych formúl nevieme vyjadriť vlastnosti, ako:

- akcia x je vždy možná,
- akcia x sa raz musí vykonať,
- ak sa raz vykoná akcia x, tak potom sa raz bude môcť vykonať akcia y.

Definujme:

$$||\Phi||^{\mathcal{E}} = \{P \in \mathcal{E} | P \models \Phi\}$$

t.j. podmnožina $\mathcal{E}$, ktorá spĺňa Φ.

Temporálne vlastnosti

Priama definícia:

$$
\begin{aligned}
||tt||^{\mathcal{E}} &\stackrel{def}{=} \mathcal{E} \\
||ff||^{\mathcal{E}} &\stackrel{def}{=} \emptyset \\
||\Phi \wedge \Psi||^{\mathcal{E}} &\stackrel{def}{=} ||\Phi||^{\mathcal{E}} \cap ||\Psi||^{\mathcal{E}} \\
||\Phi \vee \Psi||^{\mathcal{E}} &\stackrel{def}{=} ||\Phi||^{\mathcal{E}} \cup ||\Psi||^{\mathcal{E}}
\end{aligned}
$$

Temporálne vlastnosti

Zavedieme zobrazenie:

$$||\sharp||^{\mathcal{E}} : 2^{\mathcal{E}} \rightarrow 2^{\mathcal{E}}$$

pre $\sharp \in \{[K], < K >, [| \ \ |], << \ \ >>, [| \downarrow |]\}$.

$$||\sharp\Phi||^{\mathcal{E}} = ||\sharp||^{\mathcal{E}} ||\Phi||^{\mathcal{E}}$$

$$||[K]||^{\mathcal{E}}(X) = \{P \in \mathcal{E} | \text{ ak } P \xrightarrow{y} P' \text{ a } y \in K \text{ tak } P' \in X\}$$

$$|| < K > ||^{\mathcal{E}}(X) = \{P \in \mathcal{E} | \text{ existuje } P' \in X, \text{ existuje } y \in K \text{ a } P \xrightarrow{y} P'\}$$

Temporálne vlastnosti

Príklad:
$Cl_1 = tick.tak.Cl_1$
$\mathcal{E} = \{Cl_1, tak.Cl_1\}$

$$|| < K > ||^{\mathcal{E}}(X) = \{P \in \mathcal{E}| \text{ existuje } P' \in X, \text{ existuje } y \in K \text{ a } P \stackrel{y}{\rightarrow} P'\}$$

$$\begin{aligned} || < tick > tt||^{\mathcal{E}} &= || < tick > ||^{\mathcal{E}} ||tt||^{\mathcal{E}} \\ &= || < tick > ||^{\mathcal{E}} \mathcal{E} \\ &= \{P \in \mathcal{E}| \text{ existuje } P' \in \mathcal{E}, P \stackrel{tick}{\rightarrow} P'\} \\ &= \{Cl_1\} \end{aligned}$$

Temporálne vlastnosti

Množina procesov $\mathcal{E}$ je transition closed ak

$$\text{ak } P \in \mathcal{E} \text{ a } P \xrightarrow{x} P' \text{ tak } P' \in \mathcal{E}$$

$\mathcal{P}$ - bude neprázdna transition closed množina procesov.
$\mathcal{P}(\mathcal{E})$ - bude najmenšia transition closed množina procesov obsahujúca $\mathcal{E}$.

Theorem

Ak $P \in \mathcal{P}$ tak $P \in ||\Phi||^{\mathcal{P}}$ iff $P \models \Phi$.

Temporálne vlastnosti

Theorem

Nech $\mathcal{E} \subseteq \mathcal{F}$. *Potom*

$$\begin{aligned} ||\Phi||^{\mathcal{P}} \cap \mathcal{E} &\subseteq ||\Phi||^{\mathcal{P}} \cap \mathcal{F} \\ ||\Phi||^{\mathcal{P}} \cup \mathcal{E} &\subseteq ||\Phi||^{\mathcal{P}} \cup \mathcal{F} \\ ||\sharp||^{\mathcal{P}} \mathcal{E} &\subseteq ||\sharp||^{\mathcal{P}} \mathcal{F} \end{aligned}$$

Temporálne vlastnosti

Majme reťazec podmnožín $\mathcal{P} = \{\mathcal{E}_i \subseteq \mathcal{P} | i \geq 0, \mathcal{E}_i \subseteq \mathcal{E}_j$ ak $i < j\}$.

