Modely konkurentných systémov
Formálne metódy tvorby softvéru

Damas Gruska

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

Prednáška 10.

Modálny MU - kalkuls

Množina formúl:

$$\Phi := Z|\Phi_1 \wedge \Phi_2|\Phi_1 \vee \Phi_2|[K]\Phi| < k > \Phi|\nu Z.\Phi|\mu Z.\Phi$$

Z - propozičná premenná
$\mu Z, \nu Z$ - operátory pevných bodov
$K \subseteq Act$

$\sigma \in \{\mu, \nu\}$

Vo formule $\sigma Z.\Phi$ je Z viazaná.
Premenná Z je voľná, ak nie je viazaná.

Temporálne vlastnosti budeme vyjadrovať pomocou uzavrených formúl, t.j. formúl, ktoré nemajú voľné premenné.

Explicitne sme neuviedli tt a ff:

$$tt \stackrel{def}{=} \nu Z.Z$$

$$ff \stackrel{def}{=} \mu Z.Z$$

Modálny MU - kalkuls

Nech $\mathcal{P}$ je transition closed množina procesov. V ďalšom budeme v označeniach vynechávať $\mathcal{P}$.

Ideme definovať $P \models \Phi$

Problematický je prípad $P \models \sigma Z.\Psi$, keď Ψ obsahuje voľnú premennú Z.

Nepriamo: využijeme $||\Phi||^{\mathcal{P}}$ t.j. množinu všetkých procesov z $\mathcal{P}$, ktoré spĺňajú Φ.

Modálny MU - kalkuls

valuácia:

$v : Z \mapsto v(Z), \quad v(Z) \subseteq \mathcal{P}$

$v[\mathcal{E}/Z] \ldots . v'$

v' to isté zobrazenie ako v s výnimkou, že $v'(Z) = \mathcal{E}$

Modálny MU - kalkuls

Pripomenutie:

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

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

Modálny MU - kalkuls

$$
\begin{aligned}
||Z||_v &\stackrel{def}{=} v(Z) \\
||\Phi \wedge \Psi||_v &\stackrel{def}{=} ||\Phi||_v \cap ||\Psi||_v \\
||\Phi \vee \Psi||_v &\stackrel{def}{=} ||\Phi||_v \cup ||\Psi||_v \\
||[K]\Phi||_v &\stackrel{def}{=} ||[K]|| \;\; ||\Phi||_v \\
|| < K > \Phi||_v &\stackrel{def}{=} || < K > || \;\; ||\Phi||_v \\
||\nu Z.\Phi||_v &\stackrel{def}{=} \bigcup \{\mathcal{E} \subseteq \mathcal{P} | \mathcal{E} \subseteq ||\Phi||_{v_{[\mathcal{E}/Z]}}\} \\
||\mu Z.\Phi||_v &\stackrel{def}{=} \bigcap \{\mathcal{E} \subseteq \mathcal{P} | \;\; ||\Phi||_{v_{[\mathcal{E}/Z]}} \subseteq \mathcal{E}\}
\end{aligned}
$$

Modálny MU - kalkuls

$$\begin{aligned}
&||tt||_v = ||\nu Z.Z||_v \\
&= \bigcup\{\mathcal{E} \subseteq \mathcal{P} | \mathcal{E} \subseteq ||Z||_{v_{[\mathcal{E}/Z]}}\} \\
&= \bigcup\{\mathcal{E} \subseteq \mathcal{P} | \mathcal{E} \subseteq \mathcal{E}\} \\
&= \mathcal{P}
\end{aligned}$$

$$\begin{aligned}
&||ff||_v = ||\mu Z.Z||_v \\
&= \bigcap\{\mathcal{E} \subseteq \mathcal{P} |\ ||Z||_{v_{[\mathcal{E}/Z]}} \subseteq \mathcal{E}\} \\
&= \bigcap\{\mathcal{E} \subseteq \mathcal{P} | \mathcal{E} \subseteq \mathcal{E}\} \\
&= \emptyset
\end{aligned}$$

Modálny MU - kalkuls

Theorem

Ak $\mathcal{E} \subseteq \mathcal{F}$ *tak potom*

$$||\Phi||_{\upsilon_{[\mathcal{E}/Z]}} \subseteq ||\Phi||_{\upsilon_{[\mathcal{F}/Z]}}$$

t.j.

$$f(X) = ||\Phi||_{\upsilon_{[X/Z]}}$$

je monotónna funkcia.

