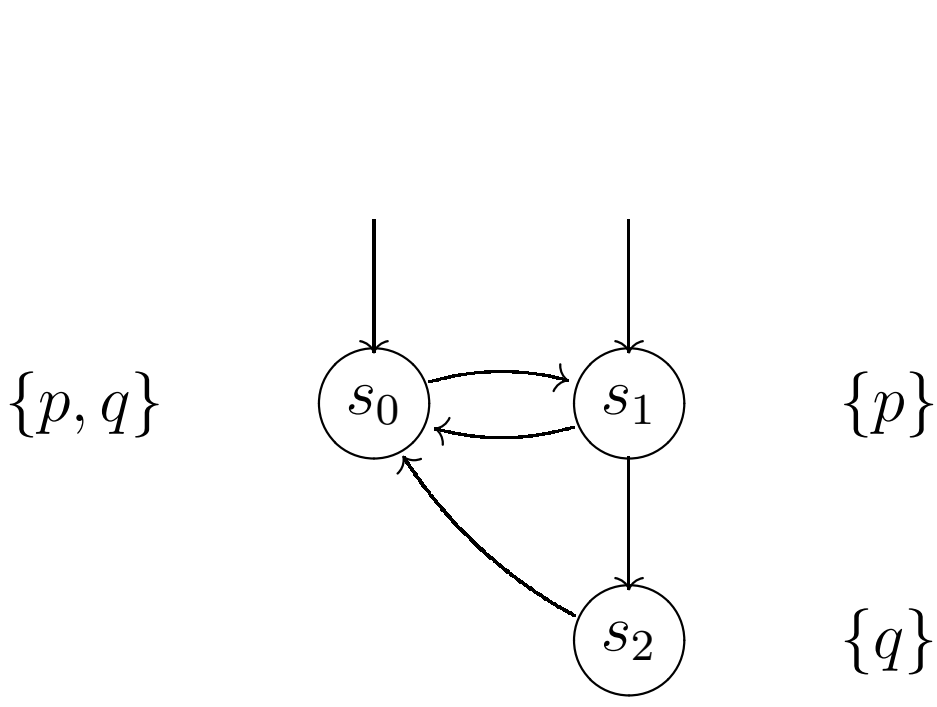
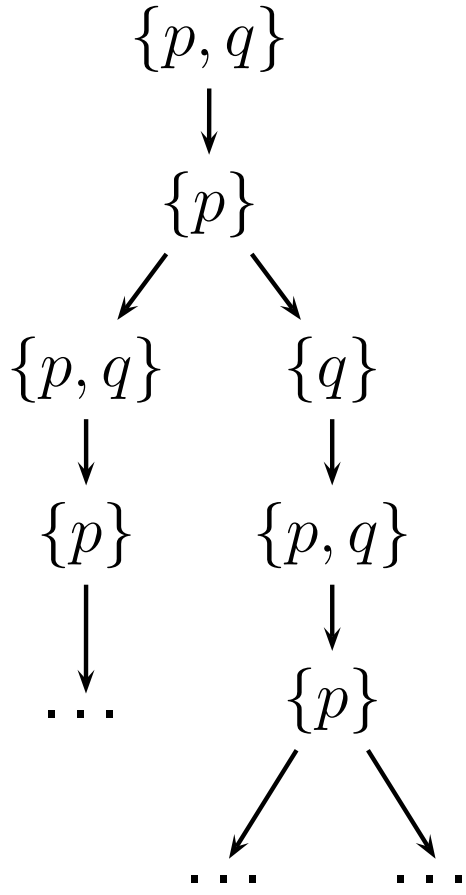
Weryfikacja wspomagana komputerowo

