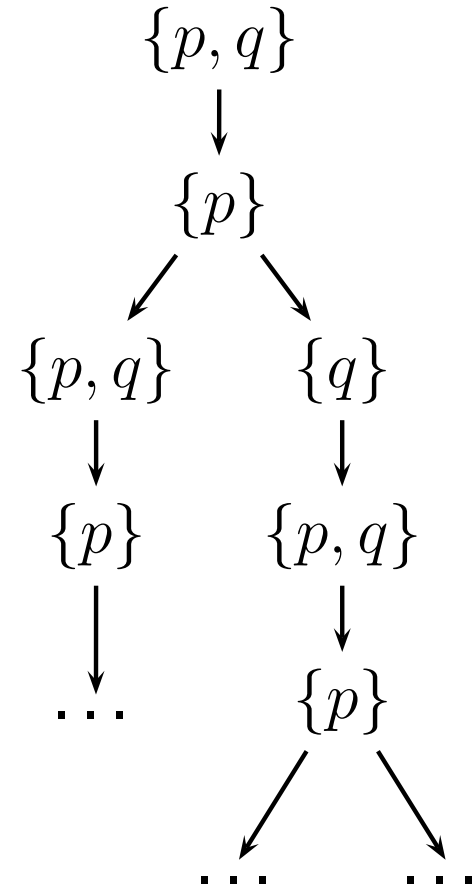
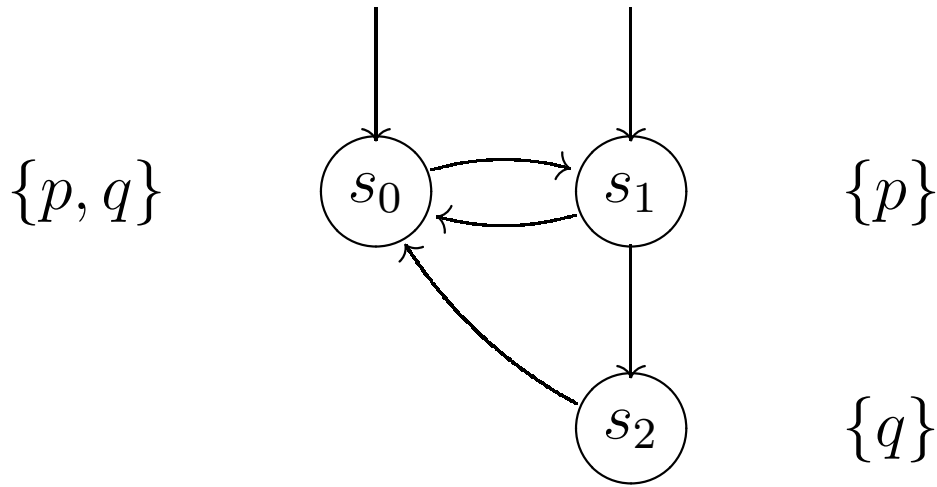


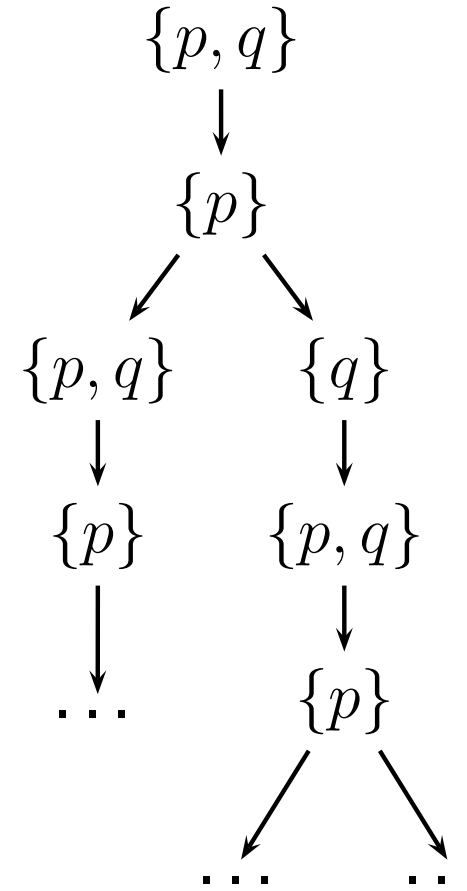
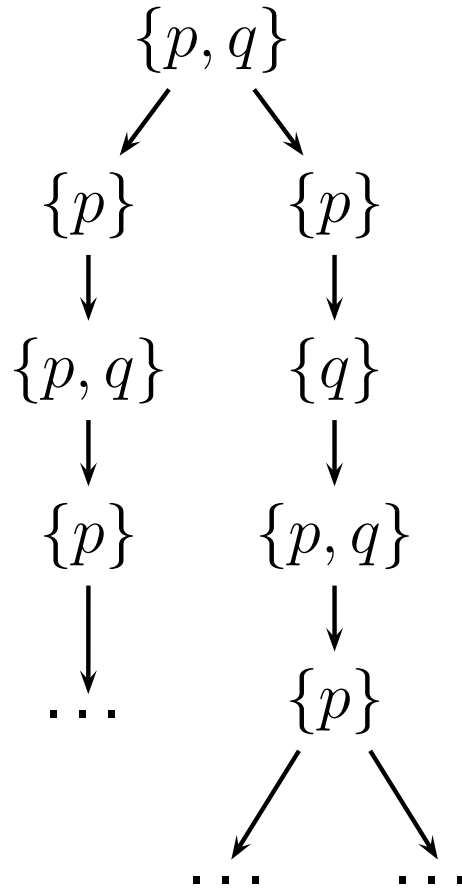
Computer aided verification

