Computer aided verification

Lecture 5:

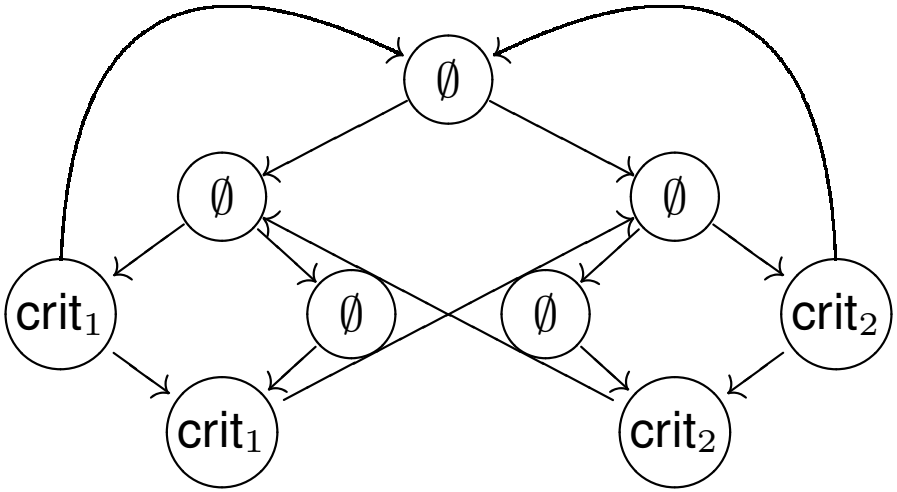
Expressing properties of systems in Computation Tree Logic (CTL)