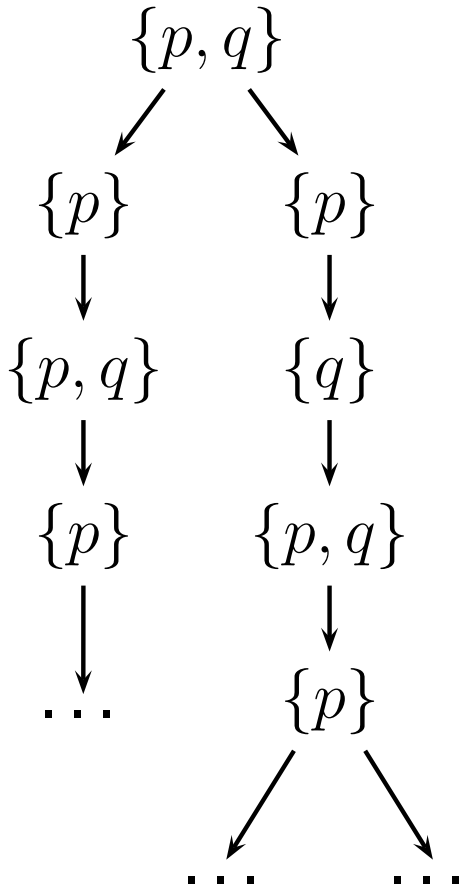
Wykład 5: CTL

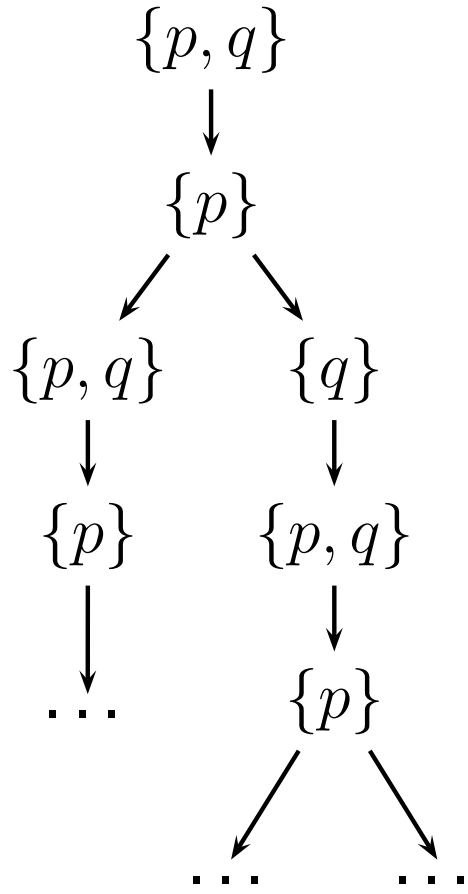
Struktura Kripkego $\mapsto$ drzewo





Czas liniowy





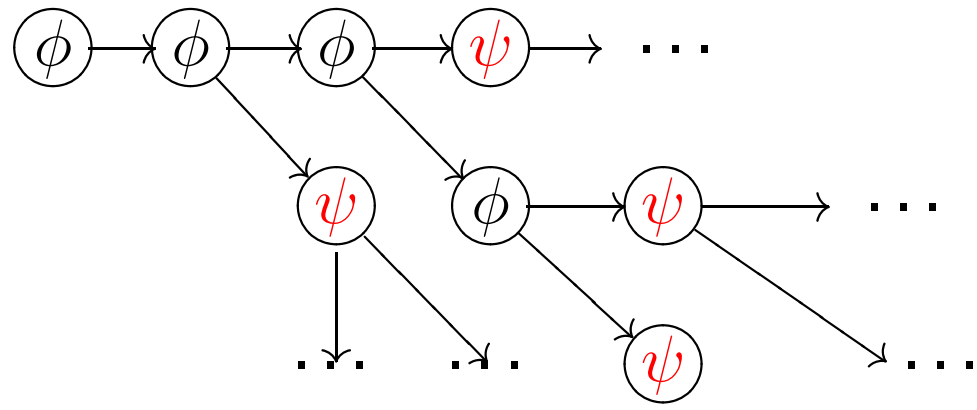
Def.: CTL (Computation Tree Logic)

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

$\mathsf{A}\,\phi\,\mathsf{U}\,\psi \quad \equiv$ na każdej ścieżce zachodzi $\phi\,\mathsf{U}\,\psi$

$\mathsf{E}\,\phi\,\mathsf{U}\,\psi \quad \equiv$ na pewnej ścieżce zachodzi $\phi\,\mathsf{U}\,\psi$

