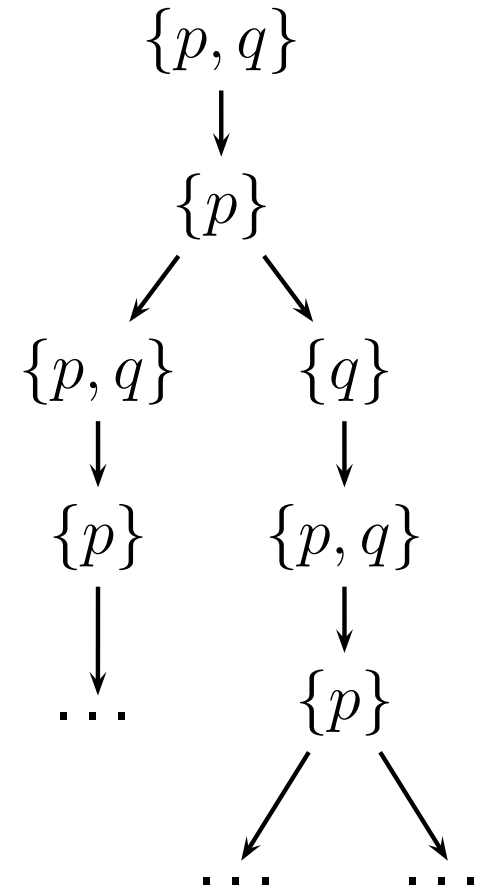
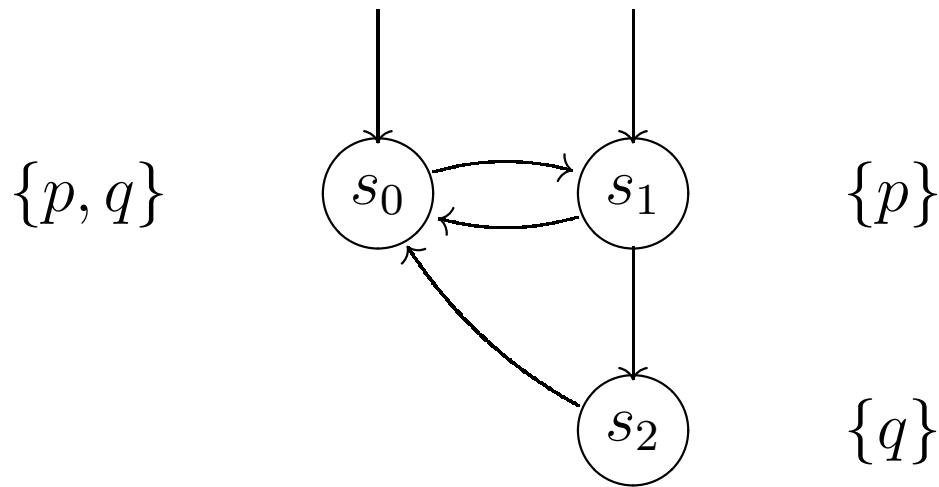


Praktyczne metody weryfikacji

Wykład 6: CTL

Struktura Kripkego \mapsto drzewo



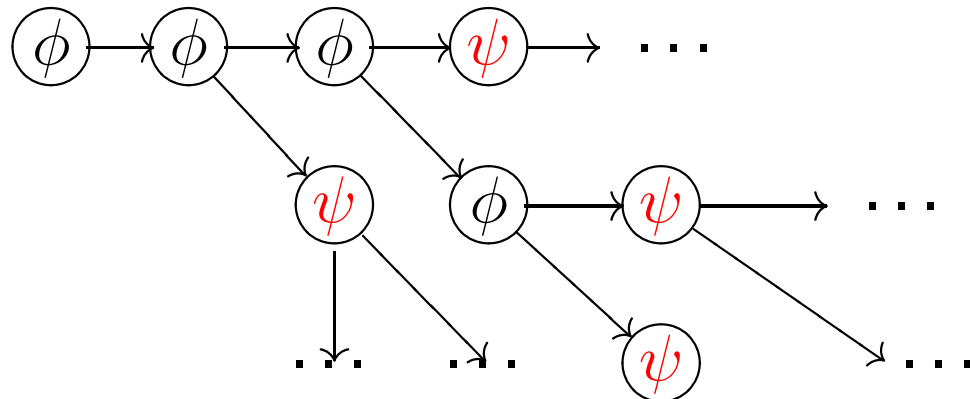
Def.: CTL (Computation Tree Logic)

