Logika

LTL és CTL

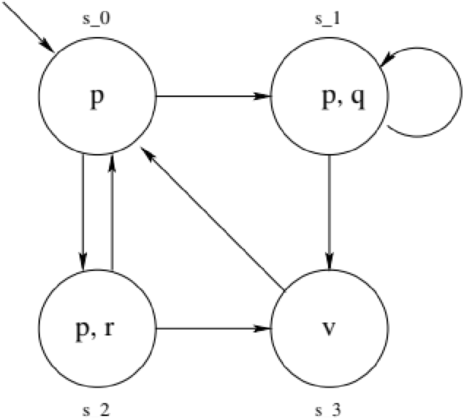
December 10, 2020

Kripke-struktúra

- Legyen adott egy AP címkehalmaz – atomi propozíciók halmaza (boolean kifejezések változók, konstansok és predikátumszimbólumok felett).
- Kripke struktúra: M = (S, I, R, L) rendezett négyes, ahol
  - adott állapotok egy véges S halmaza
  - az iniciális állapotok $I \subseteq S$ halmaza
  - az $R \subseteq S \times$ S átmenetreláció, amire $\forall s \in S, \exists s' \in S : sRs'$
  - egy $L : S \to 2^{AP}$ címkézőfüggvény

Kripke-struktúra – példa

$S = \{s_0, s_1, s_2, s_3\}$
$I = s_0$
$R = \{(s_0, s_1), (s_0, s_2), (s_1, s_1), (s_1, s_3), (s_2, s_0), (s_2, s_3), (s_3, s_0)\}$
$L = \{(s_0, \{p\}), (s_1, \{p, q\}), (s_2, \{p, r\}), (s_3, \{v\})\}$



Végtelen utak

- Az LTL és CTL végtelen utakkal foglalkozik.
- $\pi = (\pi_0, \pi_1, \pi_2 ...)$ egy végtelen út az M Kripke-struktúrában, ha $\forall i \in \mathbb{N} : \pi_i R \pi_{i+1}$, ahol R M átmenetrelációja.
- Jelölje π^i π i. szuffixét: $\pi^i = (\pi_i, \pi_{i+1}, \pi_{i+2}, ...)$
- $(\pi^i)^j = (\pi_i, \pi_{i+1}, \pi_{i+2}, ...)^j = (\pi_{i+j}, \pi_{i+j+1}, \pi_{i+j+2}, ...) = \pi^{i+j}$

LTL BNF szintaxis

A Φ LTL formulákat az alábbi BNF alakkal tudjuk megadni:

$$
\begin{array}{rrl}
\Phi ::= & \top & ;\ \text{igaz/top} \\
| & \bot & ;\ \text{hamis/bottom} \\
| & p & ;\ \text{ahol p} \in AP \\
| & \neg\Phi & ;\ \text{negáció} \\
| & \Phi \wedge \Phi & ;\ \text{konjunkció} \\
| & \Phi \vee \Phi & ;\ \text{diszjunkció} \\
| & X\Phi & ;\ \text{következő alkalommal (next time)} \\
| & F\Phi & ;\ \text{végül (eventually)} \\
| & G\Phi & ;\ \text{mindig (always)} \\
| & \Phi U \Phi & ;\ \text{amíg (until)}
\end{array}
$$

Mostantól a kisbetűk jelöljék az atomi propozíciókat (pl. p, q, r), a nagy görög betűk pedig a formulákat (pl. Φ, Ψ)!

LTL szemantika – alapok

Definiáljuk a $\models$ relációt LTL formulákra! Legyen M Kripke-struktúra, π pedig egy út benne! Ekkor $(M, \pi) \models \Phi$ jelentése: (M, π) kielégíti a Φ formulát.

- $(M, \pi) \models \top$
  Az igaz állítást minden kielégíti.
- $(M, \pi) \not\models \bot$
  A hamis állítást semmi sem elégíti ki.
- $(M, \pi) \models p \iff p \in L(\pi_0)$
  Egy atomi propozíció akkor kielégített, ha benne van a π út első elemének címkehalmazában.