$\mathsf{A}\,\phi\,\mathsf{U}\,\psi$



Notacja:

$$\begin{aligned} \mathsf{AF}\,\phi &\equiv \mathsf{A}\,\mathtt{true}\,\mathsf{U}\,\phi \\ \mathsf{EF}\,\phi &\equiv \mathsf{E}\,\mathtt{true}\,\mathsf{U}\,\phi \\ \mathsf{AG}\,\phi &\equiv \text{?} \\ \mathsf{EG}\,\phi &\equiv \text{?} \end{aligned}$$

Przykład:

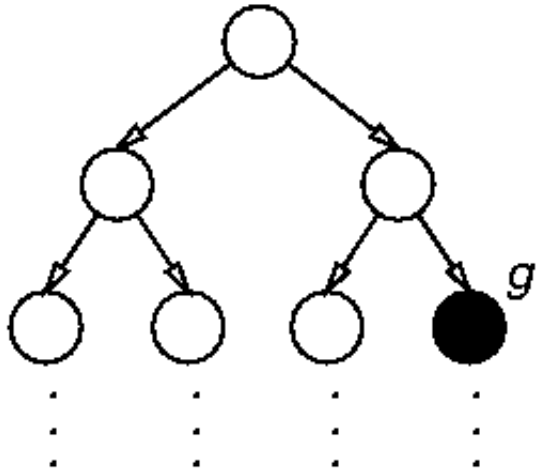
$$\mathsf{AF}\,\mathtt{sek\_kryt}, \qquad \mathsf{AF}\;\mathsf{EF}\,\mathtt{start}$$

Notacja:

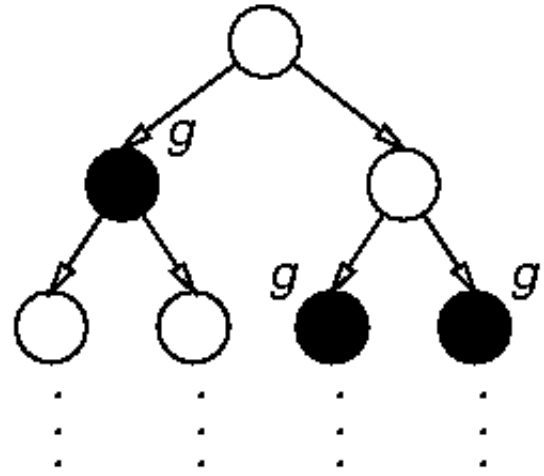
$$\begin{aligned}
\mathsf{AF}\,\phi &\equiv \mathsf{A}\,\mathtt{true}\,\mathsf{U}\,\phi \\
\mathsf{EF}\,\phi &\equiv \mathsf{E}\,\mathtt{true}\,\mathsf{U}\,\phi \\
\mathsf{AG}\,\phi &\equiv \neg\ \mathsf{EF}\,\phi \\
\mathsf{EG}\,\phi &\equiv \neg\ \mathsf{AF}\,\phi
\end{aligned}$$

Przykład:

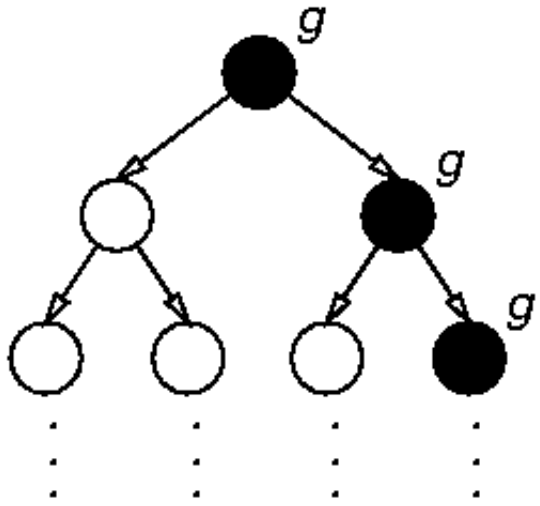
$$\mathsf{AG}\,(q \implies \mathsf{AF}\,r), \qquad \mathsf{AG}\ \mathsf{AF}\,\mathtt{enabled}$$