$\phi ::= p \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \mathbf{AX} \phi \mid \mathbf{EX} \phi \mid \mathbf{A} \phi_1 \mathbf{U} \phi_2 \mid \mathbf{E} \phi_1 \mathbf{U} \phi_2$

$\mathbf{A} \phi \mathbf{U} \psi \equiv$ na **każdej** ścieżce zachodzi $\phi \mathbf{U} \psi$

$\mathbf{E} \phi \mathbf{U} \psi \equiv$ na **pewnej** ścieżce zachodzi $\phi \mathbf{U} \psi$

$\mathbf{A} \phi \mathbf{U} \psi$



Notacja:

$AF \phi \equiv A \text{ true } U \phi$

$EF \phi \equiv E \text{ true } U \phi$

$AG \phi \equiv ?$

$EG \phi \equiv ?$

Przykład:

$AF \text{ sek_kryt}, \quad AF \text{ EF start}$

Notacja:

$$AF \phi \equiv A \text{ true } U \phi$$

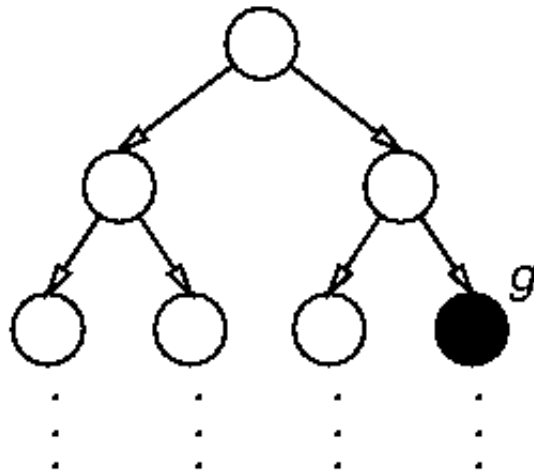
$$EF \phi \equiv E \text{ true } U \phi$$

$$AG \phi \equiv \neg EF \neg \phi$$

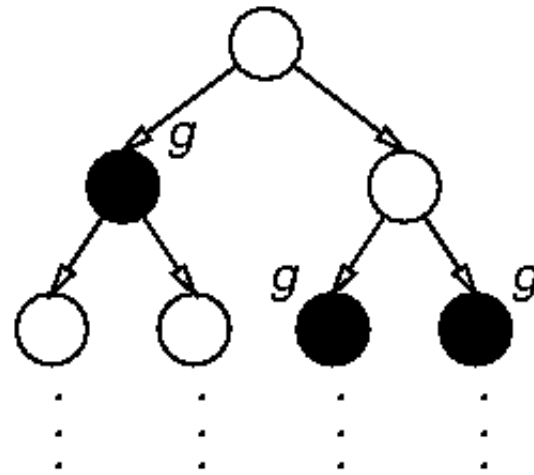
$$EG \phi \equiv \neg AF \neg \phi$$

Przykład:

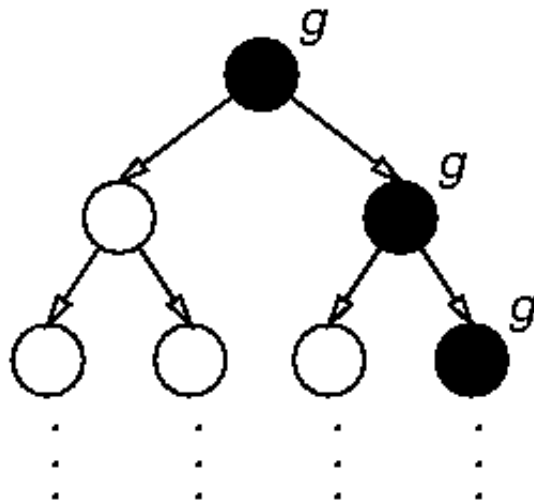
$$AG (q \implies AF r), \quad AG AF \text{ enabled}$$