$||\sharp||^{\mathcal{P}}$ je spojitý, ak pre každý takýto reťazec platí:

$$||\sharp||^{\mathcal{P}} \bigcup \mathcal{E}_i = \bigcup ||\sharp||^{\mathcal{P}} \mathcal{E}_i$$

.

Temporálne vlastnosti

Nech $\mathcal{P} = \{Cl^i, Cl | i \geq 0\}$.

Cl je rôzne od ostatných v $\mathcal{P}$ tým, že vie urobiť ľubovoľne veľa krát *tick*. Táto vlastnosť rozdeľuje $\mathcal{P}$ na dve časti $\{Cl\}$ a $\mathcal{P} \setminus \{Cl\}$ ale túto vlastnosť nemôžeme vyjadriť jednou formulou.

Theorem

Pre každé Φ *ak* $Cl \in ||\Phi||^{\mathcal{P}}$ *tak existuje* $j, j \geq 0$ *také, že pre* $k \geq j$ $Cl^k \in ||\Phi||^{\mathcal{P}}$.

Temporálne vlastnosti

Beh procesu P_0 je konečná alebo nekonečná postupnosť:

$P_0 \xrightarrow{x_0} P_1 \xrightarrow{x_1} P_2 \xrightarrow{x_2} \dots$

Ak má beh konečnú dĺžku tak jeho posledný proces je deadlock.

Temporálne vlastnosti

Ideme vyjadriť, že proces *Cl* môže vykonať akciu *tick*:

$$Z \stackrel{def}{=} < tick > tt$$

Ideme vyjadriť, že proces *Cl* môže stále vykonávať akciu *tick*:

$$Z \stackrel{def}{=} < tick > Z$$

$\mathcal{E} = || < tick > ||^{\mathcal{P}} \mathcal{E} = \{P \in \mathcal{P} |$ existuje $P' \in \mathcal{E}, P \stackrel{tick}{\rightarrow} P'\}$
t.j $\mathcal{E}$ je pevný bod nasledujúcej funkcie:

$$f(X) = || < tick > ||^{\mathcal{P}} X$$

teda $f(\mathcal{E}) = \mathcal{E}$

Temporálne vlastnosti

Inak povedané, $\mathcal{E}$ je pre-pevný bod funkcie f, t.j.

$$f(\mathcal{E}) \subseteq \mathcal{E} \qquad (|| < tick > ||^{\mathcal{P}} \mathcal{E} \subseteq \mathcal{E})$$

a zároveň post-pevný bod funkcie f, t.j.

$$\mathcal{E} \subseteq f(\mathcal{E}) \qquad (\mathcal{E} \subseteq || < tick > ||^{\mathcal{P}} \mathcal{E})$$

Temporálne vlastnosti

Z toho dostávame dve podmienky pre riešenie:

PRE:
Ak $P \in \mathcal{P}$ a $P \stackrel{tick}{\rightarrow} P'$ a $P' \in \mathcal{E}$ potom $P \in \mathcal{E}$.

POST:
Ak $P \in \mathcal{E}$ potom $P \stackrel{tick}{\rightarrow} P'$ pre nejaké $P' \in \mathcal{E}$.

Ak $\mathcal{P} = \{Cl\}$ tak úloha má dve riešenie $\emptyset, \{Cl\}$, $\emptyset \subseteq \{Cl\}$ - najmenšie a najväčšie.