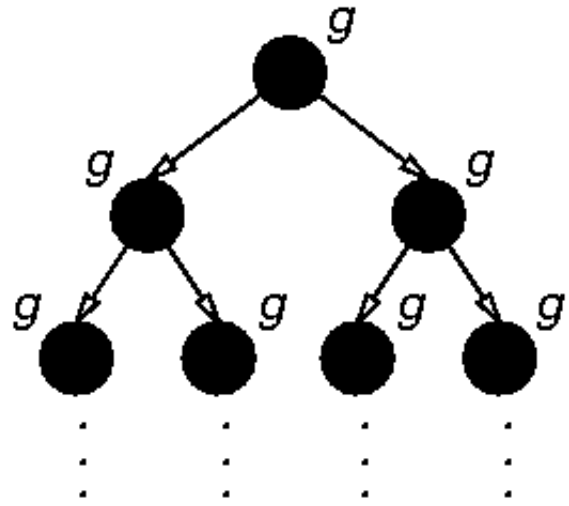
$M, s_0 \models \mathbf{EF}\, g$



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



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



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

[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 $p \in L(s)$

$s \models \mathsf{AX}\,\phi$ wtw gdy $\forall s'.\; s \rightarrow s' \implies s' \models \phi$

$s \models \mathsf{EX}\,\phi$ wtw gdy $\exists s'.\; s \rightarrow s' \wedge s' \models \phi$

$s \models \mathsf{A}\,\phi_1\,\mathsf{U}\,\phi_2$ wtw gdy $\forall \Pi.\; \Pi$ zaczyna się w $s \implies \Pi \models \phi_1\,\mathsf{U}\,\phi_2$

$(\Pi = s_0\; s_1\; \ldots \qquad \exists i.\; s_i \models \phi_2 \wedge \forall j < i.\; s_j \models \phi_1)$

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

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 $p \in L(s)$

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

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

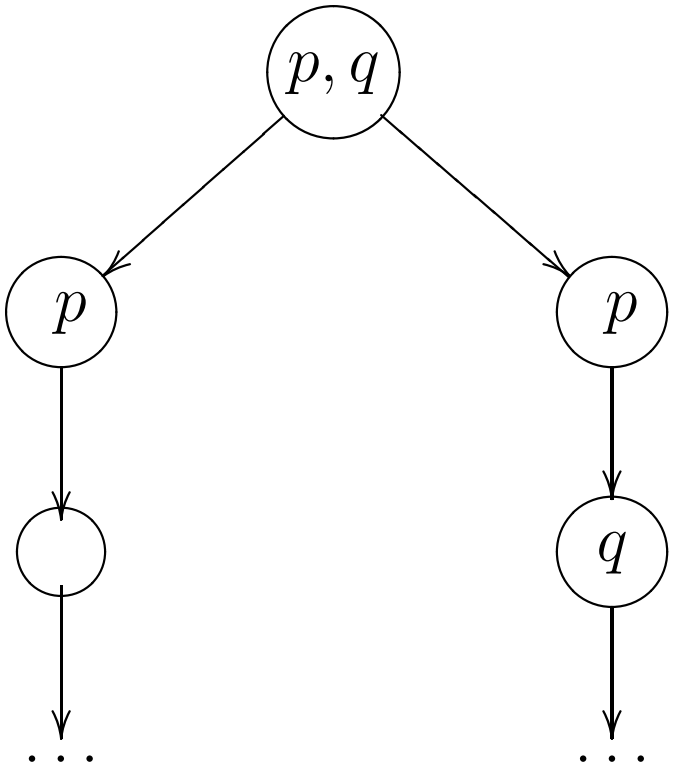
$s \models \mathsf{A}\,\phi_1\,\mathsf{U}\,\phi_2$ wtw gdy $\forall \Pi$. Π zaczyna się w $s \implies \Pi \models \phi_1\,\mathsf{U}\,\phi_2$

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

W LTL czas był **liniowy**.