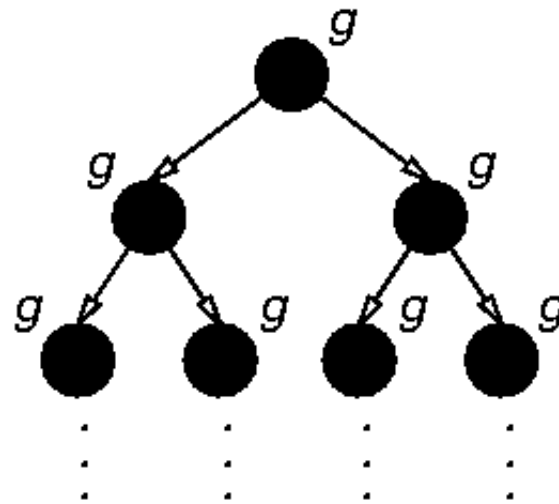
$M, s_0 \models \text{EF } g$



$M, s_0 \models \text{AF } g$



$M, s_0 \models \text{EG } g$



$M, s_0 \models \text{AG } g$

[Clarke, Grumberg, Long 1994]

Semantyka: $M = \langle S, S_{\text{pocz}}, \rightarrow, L \rangle$ struktura Kripkego

$M \models \phi$ wtw gdy $\forall s \in S_{\text{pocz}} \ s \models \phi$

$s \models \neg\phi$ wtw gdy ...

$s \models \phi_1 \wedge \phi_2$ wtw gdy ...

$s \models p$ wtw gdy $p \in L(s)$

$s \models \mathbf{AX} \phi$ wtw gdy $\forall s'. \ s \rightarrow s' \implies s' \models \phi$

$s \models \mathbf{EX} \phi$ wtw gdy $\exists s'. \ s \rightarrow s' \wedge s' \models \phi$

$s \models \mathbf{A} \phi_1 \mathbf{U} \phi_2$ wtw gdy $\forall \Pi. \ \Pi$ zaczyna się w $s \implies \Pi \models \phi_1 \mathbf{U} \phi_2$
($\Pi = s_0 \ s_1 \ \dots \quad \exists i. \ s_i \models \phi_2 \wedge \forall j < i. \ s_j \models \phi_1$)

$s \models \mathbf{E} \phi_1 \mathbf{U} \phi_2$ wtw gdy $\exists \Pi. \ \Pi$ zaczyna się w $s \wedge \Pi \models \phi_1 \mathbf{U} \phi_2$

Semantyka: $M = \langle S, S_{\text{pocz}}, \rightarrow, L \rangle$ struktura Kripkego

$M \models \phi$ wtw gdy $\forall s \in S_{\text{pocz}} s \models \phi$

$s \models \neg\phi$ wtw gdy ...

$s \models \phi_1 \wedge \phi_2$ wtw gdy ...

$s \models p$ wtw gdy $p \in L(s)$

$s \models \mathbf{AX} \phi$ wtw gdy $\forall \Pi. \Pi$ zaczyna się w $s \implies \Pi \models \mathbf{X} \phi$

$s \models \mathbf{EX} \phi$ wtw gdy $\exists \Pi. \Pi$ zaczyna się w $s \wedge \Pi \models \mathbf{X} \phi$