Lecture 5: CTL

Kripke structure \mapsto tree



Linear time



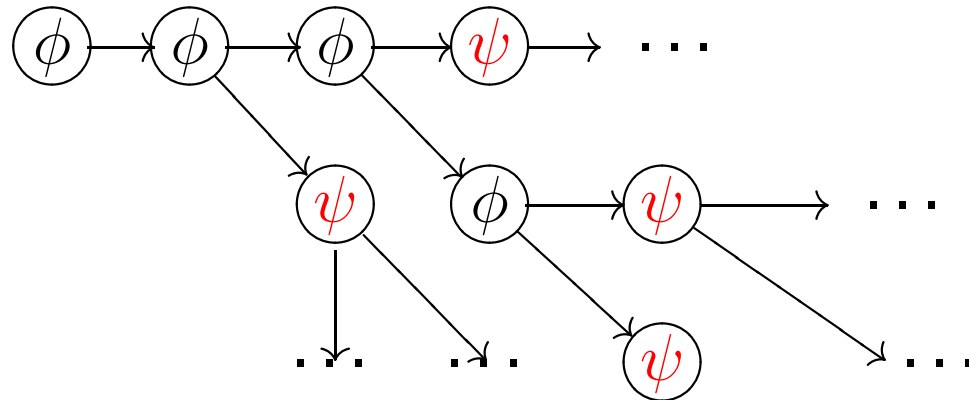
Def.: CTL (Computation Tree Logic)

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

$\mathbf{A} \phi \mathbf{U} \psi \equiv$ on **every** path it holds $\phi \mathbf{U} \psi$

$\mathbf{E} \phi \mathbf{U} \psi \equiv$ on **some** path it holds $\phi \mathbf{U} \psi$

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



Notation: $AF \phi \equiv A \text{ true } U \phi$ $EF \phi \equiv E \text{ true } U \phi$ $AG \phi \equiv ?$ $EG \phi \equiv ?$ **Example:** $AF \text{ crit_sec}, \quad AF \ EF \ \text{start}$

Notation:

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

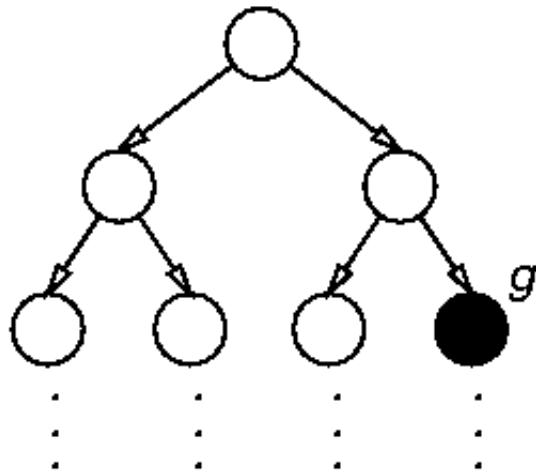
$$EF \phi \equiv E \text{ true } U \phi$$

