Temporální logiky

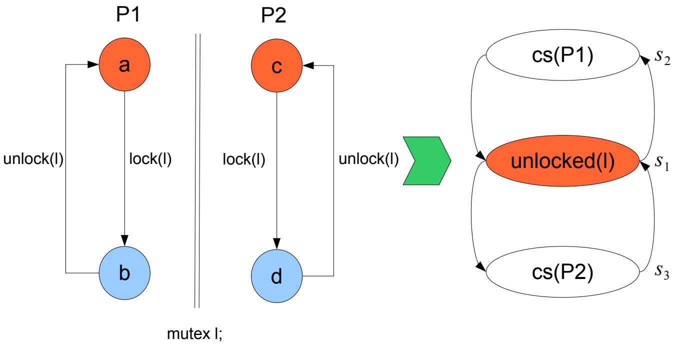
Radek Mařík

ČVUT FEL, K13133

September 6, 2011

Obsah

Přechody mezi konfiguracemi v Kripkeho struktuře [Voj10]



Cesta v Kripkeho struktuře [Voj10]

Cesta

- **Cesta** π ... v Kripkeho struktuře M je nekonečná sekvence stavů $\pi = s_0 s_1 s_3 \ldots$ taková, že $\forall i \in N..R(s_i, s_{i+1})$.
- $\Pi(M, s)$ ... množina všech cest v M, které začínají v $s \in S$
- Sufix π^i cesty $\pi = s_0 s_1 s_3 \ldots s_i s_{i+1} s_{i+2}$ je cesta $\pi^i = s_i s_{i+1} s_{i+2}$ začínající v s_i.
- $s_i = \pi[i]$

Pojem času [Voj10]

Abstrakce času

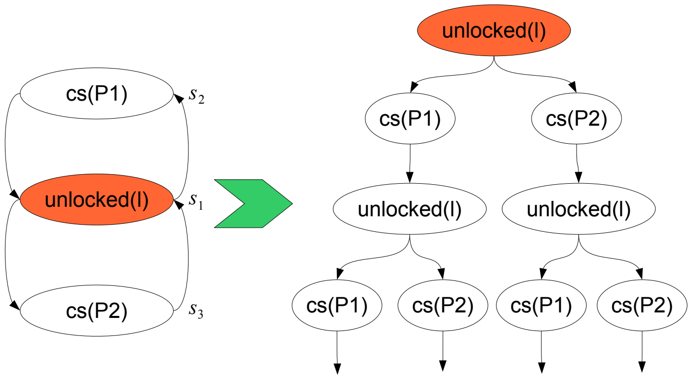
- **Logický čas** . . . pracuje s *(částečným) uspořádáním* stavů/událostí v chování systému.
- **Fyzický čas** . . . *měření* doby uběhlou mezi dvěma stavy/události.

Čas ve verifikaci modelů

- **Lineární čas** . . . dovoluje se vyjadřovat pouze o dané *lineární trase* ve stavovém prostoru.
  - Na všech trasách, x musí být následováno y.
  - Na všech trasách, x musí být následováno y nebo z.
- **Větvící se čas** . . . dovoluje kvantifikovat (existenčně i univerzálně) možné budoucnosti počínaje daným stavem. Na stavový prostor se pohlíží jako na rozvinutý *nekonečný strom*.
  - Existuje trasa, kde následující stav je x.

Výpočetní strom [Voj10]

Popisuje vlastnosti výpočetního stromu



CTL* formule [Voj10]

Skládá se z

- atomické výroky
- logické spojky
- kvantifikátory cest
- temporální operátory

CTL* kvantifikátory a operátory [Wik10, Voj10]

Kvantifikátory cest

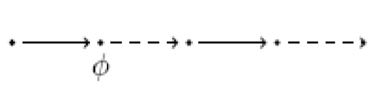
popisují strukturu větvení vypočetního stromu

- E ... existuje cesta výpočtu z daného stavu.
- A ... pro všechny cesty výpočtů z daného stavu.

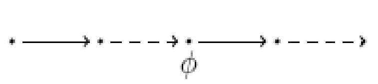
Temporální operátory

určují vlastnosti cesty ve výpočetním stromu

- $X\varphi$ (next time, $\bigcirc$)... vlastnost φ platí ve druhém (následujícím) stavu cesty..



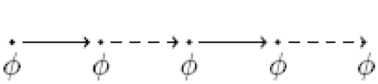
- $F\varphi$ (in future, $\Diamond$)... vlastnost φ platí v nějakém stavu cesty.



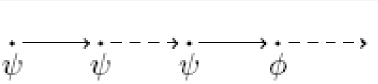
CTL* operátory [Wik10, Voj10]

Temporální operátory

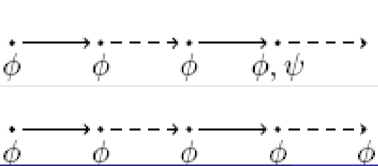
- $G\varphi$ (globally, $\Box$)... vlastnost φ platí ve všech stavech cesty.



- $\varphi U \psi$ (until)... vlastnost ψ platí v nějakém stavu cesty a vlastnost φ platí přinejmenším ve všech předcházejících stavech této cesty.