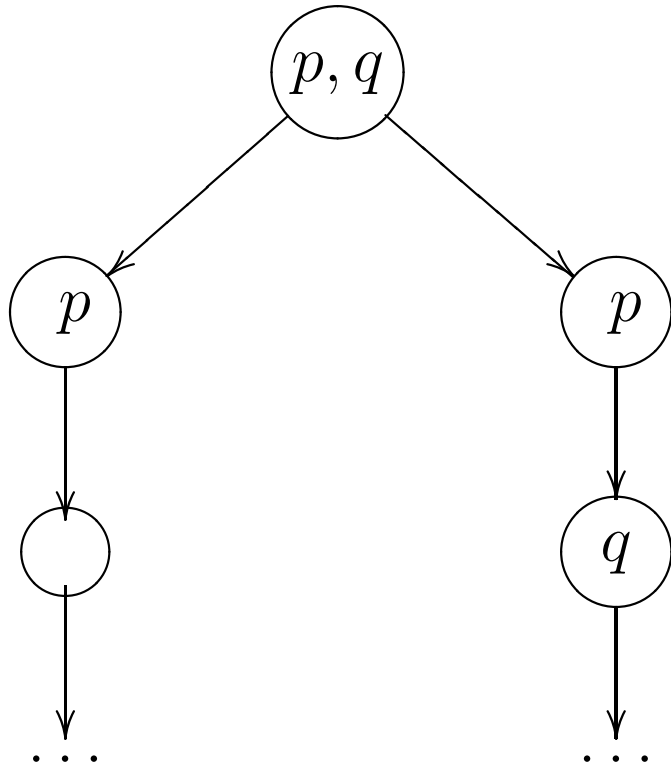
$s \models \mathbf{A} \phi_1 \mathbf{U} \phi_2$ wtw gdy $\forall \Pi. \Pi$ zaczyna się w $s \implies \Pi \models \phi_1 \mathbf{U} \phi_2$
($\Pi = s_0 s_1 \dots \quad \exists i. s_i \models \phi_2 \wedge \forall j < i. s_j \models \phi_1$)

$s \models \mathbf{E} \phi_1 \mathbf{U} \phi_2$ wtw gdy $\exists \Pi. \Pi$ zaczyna się w $s \wedge \Pi \models \phi_1 \mathbf{U} \phi_2$

W LTL czas był **liniowy**.

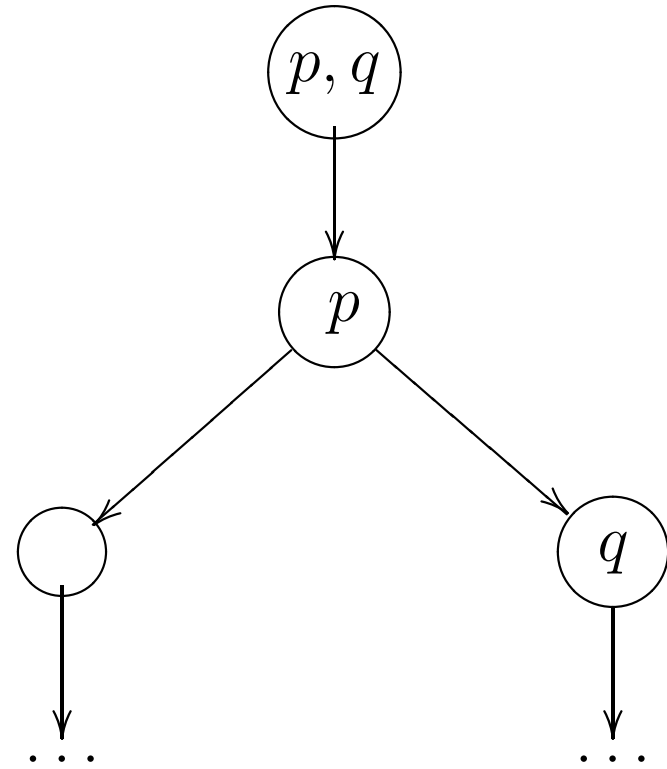
W CTL czas jest **rozgałęziony!**

czas liniowy vs czas rozgałęziony



=LTL

≠CTL



Def.: CTL⁺

$$\phi ::= p \mid \neg p \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \mathbf{AX} \phi \mid \mathbf{EX} \phi \mid$$
$$\mathbf{A} \phi_1 \mathbf{U} \phi_2 \mid \mathbf{E} \phi_1 \mathbf{U} \phi_2 \mid \mathbf{A} \phi_1 \mathbf{R} \phi_2 \mid \mathbf{E} \phi_1 \mathbf{R} \phi_2$$

$\mathbf{A} \phi \mathbf{R} \psi \equiv$ na **każdej** ścieżce zachodzi $\phi \mathbf{R} \psi$

