

Logika dla informatyków

Andrzej M. Borzyszkowski

Instytut Informatyki
Uniwersytet Gdański

inf.ug.edu.pl/~amb

Pewne równoważności logiki LTL

Definicja

Formuła φ jest semantyczną konsekwencją ψ , $\psi \Rightarrow \varphi$, jeśli dla wszystkich modeli $\mathcal{M}$ i wszystkich ścieżek π zachodzi $\pi \models \psi$ pociąga $\pi \models \varphi$.

Formuły φ oraz ψ są semantycznie równoważne, $\varphi \equiv \psi$, jeśli $\psi \Rightarrow \varphi$ oraz $\varphi \Rightarrow \psi$.

Równoważności w LTL

Pewne równoważności logiki LTL

Twierdzenie

- dualność:

$$\neg G\varphi \equiv F\neg\varphi \quad G\neg\varphi \equiv \neg F\varphi \quad \neg X\varphi \equiv X\neg\varphi \\ \neg(\varphi U \psi) \equiv \neg\varphi R \neg\psi \quad \neg(\varphi R \psi) \equiv \neg\varphi U \neg\psi$$

- rozdzielczość:

$$F(\varphi \vee \psi) \equiv F\varphi \vee F\psi \quad G(\varphi \wedge \psi) \equiv G\varphi \wedge G\psi \\ F(\varphi \wedge \psi) \Rightarrow F\varphi \wedge F\psi \quad G\varphi \vee G\psi \Rightarrow G(\varphi \vee \psi) \\ GF(\varphi \vee \psi) \equiv GF\varphi \vee GF\psi \quad FG(\varphi \wedge \psi) \equiv FG\varphi \wedge FG\psi \\ (\varphi \wedge \psi) U \sigma \equiv \varphi U \sigma \wedge \psi U \sigma \quad \varphi U (\psi \vee \sigma) \equiv \varphi U \psi \vee \varphi U \sigma$$

- idempotencja:

$$FF\varphi \equiv F\varphi \quad GG\varphi \equiv G\varphi \\ \varphi U (\varphi U \psi) \equiv \varphi U \psi \quad (\varphi U \psi) U \psi \equiv \varphi U \psi$$

- pochłanianie: $FGF\varphi \equiv GF\varphi \quad GFG\varphi \equiv FG\varphi$

- rozszerzenie: $\varphi U \psi \equiv \psi \vee (\varphi \wedge X(\varphi U \psi))$

$$F\varphi \equiv \varphi \vee XF\varphi \quad G\varphi \equiv \varphi \wedge XG\varphi$$

Pewne równoważności logiki LTL, c.d.

Wniosek

- *dualność:*
 $GF\neg\varphi \equiv \neg FG\varphi \quad FG\neg\varphi \equiv \neg GF\varphi$
- *rozdzielczość:*
 $FG\varphi \vee FG\psi \Rightarrow FG(\varphi \vee \psi) \quad GF(\varphi \wedge \psi) \Rightarrow GF\varphi \wedge GF\psi$
 $\varphi U \sigma \vee \psi U \sigma \Rightarrow (\varphi \vee \psi) U \sigma \quad \varphi U (\psi \wedge \sigma) \Rightarrow \varphi U \psi \wedge \varphi U \sigma$
- *pochłanianie:*
 $FG\varphi \equiv FG FG\varphi \equiv GF FG\varphi$
 $GF\varphi \equiv GF GF\varphi \equiv FG GF\varphi$

Pozytywna postać normalna

Negacja jest dozwolona wyłącznie dla zdań atomowych

$$\varphi ::= \top \mid \perp \mid p \mid \neg p \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi) \mid (X\varphi) \mid (\varphi U \varphi) \mid (\varphi R \varphi)$$

Pozostałe spójniki można wydefiniować na podstawie w/w wymienionych

- wystarczy któryś z zestawów: $\{U, R\}$, $\{U, W\}$, $\{U, G\}$, $\{R, F\}$ albo $\{W, F\}$
- zestawy $\{W, G\}$, $\{R, G\}$ i $\{U, F\}$ nie są wystarczające, bo:
 - nie można zdefiniować F za pomocą $\{R, G\}$ ani $\{W, G\}$
 - nie można zdefiniować G za pomocą $\{U, F\}$

może wymagać to skopiowania podformuły (problem ze złożonością)

Twierdzenie

Dla każdej formuły LTL istnieje równoważna w pozytywnej postaci normalnej, co więcej długość jest zbliżona.

Pewne równoważności logiki LTL, spójniki

Twierdzenie

- *definiowanie spójników za pomocą innych:*
 $F\varphi \equiv \top U \varphi \quad G\varphi \equiv \perp R \varphi$
 $\varphi U \psi \equiv \varphi W \psi \wedge F\psi \quad \varphi W \psi \equiv \varphi U \psi \vee G\varphi$
 $\varphi W \psi \equiv \psi R (\varphi \vee \psi) \quad \varphi R \psi \equiv \psi W (\varphi \wedge \psi)$

Nie wszystkie spójniki występujące w LTL są niezbędne

- X nie da się z niczym innym porównać, więc musi być zawsze obecny w języku
- każdy ze spójników U , W , R wystarczy by wyrazić pozostałe dwa oraz F i G