- $\varphi R \psi$ (release)... vlastnost ψ musí platit do (a včetně) stavu, kdy začne platit vlastnost φ, pokud takový stav existuje.



CTL* syntax [Voj10]

Nechť AP je neprázdná množina atomických výroků.

Syntax stavových formulí, které jsou pravdivé v daném stavu

- Jestliže $p \in AP$, potom p je stavová formule.
- Jestliže φ a ψ jsou stavové formule, potom $\neg\varphi$, $\varphi \vee \psi$, $\varphi \wedge \psi$ jsou stavové formule.
- Jestliže φ je běhová formule, potom $E\varphi$ a $A\varphi$ jsou stavové formule.

Syntax běhových formulí, které jsou pravdivé podél specifické cesty

- Jestliže φ je stavová formule, pak φ je také běhová formule.
- Jestliže φ a ψ jsou běhové formule, pak $\neg\varphi$, $\varphi \vee \psi$, $\varphi \wedge \psi$, $X\varphi$, $F\varphi$, $G\varphi$, $\varphi U \psi$ a $\varphi R \psi$ jsou běhové formule.

CTL* je množina stavových formulí generovaných výše uvedenými pravidly.

CTL* sémantika [Voj10]

- Nechť je dána Kripkeho struktura $M = (S, T, \mathcal{I}, s_0, L)$ nad množinou atomických výroků AP.
- Pro stavovou formuli φ nad AP, zapisujeme $M, s \models \varphi$ fakt, že φ platí v $s \in S$.
- Pro běhovou formuli φ nad AP, zapisujeme $M, \pi \models \varphi$ fakt, že φ platí podél cesty π v M.
- Nechť $s \in S$, π je cesta v M, φ_1, φ_2 jsou stavové formule nad AP, $p \in AP$, a ψ_1, ψ_2 jsou běhové formule nad AP.
  Pak relaci $\models$ definujeme induktivně následovně:
  - $\mathbf{M, s \models p}$ iff $p \in L(s)$.
  - $\mathbf{M, s \models \neg\varphi_1}$ iff $M, s \not\models \varphi_1$.
  - $\mathbf{M, s \models \varphi_1 \vee \varphi_2}$ iff $M, s \models \varphi_1$ nebo $M, s \models \varphi_2$.
  - $\mathbf{M, s \models \varphi_1 \wedge \varphi_2}$ iff $M, s \models \varphi_1$ a zároveň $M, s \models \varphi_2$.
  - $\mathbf{M, s \models E\psi_1}$ iff $\exists \pi \in \Pi(M, s).M, s \models \psi_1$.
  - $\mathbf{M, s \models A\psi_1}$ iff $\forall \pi \in \Pi(M, s).M, s \models \psi_1$.

CTL* sémantika [Voj10]

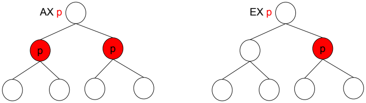
- Pokračování definice relace $\models$:
  - $\mathbf{M}, \boldsymbol{\pi} \models \boldsymbol{\varphi_1}$ iff $M, s_0 \models \varphi_1, s_0 = \pi[0]$.
  - $\mathbf{M}, \boldsymbol{\pi} \models \neg\boldsymbol{\psi_1}$ iff $M, \pi \not\models \psi_1$.
  - $\mathbf{M}, \boldsymbol{\pi} \models \boldsymbol{\psi_1} \vee \boldsymbol{\psi_2}$ iff $M, \pi \models \psi_1$ nebo $M, \pi \models \psi_2$.
  - $\mathbf{M}, \boldsymbol{\pi} \models \boldsymbol{\psi_1} \wedge \boldsymbol{\psi_2}$ iff $M, \pi \models \psi_1$ a zároveň $M, \pi \models \psi_2$.
  - $\mathbf{M}, \boldsymbol{\pi} \models \mathbf{X}\boldsymbol{\psi_1}$ iff $M, \pi^1 \models \psi_1$.
  - $\mathbf{M}, \boldsymbol{\pi} \models \mathbf{F}\boldsymbol{\psi_1}$ iff $\exists i \geq 0 . M, \pi^i \models \psi_1$.
  - $\mathbf{M}, \boldsymbol{\pi} \models \mathbf{G}\boldsymbol{\psi_1}$ iff $\forall i \geq 0 . M, \pi^i \models \psi_1$.
  - $\mathbf{M}, \boldsymbol{\pi} \models \boldsymbol{\psi_1}\mathbf{U}\boldsymbol{\psi_2}$ iff $\exists i \geq 0 . M, \pi^i \models \psi_2$ a zároveň $\forall 0 \leq j < i . M, \pi^j \models \psi_1$.
  - $\mathbf{M}, \boldsymbol{\pi} \models \boldsymbol{\psi_1}\mathbf{R}\boldsymbol{\psi_2}$ iff $\forall i \geq 0 . (\forall 0 \leq j < i . M, \pi^j \not\models \psi_1 \Rightarrow M, \pi^i \models \psi_2$.