$\mathbf{E} \phi \mathbf{R} \psi \equiv$ na **pewnej** ścieżce zachodzi $\phi \mathbf{R} \psi$

$\mathbf{A} \phi \mathbf{R} \psi \equiv ?$

$\mathbf{E} \phi \mathbf{R} \psi \equiv ?$

Def.: CTL⁺

$$\phi ::= p \mid \neg p \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \mathbf{AX} \phi \mid \mathbf{EX} \phi \mid \\ \mathbf{A} \phi_1 \mathbf{U} \phi_2 \mid \mathbf{E} \phi_1 \mathbf{U} \phi_2 \mid \mathbf{A} \phi_1 \mathbf{R} \phi_2 \mid \mathbf{E} \phi_1 \mathbf{R} \phi_2$$

$\mathbf{A} \phi \mathbf{R} \psi \equiv$ na **każdej** ścieżce zachodzi $\phi \mathbf{R} \psi$

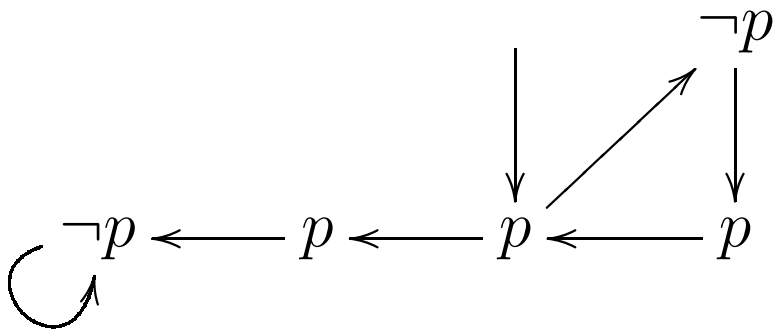
$\mathbf{E} \phi \mathbf{R} \psi \equiv$ na **pewnej** ścieżce zachodzi $\phi \mathbf{R} \psi$

$$\mathbf{A} \phi \mathbf{R} \psi \equiv \neg \mathbf{E} \neg \phi \mathbf{U} \neg \psi$$

$$\mathbf{E} \phi \mathbf{R} \psi \equiv \neg \mathbf{A} \neg \phi \mathbf{U} \neg \psi$$

LTL	CTL	uwagi
$G p, F p$	$AG p, AF p$	
$G F p$	$AG AF p$	
$G (r \implies F g)$	$AG (r \implies AF g)$	\in ACTL
—	$EF p, EG p$	$\neg(M \models G \neg p)$
—	$AG EF \text{ start}$	

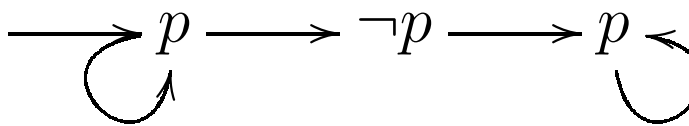
LTL vs CTL

LTL	CTL	uwagi
$F(p \wedge Xp)$ —	— $AF(p \wedge AXp)$	

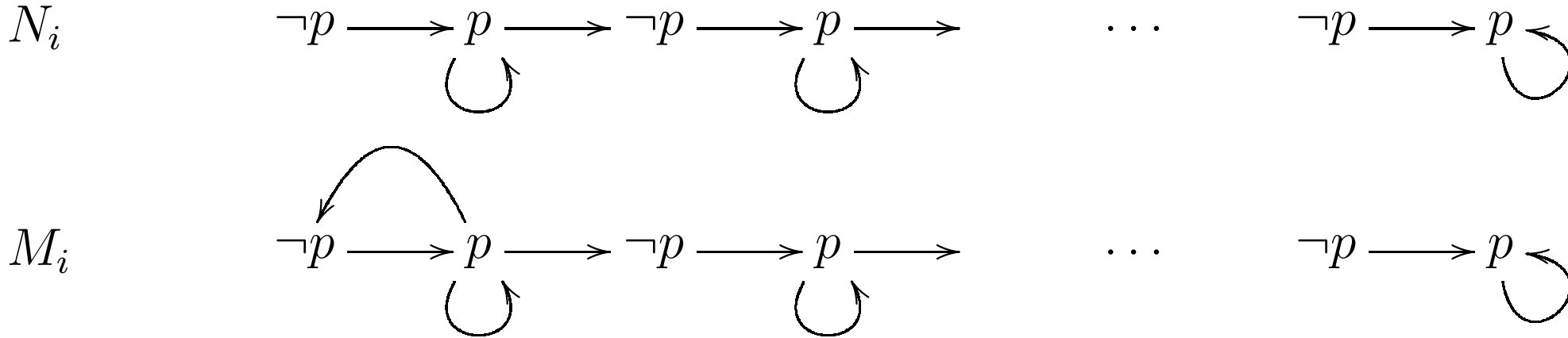
LTL	CTL	uwagi
$F G r \Rightarrow G F g$	—	
$G F r \Rightarrow G F g$	—	
—	AF AX p	∈ ACTL
—	EX AX EX p	
$F G p$	—	
—	AF AG p	∈ ACTL