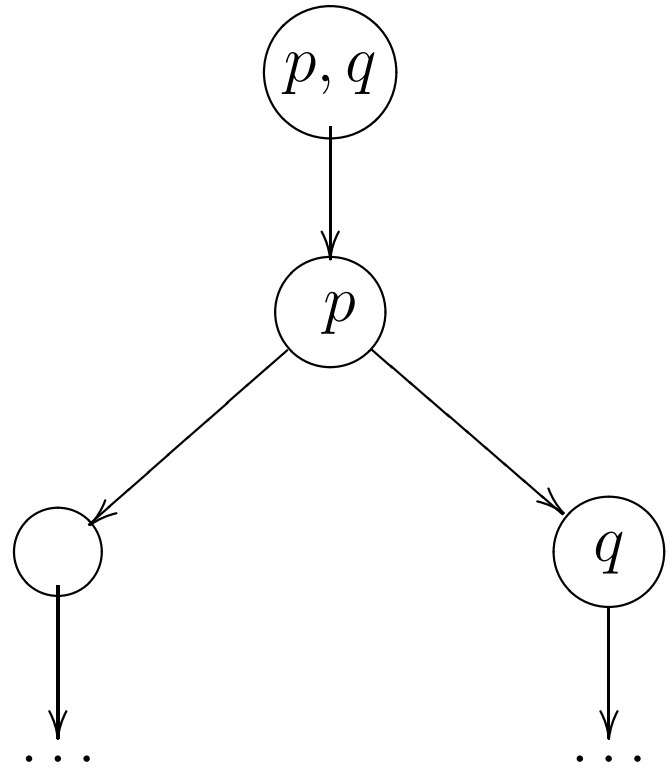
W CTL czas jest **rozgałęziony**!

Czas liniowy vs czas rozgałęziony



$=_{\text{LTL}}$

$\neq_{\text{CTL}}$



Def.: CTL$^+$

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

$\mathsf{A}\,\phi\,\mathsf{R}\,\psi \equiv$ na każdej ścieżce zachodzi $\phi\,\mathsf{R}\,\psi$

$\mathsf{E}\,\phi\,\mathsf{R}\,\psi \equiv$ na pewnej ścieżce zachodzi $\phi\,\mathsf{R}\,\psi$

$\mathsf{A}\,\phi\,\mathsf{R}\,\psi \equiv$ **?**

$\mathsf{E}\,\phi\,\mathsf{R}\,\psi \equiv$ **?**

Def.: CTL$^+$

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

$\mathsf{A}\,\phi\,\mathsf{R}\,\psi \equiv$ na każdej ścieżce zachodzi $\phi\,\mathsf{R}\,\psi$

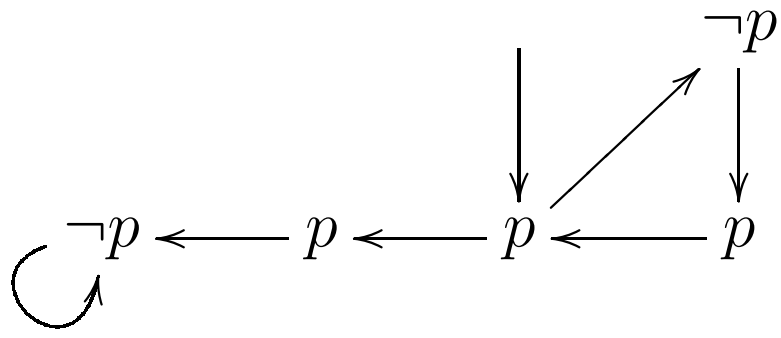
$\mathsf{E}\,\phi\,\mathsf{R}\,\psi \equiv$ na pewnej ścieżce zachodzi $\phi\,\mathsf{R}\,\psi$

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

LTL vs CTL

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

LTL vs CTL

LTL	CTL	uwagi
$\mathsf{F}\,(p \wedge \mathsf{X}\,p)$	—	
—	$\mathsf{AF}\,(p \wedge \mathsf{AX}\,p)$	

