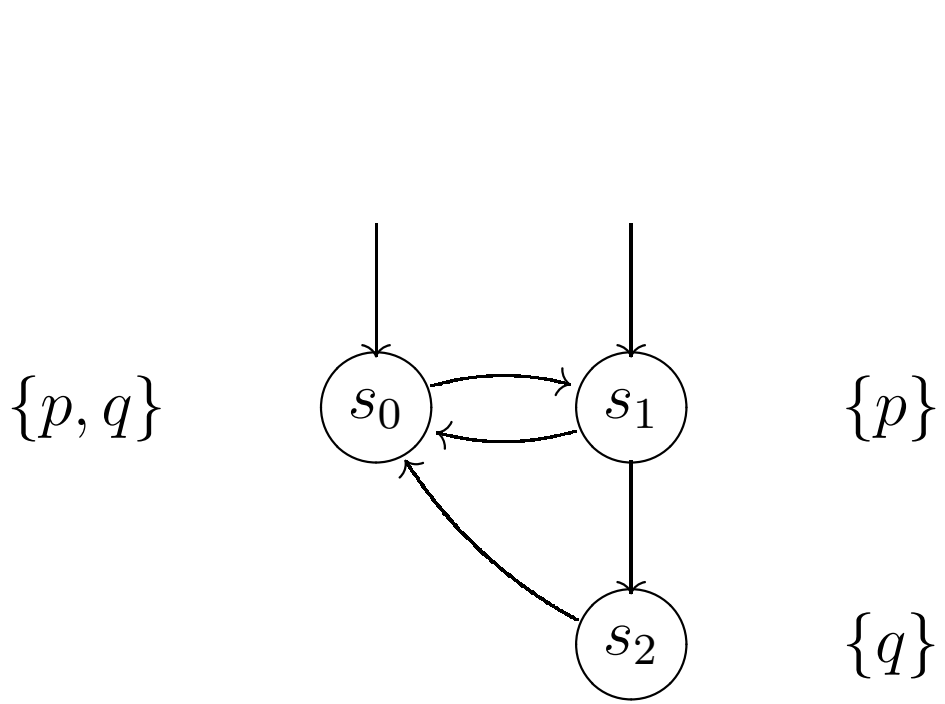
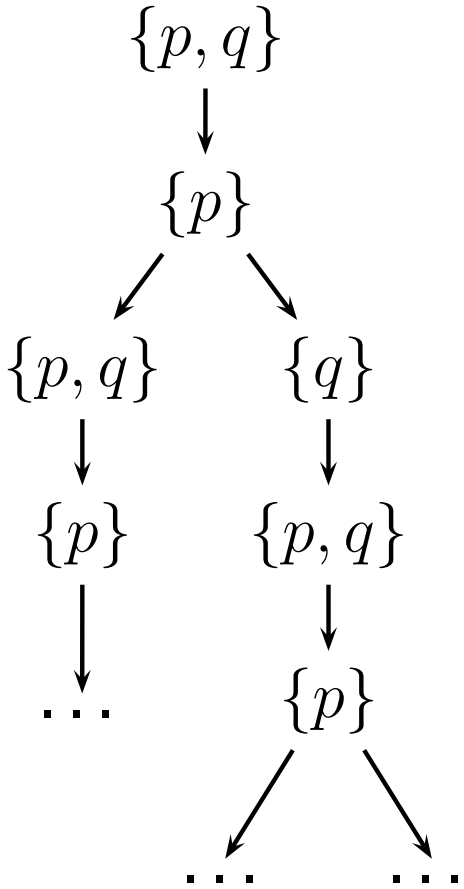
Computer aided verification