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

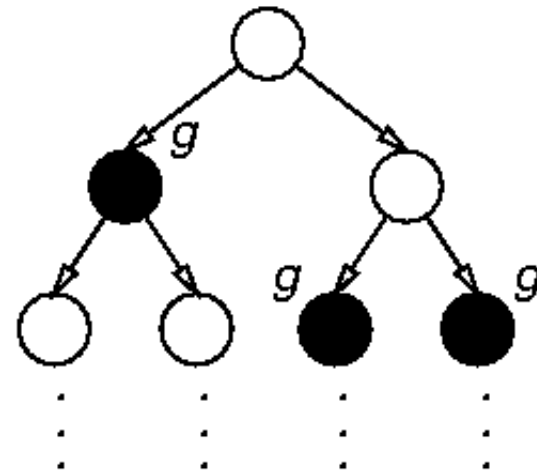
$$EG \phi \equiv \neg AF \neg \phi$$

Example:

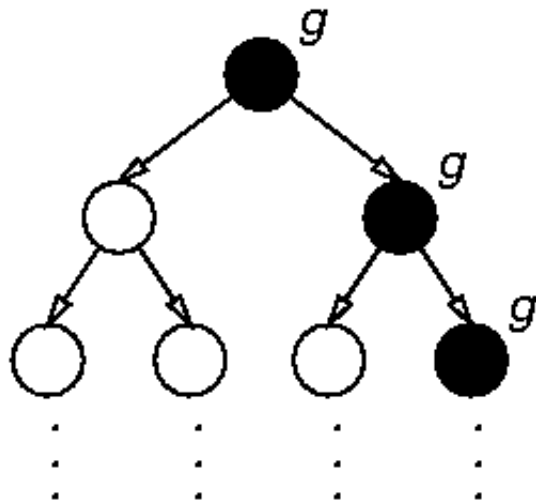
$$AG (q \implies AF r), \quad AG AF \text{ enabled}$$



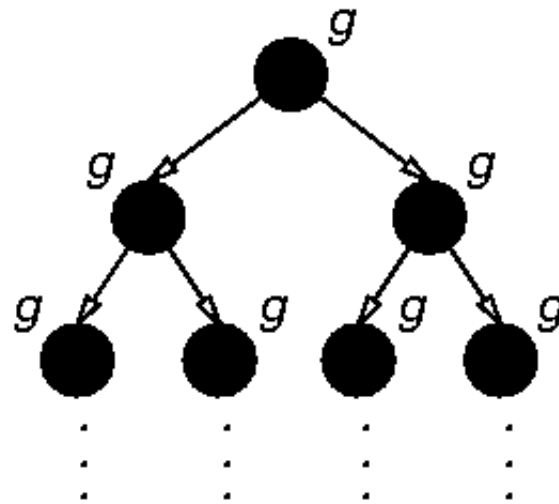
$M, s_0 \models \text{EF } g$



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



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



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

[Clarke, Grumberg, Long 1994]

$M = \langle S, S_{\text{init}}, \rightarrow, L \rangle$ 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 $p \in L(s)$

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

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

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

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

$M = \langle S, S_{\text{init}}, \rightarrow, L \rangle$ 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 $p \in L(s)$

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

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

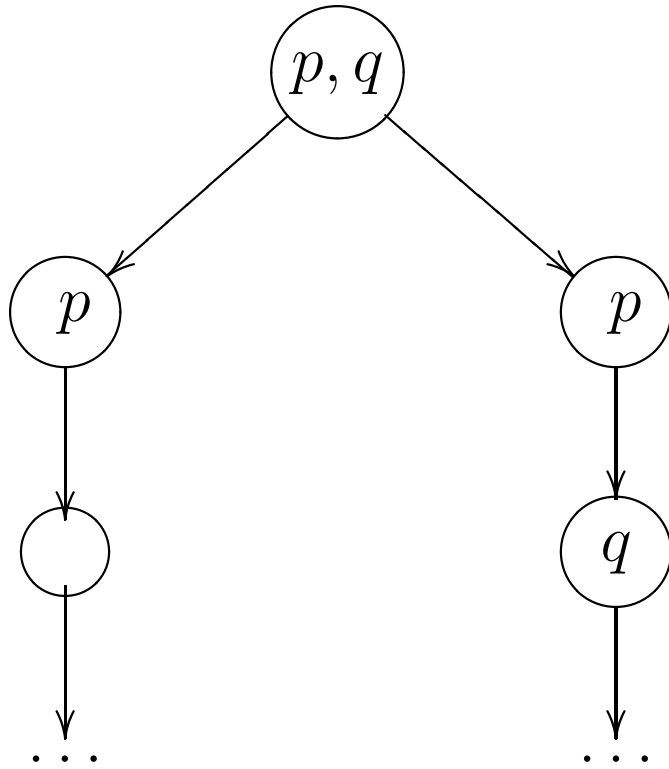
$s \models \mathbf{A} \phi_1 \mathbf{U} \phi_2$ iff $\forall \Pi. \Pi$ starts in $s \implies \Pi \models \phi_1 \mathbf{U} \phi_2$