LTL szemantika – boolean operátorok

- $(M, \pi) \models \neg\Phi \iff (M, \pi) \not\models \Phi$
- $(M, \pi) \models \Phi \wedge \Psi \iff ((M, \pi) \models \Phi) \wedge ((M, \pi) \models \Psi)$
- $(M, \pi) \models \Phi \vee \Psi \iff ((M, \pi) \models \Phi) \vee ((M, \pi) \models \Psi)$

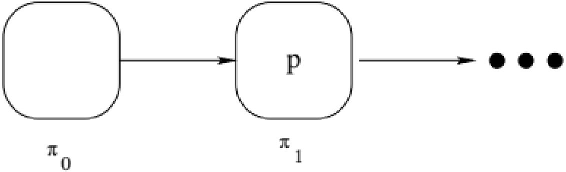
LTL szemantika – temporális operátorok

- $(M, \pi) \models X\Phi \iff (M, \pi^1) \models \Phi$
- $(M, \pi) \models F\Phi \iff \exists i \in \mathbb{N} : (M, \pi^i) \models \Phi$
- $(M, \pi) \models G\Phi \iff \forall i \in \mathbb{N} : (M, \pi^i) \models \Phi$
- $(M, \pi) \models \Phi U \Psi \iff$
  $\exists i \in \mathbb{N} : [\forall j \in \mathbb{N} : [(j < i) \supset ((M, \pi^j) \models \Phi)] \wedge ((M, \pi^i) \models \Psi)]$

Megjegyzés: az itt használt U az ún. erős until. Létezik egy gyenge változata is: $\Phi U_w \Psi \Leftrightarrow (\Phi U \Psi \vee G\Phi)$

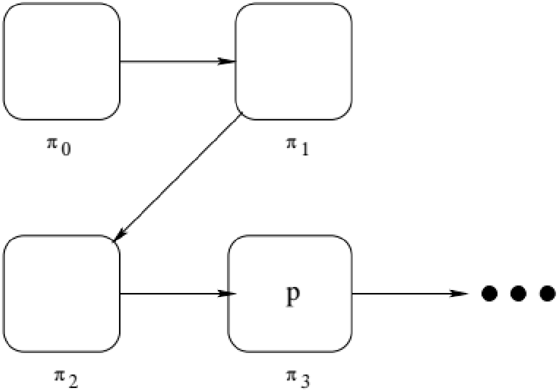
Xp – példa

$(M, (\pi_0, \pi_1, \ldots)) \models Xp$



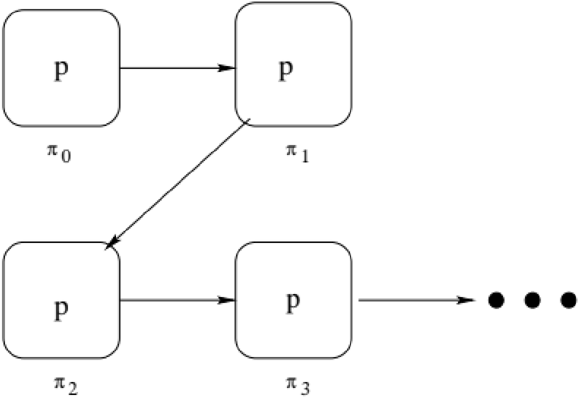
Fp – példa

$(M, (\pi_0, \pi_1, \pi_2, \pi_3, ...)) \models Fp$



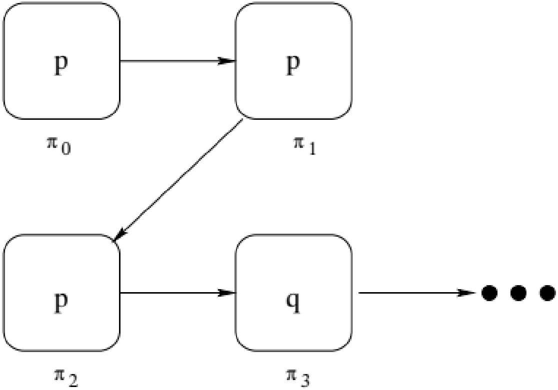
Gp – példa

$(M, (\pi_0, \pi_1, \pi_2, \pi_3, ...)) \models Gp$

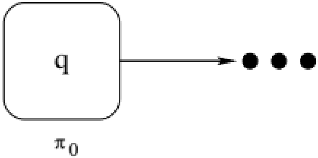


pUq – példa

$(M, (\pi_0, \pi_1, \pi_2, \pi_3, ...)) \models pUq$



pUq – példa 2.