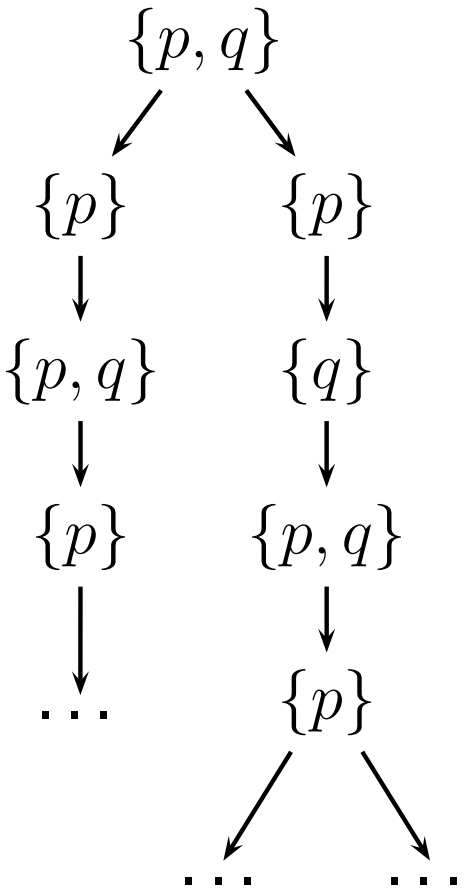
Lecture 5: CTL

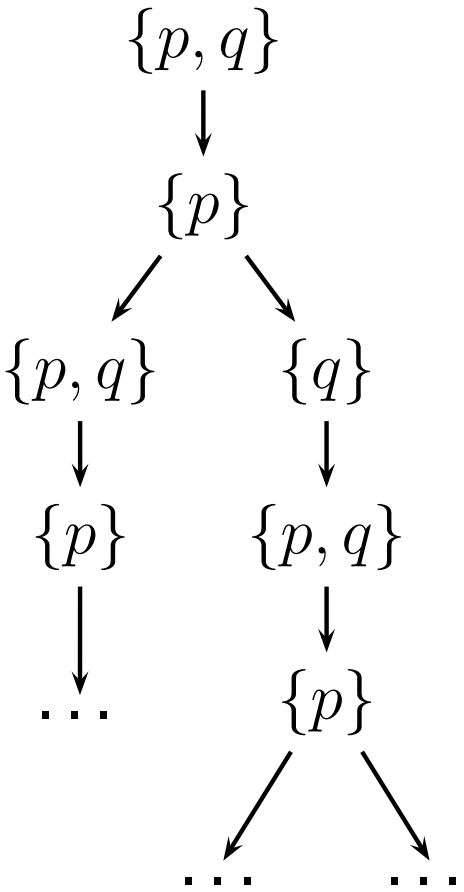
Kripke structure $\mapsto$ tree





Linear time





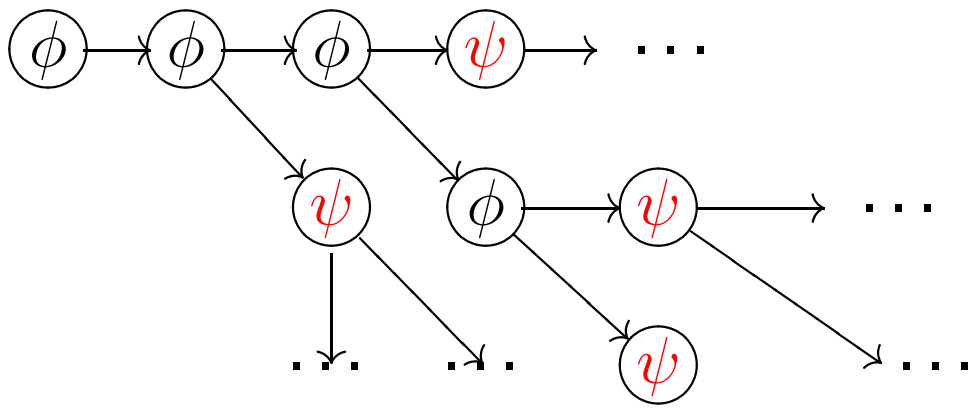
Def.: CTL (Computation Tree Logic)

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

$\mathsf{A}\,\phi\,\mathsf{U}\,\psi \quad \equiv$ on every path it holds $\phi\,\mathsf{U}\,\psi$

$\mathsf{E}\,\phi\,\mathsf{U}\,\psi \quad \equiv$ on some path it holds $\phi\,\mathsf{U}\,\psi$

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



Notation:

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

Example:

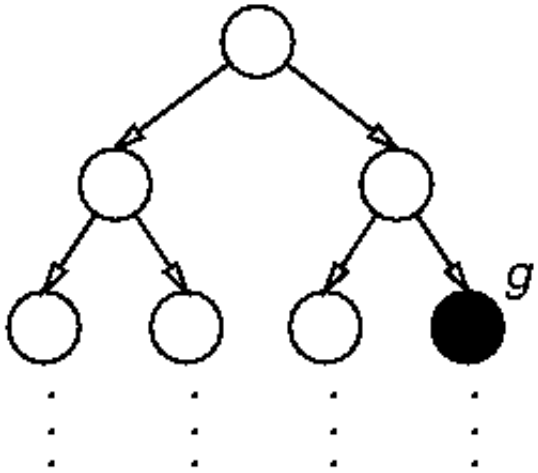
$$\mathsf{AF}\,\mathtt{crit\_sec}, \qquad \mathsf{AF}\;\mathsf{EF}\,\mathtt{start}$$

Notation:

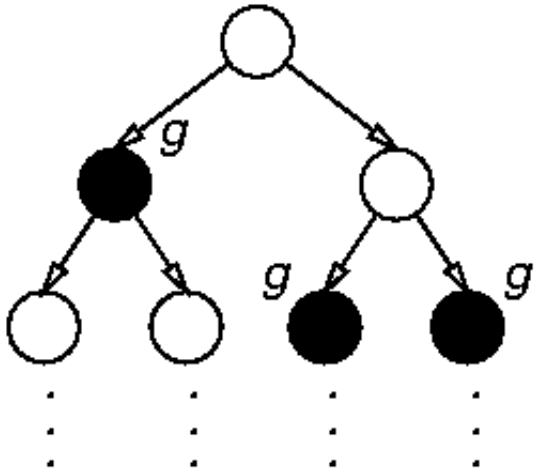
$$\begin{aligned}
\mathsf{AF}\,\phi &\equiv \mathsf{A}\,\mathtt{true}\,\mathsf{U}\,\phi \\
\mathsf{EF}\,\phi &\equiv \mathsf{E}\,\mathtt{true}\,\mathsf{U}\,\phi \\
\mathsf{AG}\,\phi &\equiv \neg\ \mathsf{EF}\,\neg\phi \\
\mathsf{EG}\,\phi &\equiv \neg\ \mathsf{AF}\,\neg\phi
\end{aligned}$$

Example:

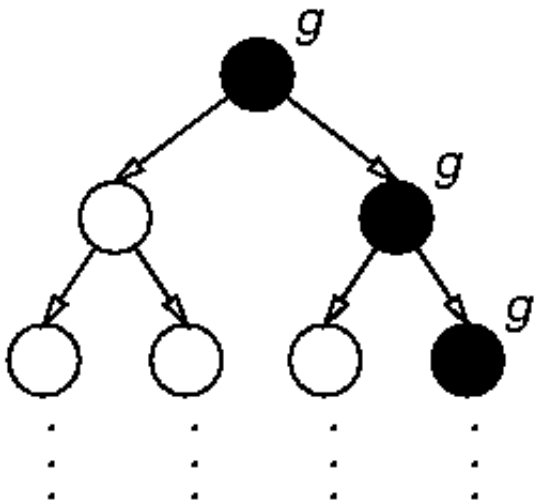
$$\mathsf{AG}\,(q \implies \mathsf{AF}\,r), \qquad \mathsf{AG}\ \mathsf{AF}\,\mathtt{enabled}$$



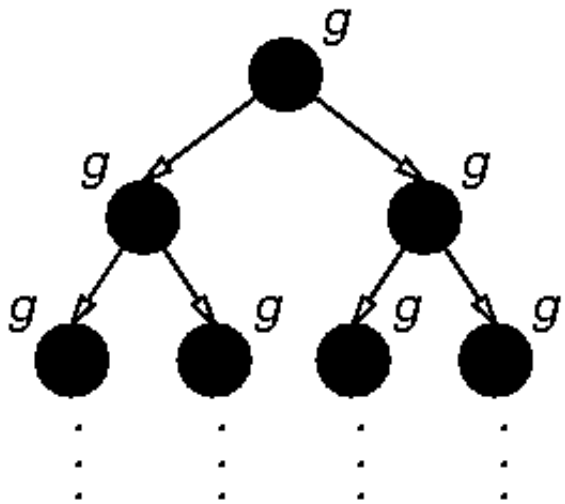
$M, s_0 \models \mathbf{EF}\, g$



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



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



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

[Clarke, Grumberg, Long 1994]