CTL* základní operátory [Voj10]

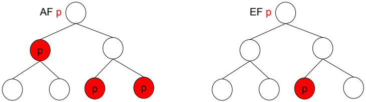
- Všechny CTL* operátory lze odvodit z $\vee$, $\neg$, X, U a E:
  - Nech $p \in AP$, $true \equiv p \vee \neg p$ (a $false \equiv \neg true$)
  - $\varphi \wedge \psi \equiv \neg(\neg\varphi \vee \neg\psi)$,
  - $F\varphi \equiv true U\varphi$,
  - $G\varphi \equiv \neg F \neg\varphi$,
  - $\varphi R \psi \equiv \neg(\neg\varphi U \neg\psi)$,
  - $A\varphi \equiv \neg E \neg\varphi$.

CTL syntaxe [Voj10]

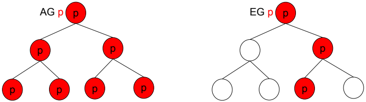
- CTL je sublogikou CTL*
  - běhové formule jsou omezeny na $X\varphi$, $F\varphi$, $G\varphi$, $\varphi U \psi$ a $\varphi R \psi$,
  - kde φ a ψ jsou stavové formule.
- Proto pouze 10 modálních CTL operátorů:
  - *AX* a *EX*



  - *AF* a *EF*

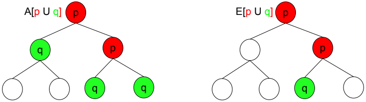


  - *AG* a *EG*

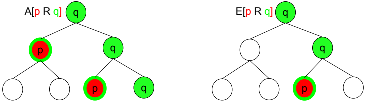


CTL modální operátory [Voj10]

- Modální CTL operátory:
  - *AU* a *EU*



  - *AR* a *ER*



- Existují 3 základní CTL modální operátory - *EX*, *EG* a *EU*:
  - $\mathbf{AX}\varphi \equiv \neg EX\neg\varphi$
  - $\mathbf{EF}\varphi \equiv E[true\, U\varphi]$
  - $\mathbf{AG}\varphi \equiv \neg EF\neg\varphi$
  - $\mathbf{AF}\varphi \equiv \neg EG\neg\varphi$
  - $\mathbf{A[\varphi U\psi]}$ $\equiv \neg E[\neg\psi U(\neg\varphi \wedge \neg\psi)] \wedge \neg EG\neg\psi$
  - $\mathbf{A[\varphi R\psi]} \equiv \neg E[\neg\varphi U\neg\psi]$
  - $\mathbf{E[\varphi R\psi]} \equiv \neg A[\neg\varphi U\neg\psi]$

BNF gramatika specifikačního jazyka [UPP10]

BNF gramatika

- $A[]Expression$
- $E <> Expression$
- $E[]Expression$
- $A <> Expression$
- $Expression --> Expression$

Poznámky

- Žadný výraz nesmí mít postranní efekty.
- Výraz *process.location* testuje, zda určitý proces je v dané pozici.

Příklady specifikačního jazyka [UPP10]

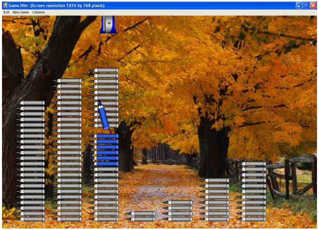
BNF gramatika

- $A[]1 < 2$
  - Invariatně $1 < 2$
- $E <> p1.cs and p2.cs$
  - Pravdivé, pokud systém může dosáhnout stavu, ve kterém procesy *p1* a *p2* jsou v jejich pozici *cs*
- $A <> p1.cs imply not p2.cs$
  - Invariantně process *p1* v pozici *cs* implikuje, že proces *p2* **není** v pozici *cs*.
- $A[] not deadlock$
  - Invariantně, process neobsahuje deadlock.

Jednoduchá varianta NIM

- NIM je hra založená na logice a strategii.
- Hrají 2 hráči.
- Hráč při svém tahu odstraní jednu až *MAX* (2) věci (zápalky, protony) z řady.
- Vyhrává ten hráč, který odstraní poslední věc.

Klasická varianta NIM



- NIM je hra založená na logice a strategii.
- Hrají 2 hráči.
- Hráči odebírají objekty z různých hromádek/řad.
- Hráč musí odstranit při svém tahu alespoň jeden objekt.
- Hráč při svém tahu odstraní libovolný počet objektů, které náleží všechny k jedné hromádce.
- Základní varianty hry:
    - **Normální** . . . Vyhrává ten hráč, který odstraní poslední věc.
    - **Prohra** . . . Prohrává ten hráč, který odstraní poslední věc.

Literatura I

Tool environment for validation and verification of real-time systems (UPPAAL pamphlet).
http://www.it.uu.se/research/group/darts/papers/texts/uppaal-pamphlet.pdf, September 2010.

Tomas Vojnar.
Formal analysis and verification.
Lecture handouts, http://www.fit.vutbr.cz/study/courses/FAV/public/, August 2010.

Linear temporal logic.
http://en.wikipedia.org/wiki/Linear_temporal_logic, November 2010.