Modálny MU - kalkuls

Theorem

$$||\sigma Z.\Phi||_\upsilon = ||\Phi[\sigma Z.\Phi/Z]||_\upsilon = ||\Phi||_{\upsilon[||\sigma Z.\Phi||_\upsilon/Z]}$$

Modálny MU - kalkuls

Príklad:

$Cl = tick.Cl$

$\mathcal{P} = \{Cl, tick.Nil, Nil\}$

$\upsilon_0 : Z \mapsto \emptyset$

$||\nu Z.(< tick > Z \vee [tick]ff)||_{\upsilon_0} =$

$\bigcup\{\mathcal{E} \subseteq \mathcal{P} | \mathcal{E} \subseteq ||(< tick > Z \vee [tick]ff||_{\upsilon_{0[\mathcal{E}/Z]}}\} = \mathcal{P}$

lebo:

$||(< tick > Z \vee [tick]ff)||_{\upsilon_{0[\mathcal{P}/Z]}} =$

$||(< tick > Z||_{\upsilon_{0[\mathcal{P}/Z]}} \cup ||[tick]ff||_{\upsilon_{0[\mathcal{P}/Z]}} =$

$\{P \in \mathcal{P} |$ existuje $P' \in \mathcal{P}, P \stackrel{tick}{\rightarrow} P'\} \cup \{Nil\} =$

$\{Cl, tick.Nil\} \cup \{Nil\}$

Ľahko sa ukáže, že:

$$||\mu Z.(< tick > Z \vee [tick]ff)||_{v_0} = \{tick.Nil, Nil\}$$

Modálny MU - kalkuls

Ak je Φ uzavretá, tak

$$||\Phi||_v = ||\Phi||_{v'}$$

pre každé v, v'.

Modálny MU - kalkuls

$$<< \; >> \Phi \stackrel{def}{=} \mu Z.(\Phi \vee < \tau > Z)$$

$$[| \; |]\Phi \stackrel{def}{=} \nu Z.(\Phi \wedge [\tau]Z)$$

$$[| \downarrow |]\Phi \stackrel{def}{=} \mu Z.(\Phi \wedge [\tau]Z)$$

$$<<\uparrow>> \Phi \stackrel{def}{=} \nu Z.(\Phi \vee < \tau > Z)$$

Modálny MU - kalkuls

$$[|K|]\Phi \stackrel{def}{=} [|\ \ |][K][|\ \ |]\Phi = \nu Z.([K](\nu Y.\Phi \wedge [\tau]Y) \wedge [\tau]Z)$$

$$[|\downarrow K|]\Phi \stackrel{def}{=} [|\downarrow|][K][|\ \ |]\Phi = \mu Z.([K](\nu Y.\Phi \wedge [\tau]Y) \wedge [\tau]Z)$$

Modálny MU - kalkuls

Theorem

Ak $P \models \Phi$ *potom existuje* P' *také, že* P' *má konečný počet stavov a* $P' \models \Phi$.

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

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

Modálny MU - kalkuls

νg - najväčší pevný bod.

Ideme iterovať.

Nech $\nu^0 g = \mathcal{P}$.

Ak $\mathcal{P}$ je post pevný bod t.j. $\mathcal{P} \subseteq g(\mathcal{P})$ tak $\nu^0 g$ je pevný bod.

Inak $\mathcal{P} \not\subseteq g(\mathcal{P})$ t.j. $\nu^0 g \not\subseteq g(\nu^0 g)$.

Nech $\nu^1 g = g(\nu^0 g)$.

Ak $\nu^1 g$ je post pevný bod t.j. $\nu^1 g \subseteq g(\nu^1 g)$ tak $\nu^1 g = \nu g$

inak $\nu^1 g \supset g(\nu^1 g) = \nu^2 g$

$\nu^0 g \supseteq \nu^1 g \supseteq \nu^2 g \supseteq \nu^3 g \supseteq \cdots \supseteq \nu^i g \ldots$

Modálny MU - kalkuls

Ak existuje i také, že $\nu^i g = \nu^{i+1} g$ tak je to post pevný bod, t.j. najväčšie $\mathcal{E}$ také, že $\mathcal{E} \subseteq g(\mathcal{E})$.

Aj je konečné a obsahuje najviac n procesov, tak takáto iterácia musí skončiť po najviac n krokoch.

Modálny MU - kalkuls

Príklad:
$\mathcal{P} = \{Cl, tick.Nil, Nil\}$

$g(X) = || < tick > Z||_{\upsilon_{[X/Z]}}$
pre nejaké υ a $X \subseteq \mathcal{P}$.

$\nu^0 g = \mathcal{P} = \{Cl, tick.Nil, Nil\}$

$\nu^1 g = || < tick > Z||_{\upsilon_{[\nu^0 g/Z]}}$

$|| < tick > Z||_{\upsilon_{[\nu^0 g/Z]}} = || < tick > || \ ||Z||_{\upsilon_{[\nu^0 g/Z]}} =$

$|| < tick > ||\mathcal{P} = \{P \in \mathcal{P} | \exists P' \in \mathcal{P}, P \stackrel{tick}{\rightarrow} P'\} = \{Cl, tick.Nil\}$

Modálny MU - kalkuls

$$\nu^1 g = || < tick > Z||_{\upsilon_{[\nu^0 g/Z]}} = \{Cl, tick.Nil\}$$

$$\nu^2 g = || < tick > Z||_{\upsilon_{[\nu^1 g/Z]}} = || < tick > || \ ||Z||_{\upsilon_{[\nu^1 g/Z]}} =$$

$$|| < tick > ||\{Cl, tick.Nil\} = \{P \in \mathcal{P} | \exists P' \in \{Cl, tick.Nil\}, P \stackrel{tick}{\rightarrow} P'\} = \{Cl\}$$

$$\nu^2 g = ||tick > Z||_{\upsilon_{[\nu^1 g/Z]}} = \{Cl\}$$

$$\nu^3 g = ||tick > Z||_{\upsilon_{[\nu^2 g/Z]}} = \{Cl\}$$

$$\nu^{n+2} g = \{Cl\}$$

Najmenší pevný bod

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

$\mu^0 g = \emptyset$

ak $g(\mu^0 g) \supset \mu^0 g$ tak $\mu^1 g = g(\mu^0 g)$

Vo všeobecnosti:

$\mu^0 g \subseteq \mu^1 g \subseteq \dots \subseteq \mu^i g \subseteq \dots$

Modálny MU - kalkuls

Príklad:
$\mathcal{P} = \{Cl, tick.Nil, Nil\}$

$$g(X) = ||[tick]ff \vee <-> Z||_{\upsilon_{[X/Z]}}$$

$$\mu^0 g = \emptyset$$

$$\mu^1 g = ||[tick]ff \vee <-> Z||_{\upsilon_{[\mu^0 g/Z]}} = \{Nil\}$$

$$\mu^2 g = ||[tick]ff \vee <-> Z||_{\upsilon_{[\mu^1 g/Z]}} = \{tick.Nil, Nil\}$$

$$\mu^3 g = ||[tick]ff \vee <-> Z||_{\upsilon_{[\mu^2 g/Z]}} = \{tick.Nil, Nil\}$$

Modálny MU - kalkuls

Theorem

Nech $\mathcal{P}$ je množina a nech $g : 2^{\mathcal{P}} \to 2^{\mathcal{P}}$ je monotónne zobrazenie vzhľadom na $\subseteq$. Potom

$$\mu g = \bigcup_{\alpha \in \Lambda} \mu^{\alpha} g$$

a

$$\nu g = \bigcap_{\alpha \in \Lambda} \nu^{\alpha} g$$

Modálny MU - kalkuls

$$\nu^0 g = \mathcal{P}$$

$$\nu^0 g = ||tt||_\upsilon$$

$$\mu^0 g = \emptyset$$

$$\mu^0 g = ||ff||_\upsilon$$

$$\nu^1 g = ||\Phi[tt/Z]||_\upsilon$$

$$\mu^1 g = ||\Phi[ff/Z]||_\upsilon$$

Modálny MU - kalkuls

Definujme:
$\nu Z^0 . \Phi = tt$

$\nu Z^{\alpha+1} \Phi = \Phi[\nu Z^\alpha \Phi / Z]$

$\nu Z^\beta \Phi = \bigwedge_{\alpha<\beta} \Phi[\nu Z^\alpha \Phi / Z]$

$\mu Z^0 . \Phi = ff$

$\mu Z^{\alpha+1} \Phi = \Phi[\mu Z^\alpha \Phi / Z]$

$\mu Z^\beta \Phi = \bigvee_{\alpha<\beta} \Phi[\nu Z^\alpha \Phi / Z]$

kde β je limitný ordinál.

Platí:
$|| \bigwedge_{i \in I} \Phi ||_v = \bigcap_{i \in I} ||\Phi||_v$ a $|| \bigvee_{i \in I} \Phi ||_v = \bigcup_{i \in I} ||\Phi||_v$

Modálny MU - kalkuls

Theorem

Nech $g(X) = ||\Phi||_{v_{[X/Z]}}$.
Potom pre všetky ordinály platí:
1. $\nu^\alpha g = ||\nu Z^\alpha \Phi||_v$
2. $\mu^\alpha g = ||\mu Z^\alpha \Phi||_v$

Dôsledok:
$P \models \nu Z \Phi$ iff $\forall \alpha, P \models \nu Z^\alpha \Phi$
$P \models \mu Z \Phi$ iff $\exists \alpha, P \models \mu Z^\alpha \Phi$

Navyše kvantifikáciu α môžeme ohraničiť veľkosťou $\mathcal{P}(P)$.

Príklad:
$\nu Z. < tick > Z \ldots \nu Z.\Phi$

$\nu Z^0\Phi = tt$
$\nu Z^1\Phi =< tick > .tt$
$\nu Z^2\Phi =< tick >< tick > .tt$
$\vdots$
$\nu Z^i\Phi =< tick >^i .tt$
$\nu Z^\omega\Phi = \bigwedge_{i\in N} < tick >^i .tt$

t.j.
$P \models \nu Z. < tick > Z$ ak P tiká večne.

Modálny MU - kalkuls

Príklad:

$$\mu Z.(\Phi \wedge [\tau]Z) \ldots \mu Z.\Psi$$

$$\mu Z^0\Psi = ff$$

$$\mu Z^1\Psi = \Phi \wedge [\tau]ff$$

$$\mu Z^2\Psi = \Phi \wedge [\tau](\Phi \wedge [\tau]ff)$$

$$\vdots$$

$$\mu Z^i\Psi = \Phi \wedge [\tau](\Phi \wedge [\tau](\ldots))$$

t.j. P má vlastnosť $\mu Z.\Psi$ ak $[| \downarrow |]\Phi$.