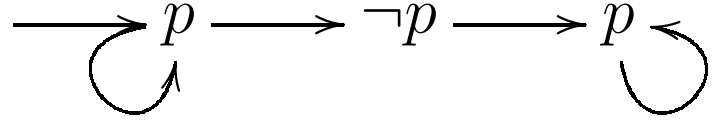
LTL vs CTL

LTL	CTL	uwagi
$\mathsf{FG}\, r \Rightarrow \mathsf{GF}\, g$	—	
$\mathsf{GF}\, r \Rightarrow \mathsf{GF}\, g$	—	
—	$\mathsf{AF}\ \mathsf{AX}\, p$	$\in$ ACTL
—	$\mathsf{EX}\ \mathsf{AX}\ \mathsf{EX}\, p$	
$\mathsf{FG}\, p$	—	
—	$\mathsf{AF}\ \mathsf{AG}\, p$	$\in$ ACTL

AF AG $p \notin$ LTL

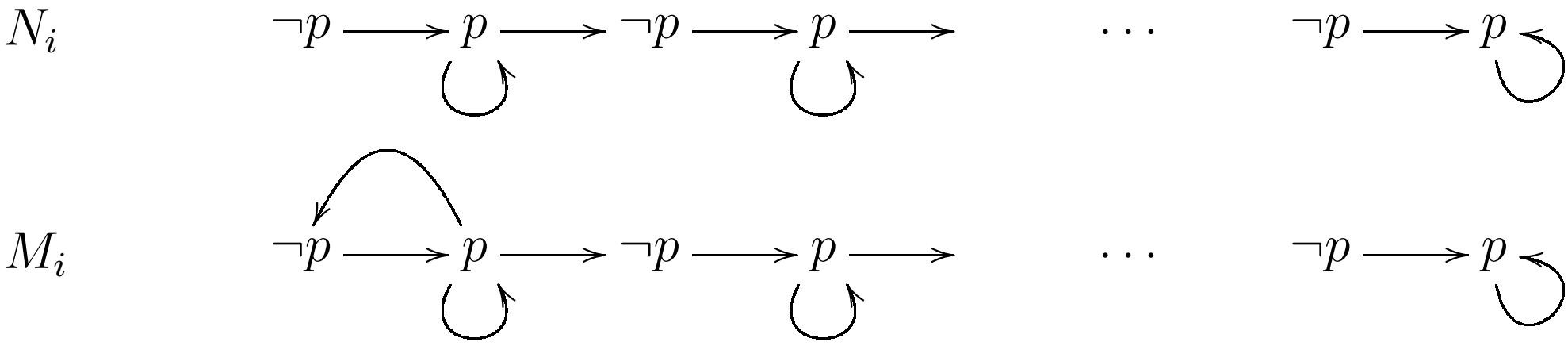
Tw.: $\mathrm{CTL} \ni \phi \xmapsto{\text{usunięcie kwantyfikatorów ścieżkowych}} \psi \in \mathrm{LTL}$

– albo $\phi \equiv \psi$ – albo nie ma $\psi \in$ LTL t. że $\phi \equiv \psi$.

LTL	CTL	uwagi
—	AF AG p	
FG p	—	(następny slajd)

(FG $p \neq$ AF AG p)

FG p $\notin$ CTL

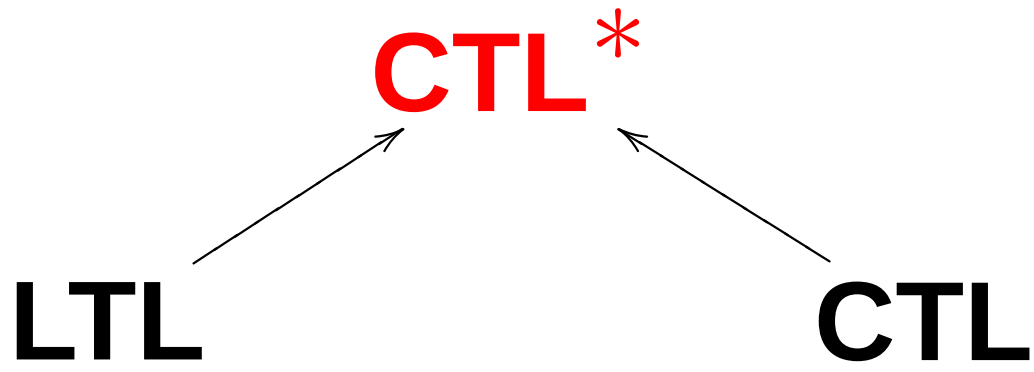


Fakt: $N_i \models$ FG p, $M_i \not\models$ FG p.