$(M, (\pi_0, ...)) \models pUq$

További LTL szemantika

- $(M \models_M \Phi) \iff \forall \pi : ((\pi_0 \in I) \supset ((M, \pi) \models \Phi))$
  Egy modell (Kripke-struktúra) akkor elégít ki egy LTL formulát, amikor minden útja kielégíti.
- $(\Phi \equiv \Psi) \iff (\forall M : [(M \models_M \Phi) \equiv (M \models_M \Psi)])$
  Két LTL formula ekvivalens, ha ugyanazok a Kripke-struktúrák elégítik ki őket.

LTL formulák ekvivalenciája – példa

$X(\Phi \wedge \Psi) \equiv X\Phi \wedge X\Psi$

Be szeretnénk látni, hogy minden M-re és π-re:

$((M, \pi) \models X(\Phi \wedge \Psi)) \equiv ((M, \pi) \models X\Phi \wedge X\Psi)$

$$
\begin{aligned}
(M, \pi) \models X(\Phi \wedge \Psi) &= \\
(M, \pi^1) \models (\Phi \wedge \Psi) &= && \text{X definíciójából} \\
((M, \pi^1) \models \Phi) \wedge ((M, \pi^1) \models \Psi) &= && \wedge \text{ definíciójából} \\
((M, \pi) \models X\Phi) \wedge ((M, \pi) \models X\Psi) &= && \text{X definíciójából} \\
((M, \pi) \models X\Phi \wedge X\Psi) & && \wedge \text{ definíciójából}
\end{aligned}
$$

További LTL-ekvivalenciák

$$X(\Phi \wedge \Psi) \equiv X\Phi \wedge X\Psi$$
$$X(\Phi \vee \Psi) \equiv X\Phi \vee X\Psi$$
$$X(\Phi U \Psi) \equiv (X\Phi) U (X\Psi)$$
$$\neg X\Phi \equiv X\neg\Phi$$

$$F(\Phi \wedge \Psi) \equiv F\Phi \wedge F\Psi$$
$$F(\Phi \vee \Psi) \equiv F\Phi \vee F\Psi$$
$$\neg F\Phi \equiv F\neg\Phi$$

$$(\Phi \wedge \Psi) U \Theta \equiv (\Phi U \Theta) \wedge (\Psi U \Theta)$$
$$\Theta U (\Phi \vee \Psi) \equiv (\Theta U \Phi) \vee (\Theta U \Psi)$$

$$FF\Phi \equiv F\Phi$$
$$GG\Phi \equiv G\Phi$$

CTL BNF szintaxis

A Φ CTL formulákat az alábbi BNF alakkal tudjuk megadni:

$$
\begin{array}{rrl}
\Phi ::= & \top & ; \\
| & \bot & ; \\
| & p & ; \\
| & \neg\Phi & ; \\
| & \Phi \wedge \Phi & ; \\
| & \Phi \vee \Phi & ; \\
| & AX\Phi & ; \text{A : minden útra} \\
| & AF\Phi & ; \\
| & AG\Phi & ; \\
| & \Phi AU\Phi & ; \\
| & EX\Phi & ; \text{E : létezik út, amire} \\
| & EF\Phi & ; \\
| & EG\Phi & ; \\
| & \Phi EU\Phi & ;
\end{array}
$$

Megjegyzés: Az AX, AF, stb. mindegyike egy (két karakterből álló) szimbólum.

CTL szemantika – alapok

Adjuk meg CTL-hez is a $\models$ relációt. Legyen M Kripke-struktúra, s pedig egy állapot benne!