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

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

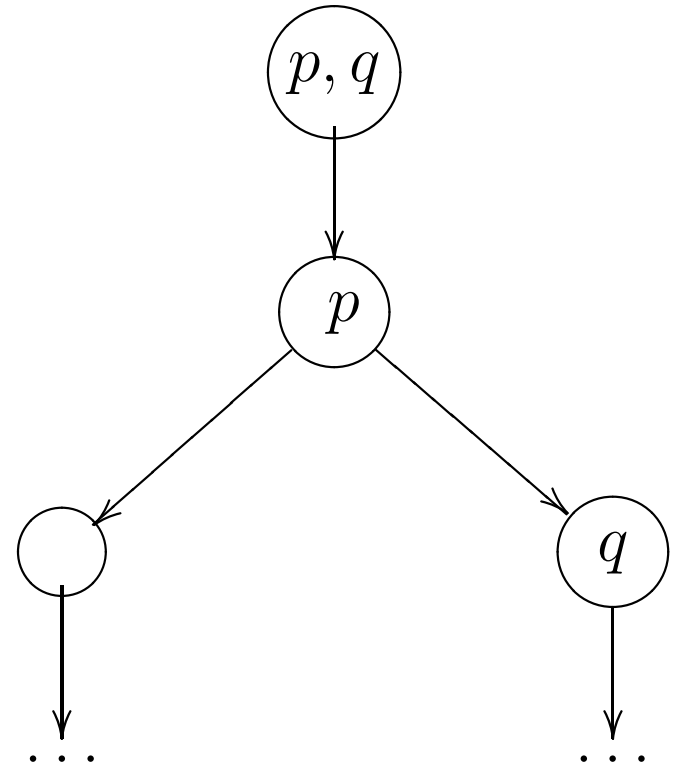
CTL is a **branching-time** logic!

Linear vs branching time



$=_{\text{LTL}}$

\neq_{CTL}



Def.: CTL⁺

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

$\mathbf{A} \phi \mathbf{R} \psi \equiv$ on **every** path it holds $\phi \mathbf{R} \psi$

$\mathbf{E} \phi \mathbf{R} \psi \equiv$ on **some** path it holds $\phi \mathbf{R} \psi$

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

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

Def.: CTL⁺

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

$\mathbf{A} \phi \mathbf{R} \psi \equiv$ on **every** path it holds $\phi \mathbf{R} \psi$

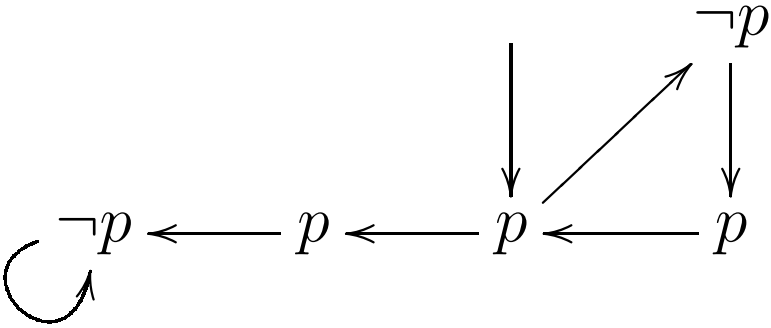
$\mathbf{E} \phi \mathbf{R} \psi \equiv$ on **some** path it holds $\phi \mathbf{R} \psi$