Semantics

$M = \langle S, S_{\text{init}}, \rightarrow, L \rangle$ Kripke structure

$M \models \phi$ iff $\forall s \in S_{\text{init}}\ s \models \phi$

$s \models \neg\phi$ iff $\ldots$

$s \models \phi_1 \wedge \phi_2$ iff $\ldots$

$s \models p$ iff $p \in L(s)$

$s \models \mathsf{AX}\,\phi$ iff $\forall s'.\ s \rightarrow s' \implies s' \models \phi$

$s \models \mathsf{EX}\,\phi$ iff $\exists s'.\ s \rightarrow s' \wedge s' \models \phi$

$s \models \mathsf{A}\,\phi_1\,\mathsf{U}\,\phi_2$ iff $\forall \Pi.\ \Pi$ starts in $s \implies \Pi \models \phi_1\,\mathsf{U}\,\phi_2$
$(\Pi = s_0\ s_1\ \ldots \qquad \exists i.\ s_i \models \phi_2 \wedge \forall j < i.\ s_j \models \phi_1)$

$s \models \mathsf{E}\,\phi_1\,\mathsf{U}\,\phi_2$ iff $\exists \Pi.\ \Pi$ starts in $s \wedge \Pi \models \phi_1\,\mathsf{U}\,\phi_2$

Semantics

$M = \langle S, S_{\text{init}}, \rightarrow, L \rangle$ Kripke structure

$M \models \phi$ iff $\forall s \in S_{\text{init}}\ s \models \phi$

$s \models \neg\phi$ iff ...

$s \models \phi_1 \wedge \phi_2$ iff ...

$s \models p$ iff $p \in L(s)$

$s \models \mathsf{AX}\,\phi$ iff $\forall \Pi.\ \Pi$ starts in $s \implies \Pi \models \mathsf{X}\,\phi$

$s \models \mathsf{EX}\,\phi$ iff $\exists \Pi.\ \Pi$ starts in $s \wedge \Pi \models \mathsf{X}\,\phi$

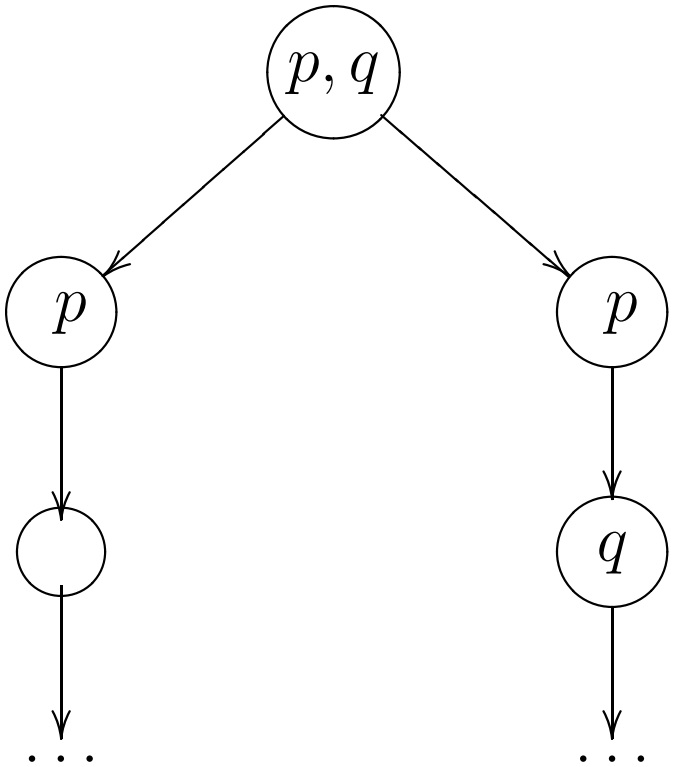
$s \models \mathsf{A}\,\phi_1\,\mathsf{U}\,\phi_2$ iff $\forall \Pi.\ \Pi$ starts in $s \implies \Pi \models \phi_1\,\mathsf{U}\,\phi_2$

$s \models \mathsf{E}\,\phi_1\,\mathsf{U}\,\phi_2$ iff $\exists \Pi.\ \Pi$ starts in $s \wedge \Pi \models \phi_1\,\mathsf{U}\,\phi_2$

LTL is a **linear-time** logic.