- $(M, s) \models \top$
- $(M, s) \not\models \bot$
- $((M, s) \models p) \iff (p \in L(s))$
  Egy atomi propozíció akkor kielégített, ha benne van az állapot címkehalmazában.

CTL szemantika – boolean operátorok

- $(M, s) \models \neg\Phi \iff (M, s) \not\models \Phi$
- $(M, s) \models \Phi \wedge \Psi \iff ((M, s) \models \Phi) \wedge ((M, s) \models \Psi)$
- $(M, s) \models \Phi \vee \Psi \iff ((M, s) \models \Phi) \vee ((M, s) \models \Psi)$

CTL szemantika – temporális operátorok (A)

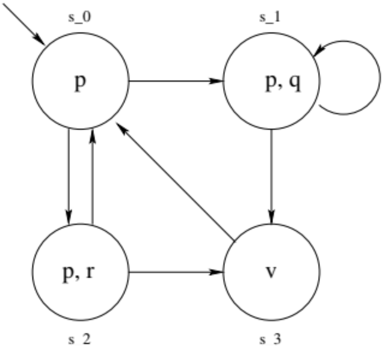
- $((M, s) \models AX\Phi) \iff (\forall \pi : ((\pi_0 = s) \supset ((M, \pi^1) \models \Phi)))$
- $((M, s) \models AF\Phi) \iff (\forall \pi : ((\pi_0 = s) \supset (\exists i : (M, \pi^i) \models \Phi)))$
- $((M, s) \models AG\Phi) \iff (\forall \pi : ((\pi_0 = s) \supset (\forall i : (M, \pi^i) \models \Phi)))$
- $((M, s) \models \Phi AU \Psi) \iff$
  $(\forall \pi : ((\pi_0 = s) \supset (\exists i : \forall j < i : ((M, \pi^j) \models \Phi) \land ((M, \pi^i) \models \Psi))$

CTL szemantika – temporális operátorok (E)

- $((M, s) \models EX\Phi) \iff (\exists\pi : ((\pi_0 = s) \supset ((M, \pi^1) \models \Phi)))$
- $((M, s) \models EF\Phi) \iff (\exists\pi : ((\pi_0 = s) \supset (\exists i : (M, \pi^i) \models \Phi)))$
- $((M, s) \models EG\Phi) \iff (\exists\pi : ((\pi_0 = s) \supset (\forall i : (M, \pi^i) \models \Phi)))$
- $((M, s) \models \Phi EU\Psi) \iff$
  $(\exists\pi : ((\pi_0 = s) \supset (\exists i : \forall j < i : ((M, \pi^j) \models \Phi) \wedge ((M, \pi^i) \models \Psi))$

AX – példa

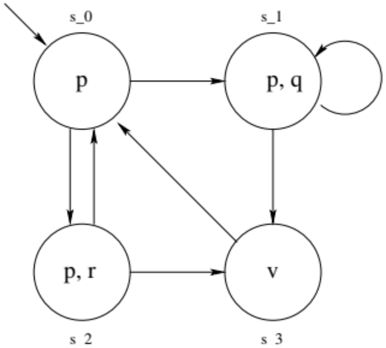
$S = \{s_0, s_1, s_2, s_3\}$
$I = s_0$
$R = \{(s_0, s_1), (s_0, s_2), (s_1, s_1), (s_1, s_3), (s_2, s_0), (s_2, s_3), (s_3, s_0)\}$
$L = \{(s_0, \{p\}), (s_1, \{p, q\}), (s_2, \{p, r\}), (s_3, \{v\})\}$



$(M, s_0) \models AXp$

EF – példa

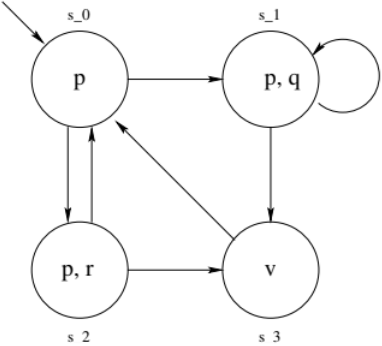
$S = \{s_0, s_1, s_2, s_3\}$
$I = s_0$
$R = \{(s_0, s_1), (s_0, s_2), (s_1, s_1), (s_1, s_3), (s_2, s_0), (s_2, s_3), (s_3, s_0)\}$
$L = \{(s_0, \{p\}), (s_1, \{p, q\}), (s_2, \{p, r\}), (s_3, \{v\})\}$



