Je Hennessy-Milner logika dostatečně silná?

Modální hloubka (stupeň zanoření - modal depth, nesting degree) pro formule Hennessy-Milner logiky:

- $md(tt) = md(ff) = 0$
- $md(F \wedge G) = md(F \vee G) = \max\{md(F), md(G)\}$
- $md([a]F) = md(\langle a \rangle F) = md(F) + 1$

Myšlenka: formule F "vidí" jen do hloubky $md(F)$.

Věta (nechť F je HM formule a $k = md(F)$)

Pokud má obránce obrannou strategii v silné bisimulační hře z s a t na k kol, pak $s \models F$ právě tehdy, když $t \models F$.

Důsledek

Neexistuje např. Hennessy-Milner formule F, která by vyjadřovala dosažitelnost deadlocku v libovolném LTS.

Temporální vlastnosti nevyjádřitelné v HM logice

$s \models \mathit{Inv}(F)$ právě tehdy, když všechny stavy dosažitelné z s splňují F
$s \models \mathit{Pos}(F)$ právě tehdy, když existuje stav dosažitelný z s splňující F

Fakt

Vlastnosti $\mathit{Inv}(F)$ a $\mathit{Pos}(F)$ nejsou vyjádřitelné v HM logice.

Nechť $Act = \{a_1, a_2, \ldots, a_n\}$ je konečná množina akcí. Definujeme

- $\langle Act \rangle F \stackrel{\text{def}}{=} \langle a_1 \rangle F \vee \langle a_2 \rangle F \vee \ldots \vee \langle a_n \rangle F$
- $[Act] F \stackrel{\text{def}}{=} [a_1] F \wedge [a_2] F \wedge \ldots \wedge [a_n] F$

$\mathit{Inv}(F) \ldots F \wedge [Act]F \wedge [Act][Act]F \wedge [Act][Act][Act]F \wedge \ldots$
$\mathit{Pos}(F) \ldots F \vee \langle Act \rangle F \vee \langle Act \rangle \langle Act \rangle F \vee \langle Act \rangle \langle Act \rangle \langle Act \rangle F \vee \ldots$

Nekonečné konjunkce a disjunkce vs. rekurze

Problémy

- nekonečně velké formule nejsou povoleny v HM logice
- nekonečně velké formule jsou obtížně zpracovatelné

A co třeba použít rekurzi?

- $Inv(F)$ vyjádřena $X \stackrel{\text{def}}{=} F \wedge [Act]X$
- $Pos(F)$ vyjádřena $X \stackrel{\text{def}}{=} F \vee \langle Act \rangle X$

Otázka: Jak definovat sémantiku takových rovnic?

Ukázky řešení rovnic

Rovnice nad přirozenými čísly ($n \in \mathbb{N}$)

$n = 2 * n$	jedno řešení $n = 0$
$n = n + 1$	žádné řešení
$n = 1 * n$	mnoho řešení (každé $n \in \mathbb{N}$ je řešením)

Rovnice nad množinami přirozených čísel ($M \in 2^{\mathbb{N}}$)

$M = (\{7\} \cap M) \cup \{7\}$	jedno řešení $M = \{7\}$
$M = \mathbb{N} \setminus M$	žádné řešení
$M = \{3\} \cup M$	mnoho řešení (každé $M \supseteq \{3\}$)

A co rovnice nad procesy?

$X \stackrel{\text{def}}{=} [a]ff \vee \langle a \rangle X \quad \Rightarrow \quad$ najít $Z \subseteq 2^{Proc}$ tž. $Z = [\cdot a \cdot]\emptyset \cup \langle \cdot a \cdot \rangle Z$

Obecný přístup – teorie svazů

Problém

Pro množinu D a funkci $f : D \to D$ nazýváme prvky $x \in D$ splňující

$$x = f(x)$$

pevnými body (fixed points) funkce f.

Částečně uspořádaná množina (Partially Ordered Set, poset)

Častečně uspořádaná množina (nebo prostě částečné uspořádání) je dvojice $(D, \sqsubseteq)$ tž.