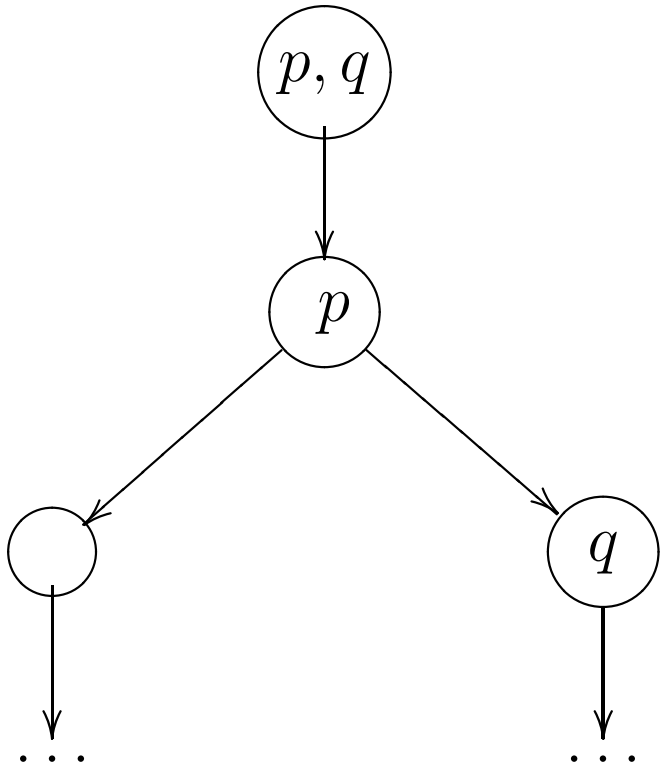
CTL is a **branching-time** logic!

Linear vs branching time



$=_{\text{LTL}}$

$\neq_{\text{CTL}}$



Def.: CTL$^+$

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

$\mathsf{A}\,\phi\,\mathsf{R}\,\psi \equiv$ on every path it holds $\phi\,\mathsf{R}\,\psi$

$\mathsf{E}\,\phi\,\mathsf{R}\,\psi \equiv$ on some path it holds $\phi\,\mathsf{R}\,\psi$

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

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

Def.: CTL$^+$

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

$\mathsf{A}\,\phi\,\mathsf{R}\,\psi \equiv$ on every path it hodls $\phi\,\mathsf{R}\,\psi$

$\mathsf{E}\,\phi\,\mathsf{R}\,\psi \equiv$ on some path it holds $\phi\,\mathsf{R}\,\psi$

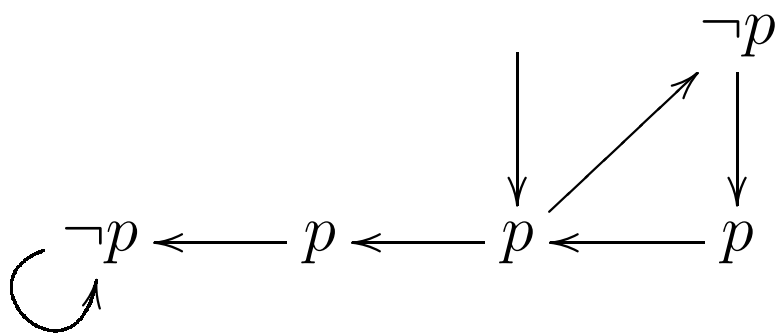
$\mathsf{A}\,\phi\,\mathsf{R}\,\psi \equiv \neg\,\mathsf{E}\,\neg\phi\,\mathsf{U}\,\neg\psi$

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

LTL vs CTL

LTL	CTL	comments
$\mathsf{G}\,p, \quad \mathsf{F}\,p$	$\mathsf{AG}\,p, \quad \mathsf{AF}\,p$	$\in$ 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	comments
$\mathsf{F}\,(p \wedge \mathsf{X}\,p)$	—	
—	$\mathsf{AF}\,(p \wedge \mathsf{AX}\,p)$	