Tw.: CTL $\ni \phi \xrightarrow{\text{usunięcie kwantyfikatorów ścieżkowych}} \psi \in \text{LTL}$

- albo $\phi \equiv \psi$
- albo nie ma $\psi \in \text{LTL}$ t. że $\phi \equiv \psi$.

LTL	CTL	uwagi
—	AF AG p	 <p>(następny slajd)</p>
F G p	—	

(F G p ≠ AF AG p)

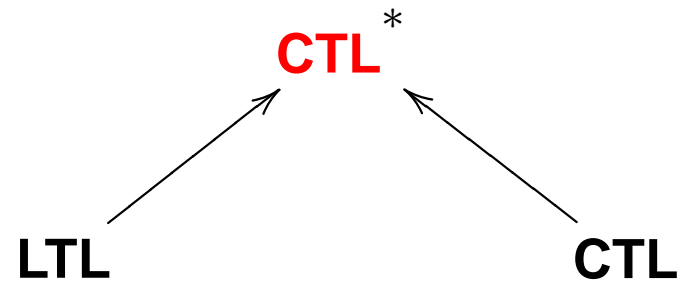


Fakt: $N_i \models F G p$, $M_i \not\models F G p$.

Niech $\phi \in \text{CTL}$.

Lem.: Gdy $i \geq \text{rozmiar}(\phi)$, $N_i \models \phi \iff N_{i+1} \models \phi$.

Lem.: Gdy $i \geq \text{rozmiar}(\phi)$, $N_i \models \phi \iff M_i \models \phi$.



Wniosek: $LTL, CTL \subset CTL^*$

Przykład: $A F G p \vee AG EF p$

$A F G p \in LTL \setminus CTL$

$AG EF p \in CTL \setminus LTL$

Def.: CTL* (Computation Tree Logic*)

formuły stanowe:

$s \models \phi$

$$\phi ::= p \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \mathbf{E} \psi$$

formuły ścieżkowe:

$\Pi \models \psi$

$$\psi ::= \phi \mid \neg\psi \mid \psi_1 \wedge \psi_2 \mid \mathbf{X} \psi \mid \psi_1 \mathbf{U} \psi_2$$

Notacja:

$$\mathbf{A} \psi \equiv \neg \mathbf{E} \neg \psi$$

$$\mathbf{F} \psi \equiv \text{true} \mathbf{U} \psi$$

$$\mathbf{G} \psi \equiv \neg \mathbf{F} \neg \psi$$

$$\psi_1 \mathbf{R} \psi_2 \equiv \neg(\neg\psi_1 \mathbf{U} \neg\psi_2)$$

Def.: CTL* (Computation Tree Logic*)

formuły stanowe:

$s \models \phi$

$$\phi ::= p \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \mathbf{E} \psi$$

formuły ścieżkowe:

$\Pi \models \psi$

$$\psi ::= \phi \mid \neg\psi \mid \psi_1 \wedge \psi_2 \mid \mathbf{X} \psi \mid \psi_1 \mathbf{U} \psi_2$$