- D je množina
- $\sqsubseteq \subseteq D \times D$ je binární relace na D, která je
  - reflexivní: $\forall d \in D : \; d \sqsubseteq d$
  - antisymetrická: $\forall d, e \in D : \; d \sqsubseteq e \;\wedge\; e \sqsubseteq d \;\Rightarrow\; d = e$
  - transitivní: $\forall d, e, f \in D : \; d \sqsubseteq e \;\wedge\; e \sqsubseteq f \;\Rightarrow\; d \sqsubseteq f$

Supremum a infimum

Horní/dolní závora (nechť $X \subseteq D$)

- $d \in D$ je horní závora (upper bound) množiny X (značíme $X \sqsubseteq d$) právě, když $x \sqsubseteq d$ pro všechna $x \in X$
- $d \in D$ je dolní závora (lower bound) množiny X (značíme $d \sqsubseteq X$) právě, když $d \sqsubseteq x$ pro všechna $x \in X$

Nejmenší dolní a největší horní závora (nechť $X \subseteq D$)

- $d \in D$ je nejmenší horní závora (supremum) for X ($\sqcup X$) právě, když
  1. $X \sqsubseteq d$
  2. $\forall d' \in D : \; X \sqsubseteq d' \;\Rightarrow\; d \sqsubseteq d'$
- $d \in D$ je největší dolní závora (infimum) for X ($\sqcap X$) právě, když
  1. $d \sqsubseteq X$
  2. $\forall d' \in D : \; d' \sqsubseteq X \;\Rightarrow\; d' \sqsubseteq d$

Úplné svazy a monotónní funkce

Úplný svaz

Částečně uspořádaná množina $(D, \sqsubseteq)$ se nazývá úplný svaz (complete lattice) právě tehdy, když $\sqcup X$ a $\sqcap X$ existují pro každé $X \subseteq D$.

V úplném svazu existuje největší ($\top \stackrel{\text{def}}{=} \sqcup D$) a nejmenší ($\bot \stackrel{\text{def}}{=} \sqcap D$) prvek.

Monotónní funkce a pevné body

Funkce $f : D \to D$ se nazývá monotónní právě tehdy, když

$$d \sqsubseteq e \quad \Rightarrow \quad f(d) \sqsubseteq f(e)$$

pro všechna $d, e \in D$.

Prvek $d \in D$ je pevný bod právě, když $d = f(d)$.

Tarského věta o pevném bodu

Věta (Tarski)

Nechť $(D, \sqsubseteq)$ je úplný svaz a nechť $f : D \to D$ je monotónní funkce.

Potom f má právě jeden největší pevný bod z_{max} a právě jeden nejmenší pevný bod z_{min} určené rovnicemi:

$$z_{max} \stackrel{\text{def}}{=} \sqcup\{x \in D \mid x \sqsubseteq f(x)\}$$

$$z_{min} \stackrel{\text{def}}{=} \sqcap\{x \in D \mid f(x) \sqsubseteq x\}$$

Výpočet pevných bodů na konečných svazech

Nechť $(D, \sqsubseteq)$ je úplný svaz a $f : D \to D$ je monotónní.

Nechť $f^1(x) \stackrel{\text{def}}{=} f(x)$ a $f^n(x) \stackrel{\text{def}}{=} f(f^{n-1}(x))$ pro $n > 1$, tj.

$$f^n(x) = \underbrace{f(f(\ldots f}_{n \text{ krát}}(x)\ldots)).$$

Věta

Když D je konečná množina, tak existují celá čísla $M, m > 0$ tž.

- $z_{max} = f^M(\top)$
- $z_{min} = f^m(\bot)$

Myšlenka (pro z_{min}): Následující sekvence se ustálí pro každé konečné D

$$\bot \sqsubseteq f(\bot) \sqsubseteq f(f(\bot)) \sqsubseteq f(f(f(\bot))) \sqsubseteq \cdots$$

Množina všech podmožin

- Pro množinu S je množina všech podmnožin $2^S = \{X \mid X \subseteq S\}$ částečně uspořádána relací být podmnožinou $\subseteq$ (reflexivní, tranzitivní a antisymetrickou).
- Částečně uspořádaná množina $(2^S, \subseteq)$ je úplným svazem.
- Funkce $f : 2^S \to 2^S$ je monotónní právě tehdy, když $X \subseteq Y$ implikuje $f(X) \subseteq f(Y)$.

Věta (Knaster, Tarski)

Nechť $f : 2^S \to 2^S$ je monotónní funkce.
Potom f má právě jeden největší pevný bod Z_{max}
a právě jeden nejmenší pevný bod Z_{min} dané vztahy:

$$Z_{max} \stackrel{\text{def}}{=} \cup\{X \subseteq S \mid X \subseteq f(X)\}$$

$$Z_{min} \stackrel{\text{def}}{=} \cap\{X \subseteq S \mid f(X) \subseteq X\}$$

Vztah nejmenšího a největšího pevného bodu

Nechť $f : 2^S \to 2^S$ je monotónní.

$$Z_{max} = \cup\{X \subseteq S \mid X \subseteq f(X)\}$$

Co je doplňkem Z_{max}, tj. $\overline{Z_{max}} = S - Z_{max}$?