$(M, s_0) \models EFv$

AG – példa

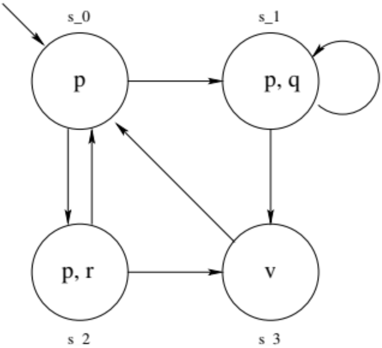
$S = \{s_0, s_1, s_2, s_3\}$
$I = s_0$
$R = \{(s_0, s_1), (s_0, s_2), (s_1, s_1), (s_1, s_3), (s_2, s_0), (s_2, s_3), (s_3, s_0)\}$
$L = \{(s_0, \{p\}), (s_1, \{p, q\}), (s_2, \{p, r\}), (s_3, \{v\})\}$



$(M, s_0) \models AG(p \vee v)$

EU – példa

$S = \{s_0, s_1, s_2, s_3\}$
$I = s_0$
$R = \{(s_0, s_1), (s_0, s_2), (s_1, s_1), (s_1, s_3), (s_2, s_0), (s_2, s_3), (s_3, s_0)\}$
$L = \{(s_0, \{p\}), (s_1, \{p, q\}), (s_2, \{p, r\}), (s_3, \{v\})\}$



$(M, s_0) \models pEUv$

További CTL szemantika

- $(M \models_M \Phi) \iff \forall\pi : ((\pi_0 \in I) \supset ((M, \pi) \models \Phi))$
  Egy modell (Kripke-struktúra) akkor elégít ki egy CTL formulát, amikor minden állapota kielégíti.
- $(\Phi \equiv \Psi) \iff (\forall M : [(M \models_M \Phi) \equiv (M \models_M \Psi)])$
  Két CTL formula ekvivalens, ha ugyanazok a Kripke-struktúrák elégítik ki őket.

CTL ekvivalenciák

$$AX(\Phi \wedge \Psi) \equiv AX\Phi \wedge AX\Psi$$
$$EX(\Phi \vee \Psi) \equiv EX\Phi \vee EX\Psi$$
$$\neg AX\Phi \equiv EX\neg\Phi$$

$$EF(\Phi \vee \Psi) \equiv EF\Phi \vee EF\Psi$$
$$AG(\Phi \wedge \Psi) \equiv AG\Phi \wedge AG\Psi$$
$$\neg AF\Phi \equiv EG\neg\Phi$$
$$\neg EF\Phi \equiv AG\neg\Phi$$

$$AFAF\Phi \equiv AF\Phi$$
$$EFEF\Phi \equiv EF\Phi$$
$$AGAG\Phi \equiv AG\Phi$$
$$EGEG\Phi \equiv EG\Phi$$

CTL vs LTL – komplexitás

- $|\Phi| = n, |M| = m$
- CTL: $O(mn)$
- LTL: $O(m * 2^n)$ – és PSPACE-teljes

LTL-CTL-ekvivalencia

Egy Φ_{LTL} LTL-formula és egy Φ_{CTL} CTL-formula ekvivalens, ha ugyanazon Kripke-struktúrák elégítik ki őket:

$$\Phi_{LTL} \equiv \Phi_{CTL} \iff [(M \models_M \Phi_{LTL}) \Leftrightarrow (M \models_M \Phi_{CTL})]$$

LTL vs CTL – E, G

- Nincs olyan E-t tartalmazó CTL-formula, ami kifejezhető LTL-ben
- Ha egy Φ_{LTL} LTL-formulára és egy Φ_{CTL} CTL-formulára $\Phi_{LTL} \equiv \Phi_{CTL}$, akkor $G\Phi_{LTL} \equiv AG\Phi_{CTL}$