Przykład:

$$\mathbf{A}(\mathbf{F} \mathbf{G} p \wedge \mathbf{G} \mathbf{F} q), \quad \mathbf{E} \mathbf{X} \mathbf{A} \mathbf{F} \mathbf{G} p$$

Semantyka: $M = \langle S, S_{\text{pocz}}, \rightarrow, L \rangle$ struktura Kripkego

$s \models \phi$

$s \models p$ wtw gdy $p \in L(s)$

$s \models \mathbf{E} \psi$ wtw gdy $\exists \Pi. \Pi$ zaczyna się w $s \wedge \Pi \models \psi$

$\Pi \models \psi, \quad \Pi = s_0 s_1 \dots$

$\Pi \models \phi$ wtw gdy $s_0 \models \phi$

$\Pi \models \mathbf{X} \psi$ wtw gdy ...

jak w LTL

$\Pi \models \psi_1 \mathbf{U} \phi_2$ wtw gdy ...

jak w LTL

LTL \subset **CTL***

ograniczenie: $A\psi$, ψ „czysto ścieżkowa”, tzn bez E , A

CTL \subset **CTL***

ograniczenie:

kwantyfikatory ścieżkowe i operatory temporalne parami

LTL \subset **CTL***

ograniczenie: $A \psi$, ψ „czysto ścieżkowa”, tzn bez E , A

CTL \subset **CTL***

ograniczenie:

kwantyfikatory ścieżkowe i operatory temporalne parami

ACTL* \subset **CTL***

(**ACTL** \subset **CTL**)

ograniczenie: kwantyfikator ścieżkowy E zabroniony

Ćw.:

Znajdź naturalną własność $\phi \in \text{CTL}^* \setminus (\text{CTL} \cup \text{LTL})$?

Ćw.: Podaj własność $\phi \notin \text{CTL}^*$

Ćw.: Podaj własność $\phi \notin \text{CTL}^*$

$\phi \equiv$ na każdej ścieżce, a zachodzi na pozycjach parzystych

I. osiągalność

$$EF \text{ crit}_1 \wedge \text{crit}_2$$

II. bezpieczeństwo

$$AG \neg \text{overflow}$$
$$A(\neg \text{start} \text{ U } \text{key} \vee G \neg \text{start})$$

III. żywotność

$AG (req \implies AF \text{ granted})$

$AG EF \text{ start}$

$A (\neg \text{start} U \text{key})$

IV. brak blokady

$AF EX \text{true}$

V. sprawiedliwość (uczciwość)

$$\overset{\infty}{F} \phi \equiv G F \phi, \quad \overset{\infty}{G} \phi \equiv F G \phi$$

$$A \overset{\infty}{F} \text{open} \equiv AG AF \text{open}$$

$$A(\overset{\infty}{F} 1 \wedge \overset{\infty}{F} 2 \wedge \dots \wedge \overset{\infty}{F} 6)$$

$$A(\overset{\infty}{F} \text{crit_req} \implies \overset{\infty}{F} \text{crit_enter})$$

$$A(\overset{\infty}{G} \text{crit_req} \implies \overset{\infty}{F} \text{crit_enter})$$

$$A(\overset{\infty}{F} \text{trans_ok} \implies G(\text{send} \implies AF \text{receive}))$$

sprawiedliwa (ang. *fair*) \models dla CTL

Semantyka: $M = \langle S, S_{\text{pocz}}, \rightarrow, L, \mathbf{F} \rangle$ $\mathbf{F} \subseteq \mathcal{P}(S)$

Π jest **sprawiedliwa** jeśli $\forall X \in F. \text{inf}(\Pi) \cap X \neq \emptyset$

$s \models_{\mathbf{F}} p \iff p \in L(s) \wedge \exists \Pi. \Pi$ **sprawiedliwa** i zaczyna się w

$s \models_{\mathbf{F}} \mathbf{A} \phi \iff \forall \Pi. \Pi$ **sprawiedliwa** i zaczyna się w $s \implies \Pi \models \phi$

$s \models_{\mathbf{F}} \mathbf{E} \phi \iff \exists \Pi. \Pi$ **sprawiedliwa** i zaczyna się w s oraz $\Pi \models \phi$