Własności uczciwości (*fairness*) w logice LTL

- bezpieczeństwo łatwo gwarantować – uniemożliwiając współbieżność procesów
- w praktyce chcemy współbieżności – trzeba coś ekstra zakładać
- uczciwość bezwarunkowa: $GF\varphi$, proces na pewno będzie mógł wykazać się zachowaniem (ale czy będzie tego żądał)
- silna własność uczciwości: $GF\varphi \rightarrow GF\psi$, jeśli proces będzie wielokrotnie żądał, to będzie wielokrotnie obsłużony (ale implementacja może cyklicznie zbierać zamówienia i akurat rozminie się w fazie)
- słaba własność uczciwości: $FG\varphi \rightarrow GF\psi$, jeśli proces będzie żądał bezustannie, to zostanie wielokrotnie obsłużony (ta własność powinna zachodzić, ale nie chcemy zachęcać procesów do bezustannego żądania)

Przykład mutex c.d.

- oprócz procesów 1 i 2 chodzących w cyklu $n \rightarrow t \rightarrow r \rightarrow n$ rozpatrujemy arbitra bezustannie losującego dostęp do obszaru krytycznego dla jednego z procesów
- nie można udowodnić, że proces 1 otrzyma dostęp, bo być może arbiter zawsze losuje nr 2
- jeśli arbiter spełnia warunek uczciwości $GF1 \wedge GF2$, i rozpatrujemy model wyłącznie z uczciwymi ścieżkami, to będzie zachodzić własność $GF_{C_1} \wedge GF_{C_2}$

Wzorce własności LTL – Nieistnienie

Własność φ jest fałszywa:

globalnie:	$G(\neg\varphi)$
przed τ :	$F\tau \Rightarrow (\neg\varphi \ U \ \tau)$
po σ :	$G(\sigma \Rightarrow G(\neg\varphi))$
pomiędzy σ i τ :	$G((\sigma \wedge \neg\tau \wedge F\tau) \Rightarrow (\neg\varphi \ U \ \tau))$
po σ do chwili, gdy τ :	$G(\sigma \wedge \neg\tau \Rightarrow (\neg\varphi \ W \ \tau))$

Wzorce użytecznych formuł LTL

Wzorce własności LTL – Istnienie

Własność φ staje się prawdziwa:

globalnie:	$F(\varphi)$
przed τ :	$\neg\tau \ W \ (\varphi \wedge \neg\tau)$
po σ :	$G(\neg\sigma) \vee F(\sigma \wedge F\varphi)$
pomiędzy σ i τ :	$G(\sigma \wedge \neg\tau \Rightarrow (\neg\tau \ W \ (\varphi \wedge \neg\tau)))$
po σ do chwili, gdy τ :	$G(\sigma \wedge \neg\tau \Rightarrow (\neg\tau \ U \ (\varphi \wedge \neg\tau)))$

Wzorce własności LTL – Uniwersalność

Własność φ jest prawdziwa:

globalnie:	$G(\varphi)$
przed τ :	$F\tau \Rightarrow (\varphi \ U \ \tau)$
po σ :	$G(\sigma \Rightarrow G(\varphi))$
pomiędzy σ i τ :	$G((\sigma \wedge \neg\tau \wedge F\tau) \Rightarrow (\varphi \ U \ \tau))$
po σ do chwili, gdy τ :	$G(\sigma \wedge \neg\tau \Rightarrow (\varphi \ W \ \tau))$

Wzorce własności LTL – Związek przyczynowo skutkowy 2

Własność ψ jest niezbędnym warunkiem własności φ :

globalnie:	$\neg\varphi \ W \ \psi$
przed τ :	$F\tau \Rightarrow (\neg\varphi \ U \ (\psi \vee \tau))$
po σ :	$G\neg\sigma \vee F(\sigma \wedge (\neg\varphi \ W \ \psi))$
pomiędzy σ i τ :	$G((\sigma \wedge \neg\tau \wedge F\tau) \Rightarrow (\neg\varphi \ U \ (\psi \vee \tau)))$
po σ do chwili, gdy τ :	$G(\sigma \wedge \neg\tau \Rightarrow (\neg\varphi \ W \ (\psi \vee \tau)))$

Wzorce własności LTL – Związek przyczynowo skutkowy 1

Własność φ pociąga własność ψ :

globalnie:	$G(\varphi \Rightarrow F\psi)$
przed τ :	$F\tau \Rightarrow (\varphi \Rightarrow (\neg\tau \ U \ (\psi \wedge \neg\tau))) \ U \ \tau$
po σ :	$G(\sigma \Rightarrow G(\varphi \Rightarrow F\psi))$
pomiędzy σ i τ :	$G((\sigma \wedge \neg\tau \wedge F\tau) \Rightarrow (\varphi \Rightarrow (\neg\tau \ U \ (\psi \wedge \neg\tau))) \ U \ \tau)$
po σ do chwili, gdy τ :	$G(\sigma \wedge \neg\tau \Rightarrow ((\varphi \Rightarrow (\neg\tau \ U \ (\psi \wedge \neg\tau))) \ W \ \tau))$

Inne wzorce

Przykłady innych „wzorców własności” wyrażonych w języku logiki LTL znaleźć można na stronie Spec Patterns:

<http://patterns.projects.cis.ksu.edu/>