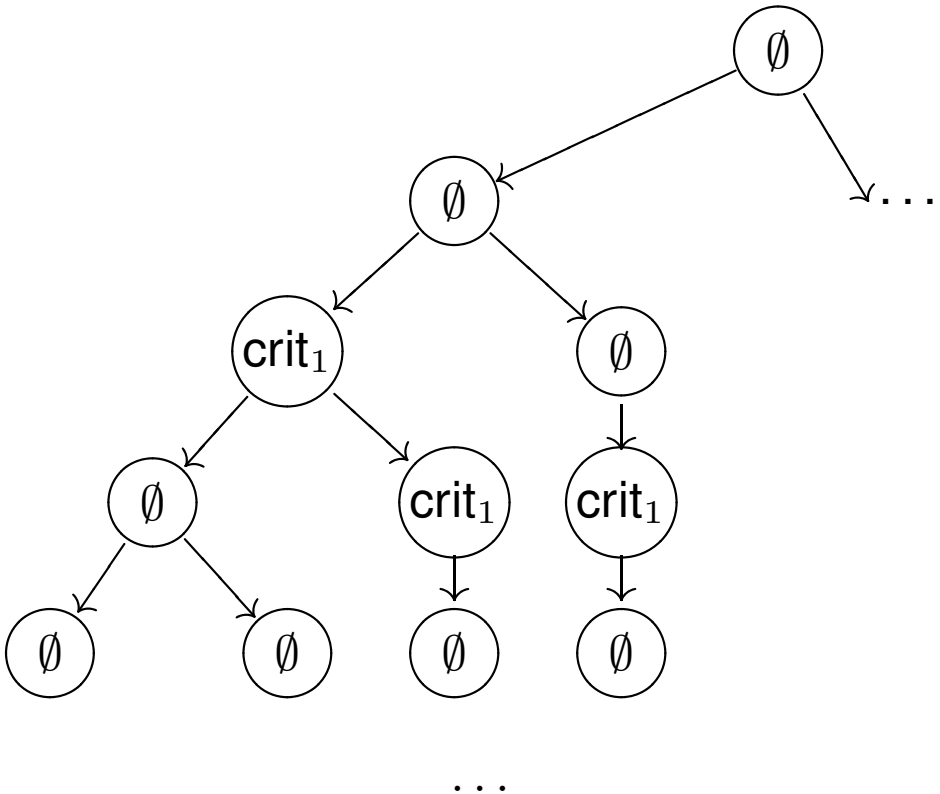
Sławomir Lasota
University of Warsaw

Plan

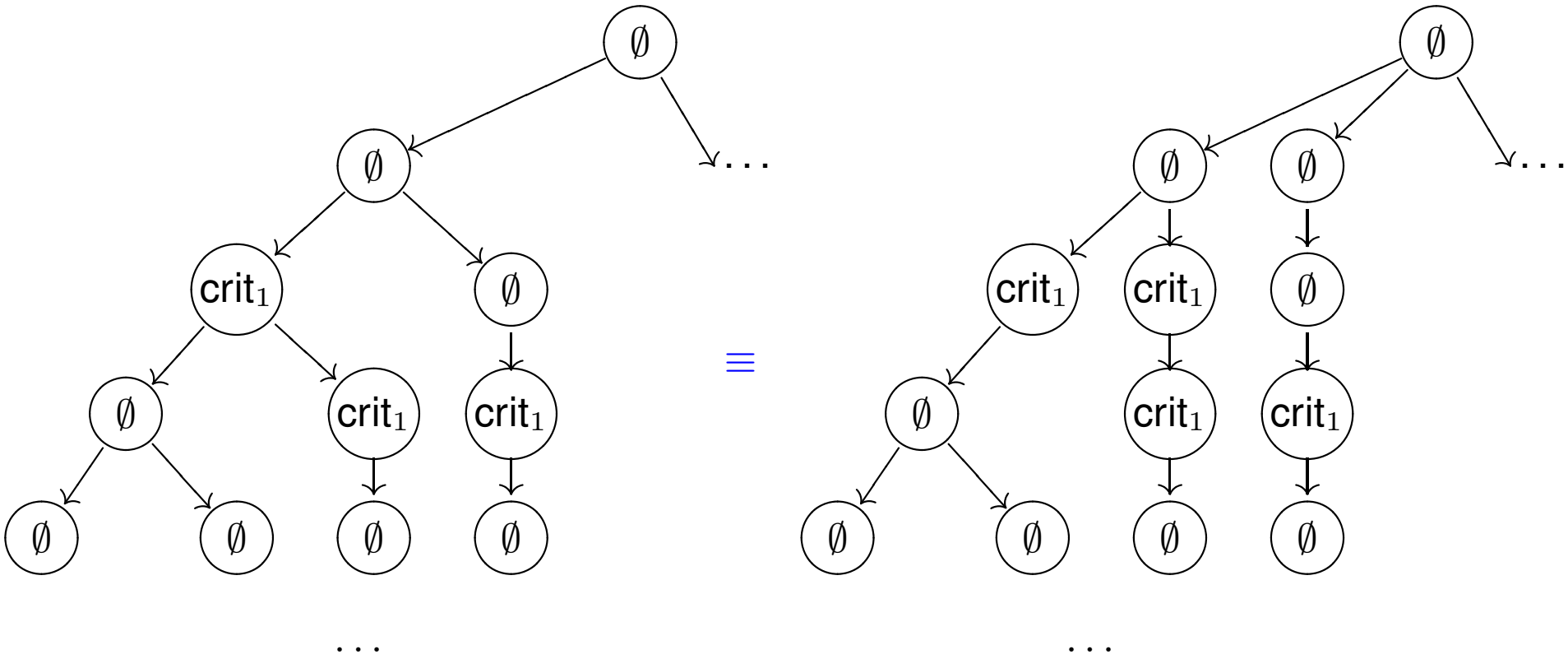
- Computation tree logic (CTL)
- CTL vs LTL
- CTL*
- Fairness in CTL
- CTL model checking
- Counterexamples

Kripke structure $\mapsto$ tree





Linear time



Computation tree logic (CTL)