Niech $\phi \in$ CTL.

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

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



Przykład: $\mathsf{A\,F\,G}\,p \;\vee\; \mathsf{AG\,EF}\,p$

$\mathsf{A\,F\,G}\,p \in \mathbf{LTL} \setminus \mathbf{CTL}$

$\mathsf{AG\,EF}\,p \in \mathbf{CTL} \setminus \mathbf{LTL}$

Wniosek: $\mathbf{LTL} \cup \mathbf{CTL} \subset \mathbf{CTL}^*$

Def.: CTL* (Computation Tree Logic*)

formuły stanowe: $s \models \phi$

$$\phi \quad ::= \quad p \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \mathsf{E}\,\psi$$

formuły ścieżkowe: $\Pi \models \psi$

$$\psi \quad ::= \quad \phi \mid \neg\psi \mid \psi_1 \wedge \psi_2 \mid \mathsf{X}\,\psi \mid \psi_1\,\mathsf{U}\,\psi_2$$

Notacja:

$$\begin{aligned} \mathsf{A}\,\psi &\equiv \neg\,\mathsf{E}\,\neg\psi \\ \mathsf{F}\,\psi &\equiv \mathtt{true}\,\mathsf{U}\,\psi \\ \mathsf{G}\,\psi &\equiv \neg F \neg\psi \\ \psi_1\,\mathsf{R}\,\psi_2 &\equiv \neg(\neg\psi_1\,\mathsf{U}\,\neg\psi_2) \end{aligned}$$

Def.: CTL* (Computation Tree Logic*)

formuły stanowe: $s \models \phi$

$$\phi \quad ::= \quad p \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \mathsf{E}\,\psi$$

formuły ścieżkowe: $\Pi \models \psi$

$$\psi \quad ::= \quad \phi \mid \neg\psi \mid \psi_1 \wedge \psi_2 \mid \mathsf{X}\,\psi \mid \psi_1\,\mathsf{U}\,\psi_2$$

Przykład:

$$\mathsf{A}\,(\mathsf{FG}\,p \wedge \mathsf{GF}\,q), \qquad \mathsf{E}\;\mathsf{X}\;\mathsf{A}\;\mathsf{FG}\,p$$

Semantyka

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

$s \models \phi$

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

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

$\Pi \models \psi$, $\Pi = s_0\, s_1 \ldots$

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

$\Pi \models \mathsf{X}\,\psi$ wtw gdy $\ldots$ jak w LTL

$\Pi \models \psi_1\, \mathsf{U}\, \phi_2$ wtw gdy $\ldots$ jak w LTL

LTL $\subset$ CTL*

ograniczenie: Aψ, ψ „czysto ścieżkowa”, tzn bez E , A

CTL $\subset$ CTL*

ograniczenie:

kwantyfikatory ścieżkowe i operatory temporalne parami

LTL $\subset$ **CTL***

ograniczenie: Aψ, ψ „czysto ścieżkowa”, tzn bez E, A

CTL $\subset$ **CTL***

ograniczenie:

kwantyfikatory ścieżkowe i operatory temporalne parami

ACTL* $\subset$ **CTL*** $\left(\right.$ **ACTL** $\subset$ **CTL** $\left.\right)$

ograniczenie: kwantyfikator ścieżkowy E zabroniony

Ćw.: Podaj własność $\phi \notin$ CTL*

Ćw.: Podaj własność $\phi \notin$ CTL*

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

Klasyfikacja własności

I. osiągalność

$$\mathsf{EF}\,\mathtt{crit}_1 \wedge \mathtt{crit}_2$$

II. bezpieczeństwo

$$\mathsf{AG}\,\neg\mathtt{overflow}$$

$$\mathsf{A}\,(\neg\mathtt{start}\,\mathsf{U}\,\mathtt{key} \vee\ \mathsf{G}\,\neg\mathtt{start})$$