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

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

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

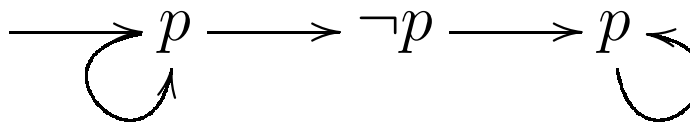
LTL vs CTL

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

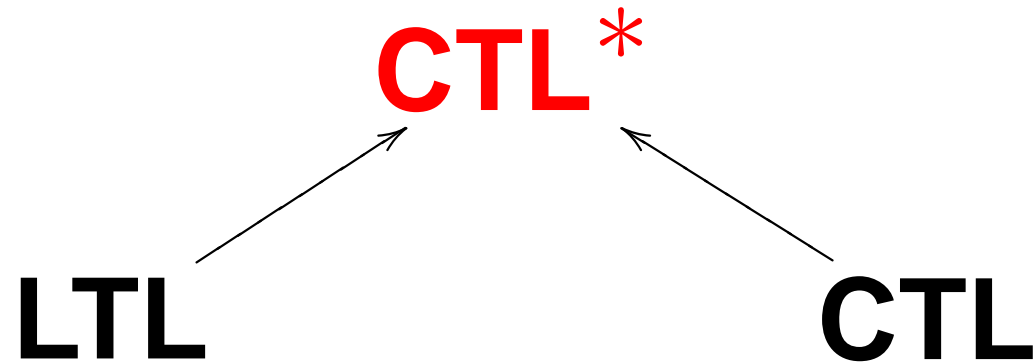
LTL	CTL	comments
$FG\ r \Rightarrow GF\ g$	—	
$GF\ r \Rightarrow GF\ g$	—	
—	AF AX p	∈ ACTL
—	EX AX EX p	
$FG\ p$	—	
—	AF AG p	∈ ACTL

Tw.: CTL $\ni \phi \xrightarrow{\text{removing path quantifiers}} \psi \in$ LTL

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

LTL	CTL	comments
-	AF AG p	 <p>(next slide)</p>
FG p	-	

(FG $p \neq$ AF AG p)



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:

$s \models \phi$

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

path formulae:

$\Pi \models \psi$

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

Notation:

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

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

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

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

Def.: CTL* (Computation Tree Logic*)

state formulae:

$$s \models \phi$$

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

path formulae:

$$\Pi \models \psi$$

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

Example:

$$\mathbf{A} (\mathbf{FG} p \wedge \mathbf{GF} q), \quad \mathbf{E} \mathbf{X} \mathbf{A} \mathbf{FG} p$$

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

$s \models \phi$

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

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

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

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

$\Pi \models \mathbf{X} \psi$ iff ...

as in LTL

$\Pi \models \psi_1 \mathbf{U} \phi_2$ iff ...

as in LTL

LTL \subset **CTL***

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

CTL \subset **CTL***

restriction:

occurrences of path quantifiers and temporal operators paired

LTL \subset **CTL***

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

CTL \subset **CTL***

restriction:

occurrences of path quantifiers and temporal operators paired

ACTL* \subset **CTL***

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

restriction: path quantifier E forbidden

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

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

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

Classification of properties

I. reachability

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

II. safety

$$AG \neg \text{overflow}$$

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

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

Classification of properties

III. liveness

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

$AG EF \text{ start}$

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

IV. deadlock freeness

$AG EX \text{true}$

V. fairness

$$A \text{ GF open} \equiv AG \text{ AF open}$$

$$A(\text{GF } 1 \wedge \text{GF } 2 \wedge \dots \wedge \text{GF } 6)$$

$$A(\text{GF crit_req} \implies \text{GF crit_enter})$$

$$A(\text{FG crit_req} \implies \text{GF crit_enter})$$

$$A(\text{FG enabled} \implies \text{GF executed})$$

$$A(\text{GF trans_ok} \implies G(\text{send} \implies F \text{receive}))$$

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

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

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

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

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

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

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

$$A (GF a \implies F b)$$

$$A (GF a_1 \wedge GF a_2 \implies b U c)$$

$$A (GF \phi_1 \wedge GF \phi_2 \wedge \dots \wedge GF \phi_n \implies \phi U \phi')$$

$$E (GF \phi_1 \wedge GF \phi_2 \wedge \dots \wedge GF \phi_n \wedge \phi U \phi')$$

...

$$A (FG a \implies F b)$$

- 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

$\phi \in \dots$	$M \models \phi$	satisfiability 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

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

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

Not necessarily! LTL may be exponentially more succinct.

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

CTL (\neg , \wedge , **EX**, **E_U_**, **EG**) (these connectives are sufficient)

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

E ϕ U ψ : start in states satisfying ψ , propagate backwards \rightarrow

EX ϕ : one step

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

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

Fair CTL model-checking

$M \models_{\mathbf{F}} \phi$

$F = \{\phi_1, \dots, \phi_n\} \mapsto F = \{F_1, \dots, F_n\}$

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

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

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

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

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

$EX \phi$:

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

$E \phi U \psi$:

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

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

Counterexamples?