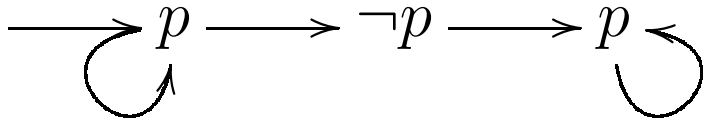
LTL vs CTL

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

AF AG $p \notin$ LTL

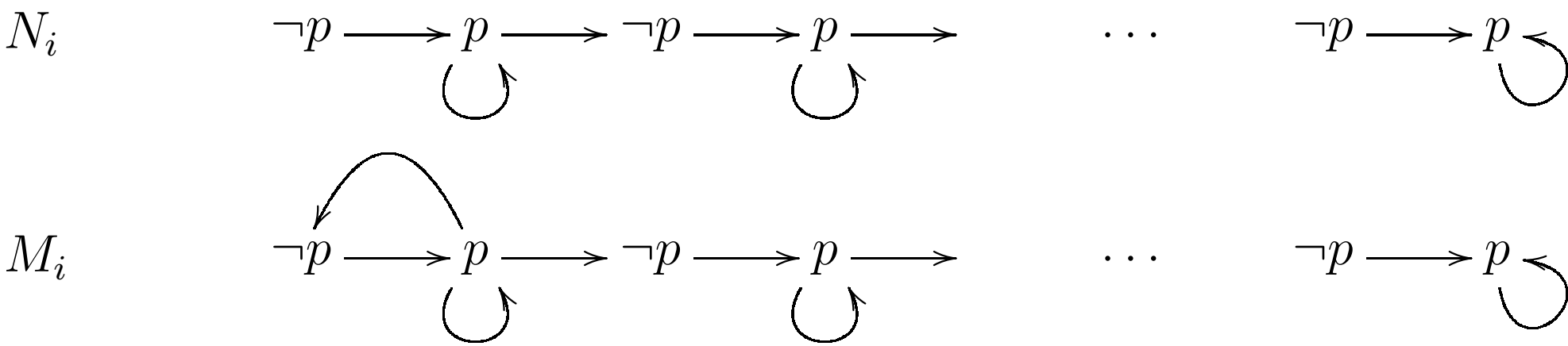
Tw.: $\mathrm{CTL} \ni \phi \longmapsto \psi \in \mathrm{LTL}$ (removing path quantifiers)

– either $\phi \equiv \psi$ – or no $\psi \in$ LTL such that $\phi \equiv \psi$.

LTL	CTL	comments
—	AF AG p	
FG p	—	(next slide)

(FG $p \neq$ AF AG p)

FG p $\notin$ CTL

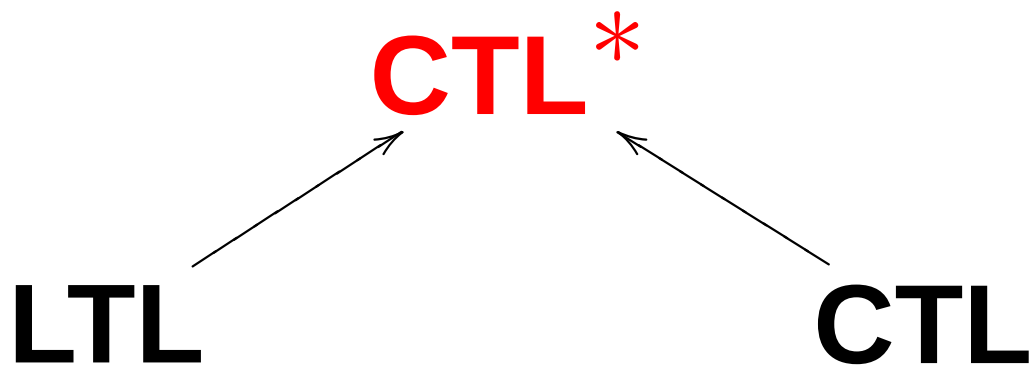


Fact: $N_i \models$ FG p, $M_i \not\models$ FG p.

Let $\phi \in$ CTL.

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

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



Example: A F G p $\vee$ AG EF p

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

AG EF p $\in$ **CTL** $\setminus$ **LTL**

Corollary: **LTL** $\cup$ **CTL** $\subset$ **CTL***

Def.: CTL* (Computation Tree Logic*)

state formulae: $s \models \phi$

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

path formulae: $\Pi \models \psi$

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

Notation:

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

Def.: CTL* (Computation Tree Logic*)

state formulae: $s \models \phi$

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

path formulae: $\Pi \models \psi$

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

Example:

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

Semantics

$M = \langle S, S_{\text{pocz}}, \rightarrow, L \rangle$ Kripke structure

$s \models \phi$

$s \models p$ iff $p \in L(s)$

$s \models \mathsf{E}\,\psi$ iff $\exists \Pi.\ \Pi$ starts in $s \wedge \Pi \models \psi$