Príklad:
$\mathcal{P} = \{C_i | i \in N\}$

$$\begin{aligned} C_0 &\stackrel{def}{=} tick.C_0 + inc.C_1 \\ C_{2i+1} &\stackrel{def}{=} inc.C_{2i+2} + dec.C_{2i} \\ C_{2i+2} &\stackrel{def}{=} tick.C_{2i+2} + inc.C_{2i+3} + dec.C_{2i+1} \end{aligned}$$

Každá podmnožina $\{C_{2i} | i \in N\}$ spĺňa PRE a POST.

$\emptyset$ je najmenšie riešenie,

$\{C_{2i} | i \in N\}$ je najväčšie riešenie a má to nekonečne veľa riešení.

Nech $\mathcal{P}$ je generované z $Cl_1 = tick.tak.Cl_1$. Potom to má len jedno riešenie - $\emptyset$.

Temporálne vlastnosti

Vo všeobecnosti majú takéto rovnosti dve špeciálne riešenia - najväčšie a najmenšie (v množinovom zmysle - $\subseteq$), i keď tieto môžu byť rovnaké.
Najmenšie riešenie je prienik všetkých pre pevných bodov a najväčšie je zjednotenie všetkých post=pevných bodov.

Theorem

Nech $\mathcal{P}$ je množina a nech $g : 2^{\mathcal{P}} \rightarrow 2^{\mathcal{P}}$ je monotónne zobrazenie vzhľadom na $\subseteq$. Potom
- g má najmenší pevný bod vzhľadom na $\subseteq$ daný

$$\bigcap\{\mathcal{E} \subseteq \mathcal{P} | g(\mathcal{E}) \subseteq \mathcal{E}\}$$

- g má najväčší pevný bod vzhľadom na $\subseteq$ daný

$$\bigcup\{\mathcal{E} \subseteq \mathcal{P} | \mathcal{E} \subseteq g(\mathcal{E})\}$$

Temporálne vlastnosti

Ozančme
- najmenší pevný bod $\mu Z. < tick > Z$
- najväčší pevný bod $\nu Z. < tick > Z$

rovnice

$Z =< tick > Z$

najmenšie riešenie $\emptyset$ nehovorí nič.

Nech $\mathcal{E} \subseteq \mathcal{P}$ pozostáva zo všetkých procesov, ktoré majú nekonečný beh
$P_0 \overset{tick}{\rightarrow} P_1 \overset{tick}{\rightarrow} P_2 \overset{tick}{\rightarrow} \ldots$
Zrejme to spĺňa POST a teda to musí byť v $\nu Z. < tick > Z$. Nech existuje $\mathcal{E} \subset \mathcal{E}'$, ktoré tiež spĺňa POST. Nech $Q_0 \in \mathcal{E}' \setminus \mathcal{E}$.
Z POST máme, že $Q_0 \overset{tick}{\rightarrow} Q_1$ a $Q_1 \in \mathcal{E}'$ ale opäť $Q_1 \overset{tick}{\rightarrow} Q_2$ atď. a to je v spore že $Q_0 \notin \mathcal{E}$
Teda $\mathcal{E}$ je najväčšie riešenie $Z =< tick > Z$ - vyjadruje schopnosť stáleho tikania, čo sme predtým nevedeli vyjadriť.

Temporálne vlastnosti

Vo všeobecnosti, $\nu Z. < K > Z$ vyjadruje schopnosť vykanávať akcie z K donekonečna.

$\nu Z. < - > Z$ - nekonečné chovanie

$\nu Z. < \tau > Z$ - divergencia

Predchádzajúca veta sa dá aplikovať na každú modálnu rovnicu $Z \stackrel{def}{=} \Psi$, kde Ψ pozostáva z modálnych a boolovských spojok, konštánt tt, ff a Z.