$\overline{Z_{max}} = \overline{\cup\{X \mid X \subseteq f(X)\}} = \cap\{\overline{X} \mid X \subseteq f(X)\} = \cap\{Y \mid \overline{Y} \subseteq f(\overline{Y})\} =$
$\cap\{Y \mid \overline{f(\overline{Y})} \subseteq Y\} = \cap\{Y \mid f_d(Y) \subseteq Y\}$

kde $f_d(Y) = \overline{f(\overline{Y})}$ (f_d je duální funkce k f)
Pozn. f_d je také monotónní
$X \subseteq Y \Rightarrow \overline{Y} \subseteq \overline{X} \Rightarrow f(\overline{Y}) \subseteq f(\overline{X}) \Rightarrow \overline{f(\overline{X})} \subseteq \overline{f(\overline{Y})} \Rightarrow f_d(X) \subseteq f_d(Y))$
a proto

Pozorování

Doplněk největšího pevného bodu funkce f je nejmenším pevným bodem duální funkce f_d.

Výpočet pevných bodů na konečných množinách

Věta

Když S je konečná a $f : 2^S \to 2^S$ je monotónní, pak existují celá čísla $M, m > 0$ tž.

- $Z_{max} = f^M(S)$
- $Z_{min} = f^m(\emptyset)$

Silná bisimilarita (připomenutí)

Nechť $(Proc, Act, \{\xrightarrow{a} | \ a \in Act\})$ je LTS.

Silná bisimulace (Strong Bisimulation)

Binární relace $R \subseteq Proc \times Proc$ je silná bisimulace (strong bisimulation) právě tehdy, když kdykoliv $(s, t) \in R$ potom pro každé $a \in Act$:

- jestliže $s \xrightarrow{a} s'$, pak $t \xrightarrow{a} t'$ pro nějaké t' takové, že $(s', t') \in R$
- jestliže $t \xrightarrow{a} t'$, pak $s \xrightarrow{a} s'$ pro nějaké s' takové, že $(s', t') \in R$.

Silná bisimilarita (Strong Bisimilarity)

Dva procesy $p, q \in Proc$ jsou silně bisimulačně ekvivalentní (strongly bisimilar, $p \sim q$) právě tehdy, když existuje silná bisimulace R tž. $(p, q) \in R$.

$$\sim \ = \ \cup\{R \mid R \text{ je silná bisimulace}\}$$

Silná bisimulace a největší pevný bod

Funkce $\mathcal{F} : 2^{(Proc \times Proc)} \longrightarrow 2^{(Proc \times Proc)}$

Nechť $X \subseteq Proc \times Proc$. Potom definujeme $\mathcal{F}(X)$ následovně:

$(s, t) \in \mathcal{F}(X)$ právě tehdy, když pro každé $a \in Act$:

- jestli $s \xrightarrow{a} s'$ potom $t \xrightarrow{a} t'$ pro nějaké t' tž. $(s', t') \in X$
- jestli $t \xrightarrow{a} t'$ potom $s \xrightarrow{a} s'$ pro nějaké s' tž. $(s', t') \in X$.

Pozorování

- $\mathcal{F}$ je monotónní
- S je silná bisimulace právě tehdy, když $S \subseteq \mathcal{F}(S)$

Silná bisimilarita je největší pevný bod $\mathcal{F}$

$$\sim = \bigcup \{S \in 2^{(Proc \times Proc)} \mid S \subseteq \mathcal{F}(S)\}$$

HML s jednou rekurzivně definovanou proměnnou

Syntaxe formulí

Formule jsou dány následující abstraktní syntaxí

$$F ::= X \mid tt \mid ff \mid F_1 \wedge F_2 \mid F_1 \vee F_2 \mid \langle a \rangle F \mid [a]F$$

kde $a \in Act$ a X je proměnná s definicí

- $X \stackrel{\min}{=} F_X$, or $X \stackrel{\max}{=} F_X$

taková, že F_X je formule logiky (která může obsahovat X).

Jak definovat sémantiku?

Pro každou formuli F definujeme funkci $O_F : 2^{Proc} \to 2^{Proc}$ tž.

- pokud S je množina procesů, která splňuje X, potom
- $O_F(S)$ je množina procesů splňujících F.

Definice $O_F : 2^{Proc} \to 2^{Proc}$ (nechť $S \subseteq Proc$)

$$
\begin{aligned}
O_X(S) &= S \\
O_{tt}(S) &= Proc \\
O_{ff}(S) &= \emptyset \\
O_{F_1 \wedge F_2}(S) &= O_{F_1}(S) \cap O_{F_2}(S) \\
O_{F_1 \vee F_2}(S) &= O_{F_1}(S) \cup O_{F_2}(S) \\
O_{\langle a \rangle F}(S) &= \langle \cdot a \cdot \rangle O_F(S) \\
O_{[a]F}(S) &= [\cdot a \cdot] O_F(S)
\end{aligned}
$$

O_F je monotónní pro každou formuli F

$$S_1 \subseteq S_2 \;\Rightarrow\; O_F(S_1) \subseteq O_F(S_2)$$

Důkaz: jednoduchý (indukcí podle struktury formule F).