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

$\Pi \models \phi$ iff $s_0 \models \phi$

$\Pi \models \mathsf{X}\,\psi$ iff $\ldots$ as in LTL

$\Pi \models \psi_1\, \mathsf{U}\, \phi_2$ iff $\ldots$ as in LTL

LTL $\subset$ CTL*

restriction: $\mathsf{A}\,\psi$, where ψ „purely path formula” (without E, A)

CTL $\subset$ CTL*

restriction:

occurences of path quantifiers and temporal operators paired

LTL $\subset$ **CTL***

restriction: $\mathsf{A}\,\psi$, where ψ „purely path formula” (without E, A)

CTL $\subset$ **CTL***

restriction:

occurences of path quantifiers and temporal operators paired

ACTL* $\subset$ **CTL*** $\quad\left(\textbf{ACTL} \subset \textbf{CTL}\right)$

restriction: path quantifier E forbidden

Exercise: Find a property $\phi \notin \text{CTL}^*$

Exercise: Find a property $\phi \notin$ CTL*

$\phi \equiv$ on every path, a appears on even positions

Classification of properties

I. reachability

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

II. safety

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

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

$$(\text{safety} \quad \rightsquigarrow \quad \text{reachability})$$

Classification of properties

III. liveness

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

$$\mathsf{AG}\,\mathsf{EF}\,\texttt{start}$$

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

IV. deadlock freeness

$$\mathsf{AG}\,\mathsf{EX}\,\texttt{true}$$

Classification of properties

V. fairness

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

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

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

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

$$\mathsf{A}\,(\mathsf{FG}\,\texttt{enabled} \Longrightarrow \mathsf{GF}\,\texttt{executed})$$

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

Fair CTL

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

Π is fair if $\forall X \in F.\ \inf(\Pi) \cap X \neq \emptyset$

$s \models_{\mathbf{F}} p \iff p \in L(s) \wedge \exists \Pi.\ \Pi$ fair and starts in s

$s \models_{\mathbf{F}} \mathsf{A}\,\phi \iff \forall \Pi.\ \Pi$ fair and starts in $s \implies \Pi \models \phi$

$s \models_{\mathbf{F}} \mathsf{E}\,\phi \iff \exists \Pi.\ \Pi$ fair and starts in s and $\Pi \models \phi$

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

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

Examples

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

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

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

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

$$\ldots$$

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

CTL model-checking

CTL $(\neg,\ \wedge,\ \mathbf{EX},\ \mathbf{E\_U\_},\ \mathbf{EG})$ (these connectives are sufficient)

$M \models \phi$: Algorithm labels states of M by subformulae of ϕ
(global algorithm)

$\mathsf{E}\,\phi\,\mathsf{U}\,\psi$: start in states satisfying ψ, propagate backwards $\longrightarrow$

$\mathsf{EX}\,\phi$: one step

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

$$s \models \mathsf{EG}\,\phi \iff \begin{cases} s \in S' \wedge \\ \text{there is a } s\text{-path in } M' \text{ going to a non-trivial scc} \end{cases}$$

Fair CTL model-checking

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

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

$$s \models_{\mathbf{F}} \text{EG}\,\phi \iff \begin{cases} s \in S' \wedge \\ \text{there is a } s\text{-path in } M' \text{ going to a non-trivial} \\ \text{fair scc} \end{cases}$$

scc $C \subseteq S$ is fair $\iff \forall i.\ C \cap F_i \neq \emptyset$

p: $\quad$ add `fair` to $L(s)$ $\iff$ $s \models_{\mathbf{F}} \text{EG}\,\texttt{true}$

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

Fair CTL model-checking

EX ϕ:

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

E ϕ U ψ:

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

Running time $\mathcal{O}(|M| \cdot (|\phi| + |F|))$

Conclusions

- CTL is less expensive ($\mathcal{O}(|M| \cdot |\phi|)$ time)
- LTL is more expressive (path properties)
- CTL_F is sufficiently expressive for practical applications
- CTL^* is too complex

Complexity

$\phi \in \ldots$	$M \models \phi$		satisfability 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

Complexity

$\phi \in \ldots$	$M \models \phi$		satisfability 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

Question: Is CTL model-checking less expensive than LTL one?

Not necessarily!