$$\text{(bezpieczeństwo} \quad \rightsquigarrow \quad \text{osiągalność)}$$

Klasyfikacja własności

III. żywotność

$$\mathsf{AG}\,(\mathtt{req} \implies \mathsf{AF}\,\mathtt{granted})$$

$$\mathsf{AG}\;\mathsf{EF}\,\mathtt{start}$$

$$\mathsf{A}\,(\neg\mathtt{start}\,\mathsf{U}\,\mathtt{key})$$

IV. brak blokady

$$\mathsf{AG}\;\mathsf{EX}\,\mathtt{true}$$

V. sprawiedliwość (uczciwość)

$$\mathsf{A}\,\mathsf{GF}\,\texttt{open} \;\equiv\; \mathsf{AG}\,\mathsf{AF}\,\texttt{open}$$

$$\mathsf{A}\,(\mathsf{GF}\,1 \;\wedge\; \mathsf{GF}\,2 \;\wedge\; \ldots\; \mathsf{GF}\,6)$$

$$\mathsf{A}\,(\mathsf{GF}\,\texttt{crit\_req} \;\Longrightarrow\; \mathsf{GF}\,\texttt{crit\_enter})$$

$$\mathsf{A}\,(\mathsf{FG}\,\texttt{crit\_req} \;\Longrightarrow\; \mathsf{GF}\,\texttt{crit\_enter})$$

$$A(\,\mathsf{GF}\,\texttt{trans\_ok} \;\Longrightarrow\; \mathsf{G}\,(\texttt{send} \;\Longrightarrow\; \mathsf{AF}\,\texttt{receive}))$$

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

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

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

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

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

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

Najczęściej $\mathbf{F} = \{\phi_1, \ldots, \phi_n\}, \quad \phi_i \in$ CTL

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

Przykłady

$$\mathsf{A}(\mathsf{GF}\, a \implies \mathsf{F}\, b)$$

$$\mathsf{A}(\mathsf{GF}\, a_1 \wedge \mathsf{GF}\, a_2 \implies b\, \mathsf{U}\, c)$$

$$\mathsf{A}(\mathsf{GF}\, \phi_1 \wedge \mathsf{GF}\, \phi_2 \wedge \ldots \wedge \mathsf{GF}\, \phi_n \implies \phi\, \mathsf{U}\, \phi')$$

$$\mathsf{E}(\mathsf{GF}\, \phi_1 \wedge \mathsf{GF}\, \phi_2 \wedge \ldots \wedge \mathsf{GF}\, \phi_n \wedge \phi\, \mathsf{U}\, \phi')$$

$$\ldots$$

$$\mathsf{A}(\mathsf{FG}\, a \implies \mathsf{F}\, b)$$

Morały

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

Złożoność

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

Złożoność

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

Pytanie: Czy weryfikacja CTL jest tańsza niż LTL?

NIE! LTL może być wykładniczo bardziej zwięzły.

$$\mathsf{F}\, w_1 \ \wedge \ \ldots \ \wedge \ \mathsf{F}\, w_k \ \wedge \ \mathsf{X}^{k+1} w_0$$

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

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

Sprawiedliwa weryfikacja modelowa dla CTL

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

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

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

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

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

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

Sprawiedliwa weryfikacja modelowa dla CTL

EX ϕ:

$$s \models_{\mathbf{F}} \mathsf{EX}\,\phi \quad \Longleftrightarrow \quad s \models \mathsf{EX}\,(\phi \wedge \mathtt{fair})$$

E ϕ U ψ:

$$s \models_{\mathbf{F}} \mathsf{E}\,\phi\,\mathsf{U}\,\psi \quad \Longleftrightarrow \quad s \models \mathsf{E}\,\phi\,\mathsf{U}\,(\psi \wedge \mathtt{fair})$$

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

Kontrprzykłady?