Temporálne vlastnosti

Nech Ψ neobsahuje Z a
$Z = \Psi \vee < K > Z$

každé riešenie $\mathcal{E} \subseteq \mathcal{P}$ musí spĺňať
$\mathcal{E} = ||\Psi||^{\mathcal{P}} \cup || < K > ||^{\mathcal{P}} \mathcal{E}$

PRE $(f(\mathcal{E}) \subseteq \mathcal{E})$
ak $P \in \mathcal{P}$ a $(P \models \Psi$ alebo $P \xrightarrow{x} P'$ pre $x \in K$ a $P' \in \mathcal{E})$ potom $P \in \mathcal{E}$

POST $(\mathcal{E} \subseteq f(\mathcal{E}))$
ak $P \in \mathcal{E}$ potom $P \models \Psi$ alebo $P \xrightarrow{x} P'$ pre nejaké $x \in K$ a nejaké $P' \in \mathcal{E}$

Temporálne vlastnosti

- najmenšie riešenie je prienik všetkých PRE a najväčšie riešenie je zjednotenei všetkých POST

- každé riešenie $\mathcal{E}$ čo spĺňa PRE musí obsahovať tie procesy z $\mathcal{P}$ s vlastnosťou Ψ.

Obsahuje aj tie, čo nemajú vlastnosť Ψ ale môžu vykonať postupnosť akcií z K a výsledok spĺňa Ψ.

P_0 má vlastnosť $\mu Z.\Psi \vee < K > Z$ ak
$P_0 \xrightarrow{x_0} P_1 \xrightarrow{x_1} P_2 \xrightarrow{x_2} \ldots$
kde $P_n \models \Psi$ pre nejaké n a pre $j < n$ platí $x_j \in K$.

Maximálne riešenie obsahuje i proces, keď Ψ nikdy nebude platiť.

Temporálne vlastnosti

$\mu Z.\Psi \vee < - > Z$

raz bude Ψ platiť

$\mu Z.\Psi \vee < \tau > Z$

$<< \; >> \Psi$

Temporálne vlastnosti

Nech Ψ neobsahuje Z a
$Z = \Psi \wedge < K > Z$

- najmenšie riešenie *ff*

- najväčšie riešenie

POST $(\mathcal{E} \subseteq f(\mathcal{E}))$
ak $P \in \mathcal{E}$ potom $P \models \Psi$ a $P \xrightarrow{x} P'$ pre nejaké $x \in K$ a nejaké $P' \in \mathcal{E}$

procesy majú nekonečné behy a všetky spĺňajú Ψ

Dualita

$$||\neg\Psi||^{\mathcal{P}} = \mathcal{P} \setminus ||\Psi||^{\mathcal{P}}$$

no nechceme negáciu - keďže s ňou nie je zaručená monotónnosť a teda riešenie rovníc - existencia pevného bodu

Príklad:
$Z = \neg Z$

Mohli by sme používať negáciu ak by v rovnici

$Z = \Psi$

v Ψ bolo Z obsiahnuté v rozsahu párneho počtu negácií.

Dualita

negácií sa možno vyhnúť

Ψ^c ... komplementárna formula k Ψ

$$
\begin{array}{rcl}
tt^c & = & ff \\
ff^c & = & tt \\
(\Psi \wedge \Phi)^c & = & \Psi^c \vee \Phi^c \\
(\Psi \vee \Phi)^c & = & \Psi^c \wedge \Phi^c \\
([K]\Psi)^c & = & < K > \Psi^c \\
(< K > \Psi)^c & = & [K]\Psi^c \\
(\mu Z.\Psi)^c & = & \nu Z.\Psi^c \\
(\nu Z.\Psi)^c & = & \mu Z.\Psi^c
\end{array}
$$

Dualita

Príklad:

$(< tick > tt \wedge < tak >)^c = [tik]ff \vee [tak]ff$

Theorem

$$||\Psi^c||^{\mathcal{P}} = \mathcal{P} \setminus ||\Psi||^{\mathcal{P}}$$

Dualita

Príklad:

$\nu Z < \tau > Z$ ... divergencia

$(\nu Z < \tau > Z)^c = \mu Z[\tau]Z$ ... konvergencia

P má vlastnosť $\mu Z[K]Z$ ak nedokáže urobiť nekonečný beh pozostávajúci výlučne z K akcií.

P má vlastnosť $\mu Z[-]Z$ ak nemá nekonečné behy.

(neznamená to, že existuje n také, že po n krokoch proces skončí)