Najczęściej $\mathbf{F} = \{\phi_1, \dots, \phi_n\}$, $\phi_i \in \text{CTL}$

$$|F| = |\phi_1| + \dots + |\phi_n|$$

Morały:

- CTL jest najtańsza (czas $\mathcal{O}(|M| \cdot |\phi|)$)
- LTL jest bardziej ekspresywna (własności ścieżkowe)
- CTL_F jest wystarczająco ekspresywna w praktyce
- LTL nadaje się do weryfikacji w locie
- CTL^* jest zbyt skomplikowana

$\phi \in \dots$	$M \models \phi$	spełnialność ϕ
LTL	PSPACE $ M \cdot 2^{\mathcal{O}(\phi)}$	PSPACE
CTL	P $\mathcal{O}(M \cdot \phi)$	EXPTIME
CTL _F	P $\mathcal{O}(M \cdot (\phi + F))$	EXPTIME
CTL*	PSPACE $ M \cdot 2^{\mathcal{O}(\phi)}$	2-EXPTIME
$L\mu$	NP \cap co-NP $\mathcal{O}(M ^{ \phi })$	EXPTIME

$\phi \in \dots$	$M \models \phi$	spełnialność ϕ
LTL	PSPACE $ M \cdot 2^{\mathcal{O}(\phi)}$	PSPACE
CTL	P $\mathcal{O}(M \cdot \phi)$	EXPTIME

Pytanie: Czy weryfikacja CTL jest tańsza niż CTL?

NIE! LTL może być wykładniczo bardziej zwięzły.

$$\mathbf{F} w_1 \wedge \dots \wedge \mathbf{F} w_k \wedge \mathbf{X}^{k+1} w_0$$

Weryfikacja modelowa dla CTL

CTL (\neg , \wedge , **EX**, **E_U_**, **EG**)

(wystarczy te spójniki)

$M \models \phi$: Algorytm etykietuje stany w M podformułami ϕ
(algorytm **globalny**)

E ϕ U ψ : startujemy od stanów spełniających ψ , wstecz relacji \rightarrow

EX ϕ : tylko jeden krok

EG ϕ : $S' := \{s \in S \mid s \models \phi\} \mapsto M'$

$s \models \mathbf{EG} \phi \iff \begin{cases} s \in S' \wedge \\ \text{w } M' \text{ istnieje ścieżka z } s \text{ do nietrywialnej s.s.s.} \end{cases}$

Sprawiedliwa weryfikacja modelowa dla CTL

$$M \models_{\mathbf{F}} \phi \qquad F = \{\phi_1, \dots, \phi_n\} \mapsto F = \{F_1, \dots, F_n\}$$

$$\mathbf{EG} \phi: \quad S' := \{s \in S \mid s \models \phi\}, \quad F' := \{F_i \cap S'\} \mapsto M'$$

$$s \models_{\mathbf{F}} \mathbf{EG} \phi \iff \begin{cases} s \in S' \wedge \\ \text{w } M' \text{ istnieje ścieżka z } s \text{ do nietrywialnej} \\ \text{sprawiedliwej s.s.s.} \end{cases}$$

$$\text{s.s.s. } C \subseteq S \text{ jest } \mathbf{sprawiedliwa} \iff \forall i. C \cap F_i \neq \emptyset$$

$$p: \quad \text{dodajemy } \mathbf{fair} \text{ do } L(s) \iff s \models_{\mathbf{F}} \mathbf{EG} \text{ true}$$

$$s \models_{\mathbf{F}} p \iff s \models p \wedge \mathbf{fair}$$

Sprawiedliwa weryfikacja modelowa dla CTL

$EX \phi$:

$$s \models_{\mathbf{F}} EX \phi \iff s \models EX (\phi \wedge \mathbf{fair})$$

$E \phi U \psi$:

$$s \models_{\mathbf{F}} E \phi U \psi \iff s \models E \phi U (\psi \wedge \mathbf{fair})$$

Koszt czasowy $\mathcal{O}(|M| \cdot (|\phi| + |F|))$

Kontrprzykłady?