Sémantika

Pozorování

O_F je monotónní na $(2^{Proc}, \subseteq)$, takže O_F má právě jeden největší pevný bod a právě jeden nejmenší pevný bod.

Sémantika proměnné X

- Pokud $X \stackrel{\max}{=} F_X$ potom

$$[\![X]\!] = \bigcup \{S \subseteq Proc \mid S \subseteq O_{F_X}(S)\}.$$

- Pokud $X \stackrel{\min}{=} F_X$ potom

$$[\![X]\!] = \bigcap \{S \subseteq Proc \mid O_{F_X}(S) \subseteq S\}.$$

Herní charakterizace

Intuice: útočník tvrdí $s \not\models F$, obránce tvrdí $s \models F$.

Konfigurace hry jsou tvaru (s, F)

- (s, tt) a (s, ff) nemají následovníky
- (s, X) má jednoho následovníka (s, F_X)
- $(s, F_1 \wedge F_2)$ má dva následovníky (s, F_1) a (s, F_2)
  (vybírá útočník)
- $(s, F_1 \vee F_2)$ má dva následovníky (s, F_1) and (s, F_2)
  (vybírá obránce)
- $(s, [a]F)$ má následovníky (s', F) pro každé s' tž. $s \xrightarrow{a} s'$
  (vybírá útočník)
- $(s, \langle a \rangle F)$ má následovníky (s', F) pro každé s' tž. $s \xrightarrow{a} s'$
  (vybírá obránce)

Kdo je vítěz?

Partie (play) je maximální sekvence konfigurací vytvořená podle pravidel hry danými na předchozím slidu.

Konečná partie

- Útočník vyhrává konečnou hru, když obránce nemá tah nebo hráči dosáhnou konfiguraci (s, ff).
- Obránce vyhrává konečnou hru, když útočník nemá tah nebo hráči dosáhnou konfiguraci (s, tt).

Nekonečná partie

- Útočník vyhrává nekonečnou hru, když je X definováno jako $X \overset{\min}{=} F_X$.
- Obránce vyhrává nekonečnou hru, když je X definováno jako $X \overset{\max}{=} F_X$.

Herní charakterizace

Věta

- $s \models F$ právě tehdy, když obránce má univerzální vítěznou strategii z (s, F)
- $s \not\models F$ právě tehdy, když útočník má univerzální vítěznou strategii z (s, F)

Výběr temporálních vlastností

- $Inv(F)$: $X \overset{\max}{=} F \wedge [Act]X$
- $Pos(F)$: $X \overset{\min}{=} F \vee \langle Act \rangle X$

- $Safe(F)$: $X \overset{\max}{=} F \wedge ([Act]ff \vee \langle Act \rangle X)$
- $Even(F)$: $X \overset{\min}{=} F \vee (\langle Act \rangle tt \wedge [Act]X)$

- $F \; \mathcal{U}^w \; G$: $X \overset{\max}{=} G \vee (F \wedge [Act]X)$
- $F \; \mathcal{U}^s \; G$: $X \overset{\min}{=} G \vee (F \wedge \langle Act \rangle tt \wedge [Act]X)$

S využitím operátoru until můžeme vyjádřit např. $Inv(F)$ a $Even(F)$:

$$Inv(F) \equiv F \; \mathcal{U}^w \; ff \qquad\qquad Even(F) \equiv tt \; \mathcal{U}^s \; F$$

Příklady složitějších rekurzivních formulí

Vnořené definice rekurzivních proměnných

$$X \overset{\min}{=} Y \vee \langle Act \rangle X \qquad\qquad Y \overset{\max}{=} \langle a \rangle tt \wedge \langle Act \rangle Y$$

Řešení: spočítat nejprve $[\![Y]\!]$ a potom $[\![X]\!]$.

Vzájemně rekurzivní funkce

$$X \overset{\max}{=} [a] Y \qquad\qquad Y \overset{\max}{=} \langle a \rangle X$$

Řešení: uvažujeme úplný svaz $(2^{Proc} \times 2^{Proc}, \sqsubseteq)$ kde $(S_1, S_2) \sqsubseteq (S_1', S_2')$ právě tehdy, když $S_1 \subseteq S_1'$ a $S_2 \subseteq S_2'$.

Pozn.: V předchozím příkladě odkazujeme na verzi Tarského věty pro všechny úplné svazy.