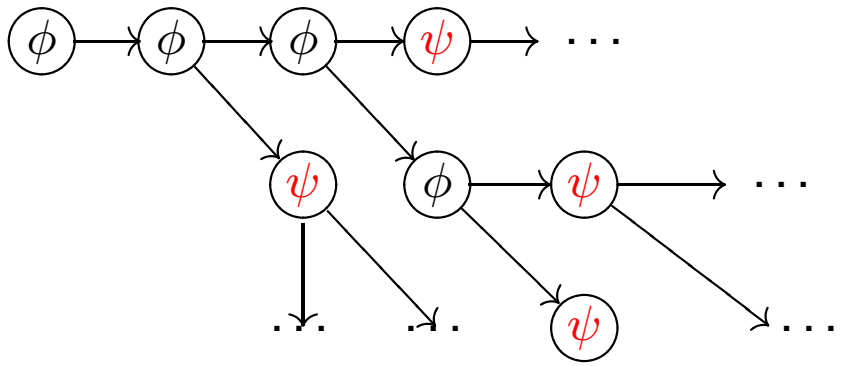
Def.: CTL (Computation Tree Logic)

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

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

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

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



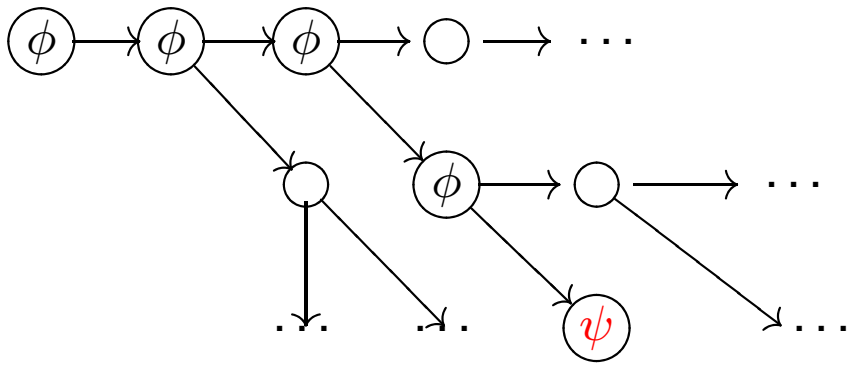
Def.: CTL (Computation Tree Logic)

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

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

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

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



Semantics

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

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

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

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

Semantics

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

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

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

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

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

Semantics

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

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

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

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

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

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

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

Semantics

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

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

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

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

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

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

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

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

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

$\Pi =$ 

$\Pi \models \mathsf{X}\,\phi$ iff $M, s_1 \models \phi$

$\Pi \models \phi_1\,\mathsf{U}\,\phi_2$ iff $\exists i < |\Pi|.\ M, s_i \models \phi_2 \wedge \forall j < i.\ M, s_j \models \phi_1$

Semantics

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

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

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

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

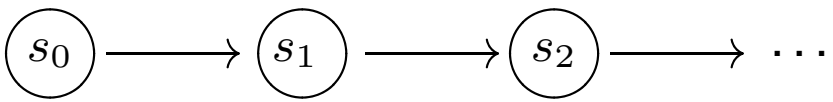
$M, s \models p$ iff $p \in L(s)$

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

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

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

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

$\Pi =$ 

$\Pi \models \mathsf{X}\,\phi$ iff $M, s_1 \models \phi$

$\Pi \models \phi_1\,\mathsf{U}\,\phi_2$ iff $\exists i < |\Pi|.\ M, s_i \models \phi_2 \wedge \forall j < i.\ M, s_j \models \phi_1$

Notation:

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

Example:

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

Notation:

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

Example:

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

Notation:

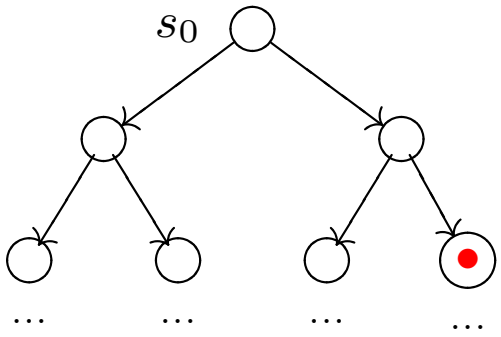
$$\begin{array}{lcl} \mathsf{AF}\,\phi & \equiv & \mathsf{A}\,\mathtt{true}\,\mathsf{U}\,\phi \\ \mathsf{EF}\,\phi & \equiv & \mathsf{E}\,\mathtt{true}\,\mathsf{U}\,\phi \\ \mathsf{AG}\,\phi & \equiv & \neg\ \mathsf{EF}\,\neg\phi \\ \mathsf{EG}\,\phi & \equiv & \neg\ \mathsf{AF}\,\neg\phi \end{array}$$

Example:

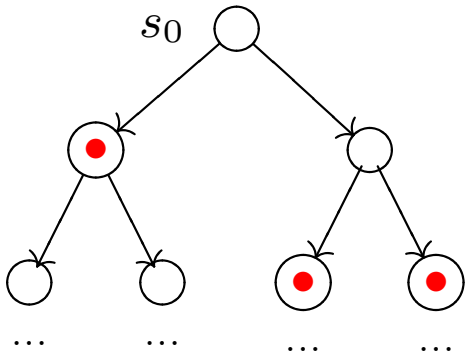
$$\mathsf{AG}\,(q \implies \mathsf{AF}\,r), \qquad \mathsf{AG}\ \mathsf{AF}\,\mathtt{enabled}$$

De Morgan's laws:

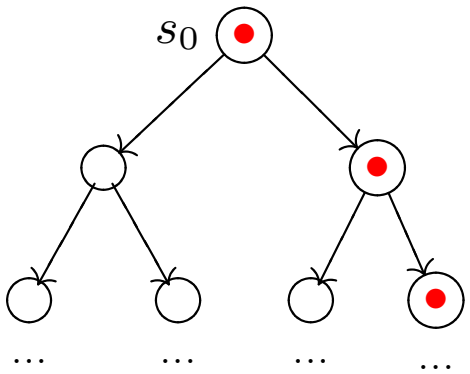
$$\begin{array}{lcl} \mathsf{AG}\,\phi & \equiv & \neg\ \mathsf{EF}\,\neg\phi \\ \mathsf{EG}\,\phi & \equiv & \neg\ \mathsf{AF}\,\neg\phi \\ \mathsf{AX}\,\phi & \equiv & \neg\ \mathsf{EX}\,\neg\phi \\ \phi_1 \vee \phi_2 & \equiv & \neg(\neg\phi_1 \wedge \neg\phi_2) \end{array} \qquad \begin{array}{lcl} ? & \equiv & \neg\,\mathsf{A}\,\neg\psi\,\mathsf{U}\,\neg\phi \\ ? & \equiv & \neg\,\mathsf{E}\,\neg\psi\,\mathsf{U}\,\neg\phi \end{array}$$



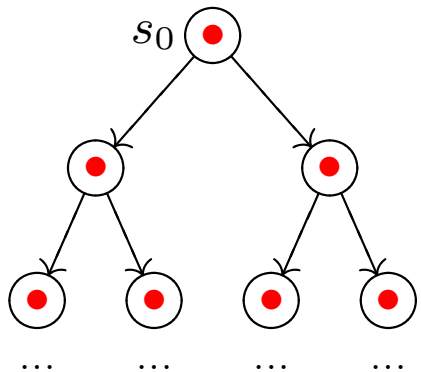
$M, s_0 \models$ EF ●



$M, s_0 \models$ AF ●



$M, s_0 \models$ EG ●



$M, s_0 \models$ AG ●

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 $\phi\,\mathsf{R}\,\psi$

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

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

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 $\phi\,\mathsf{R}\,\psi$

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

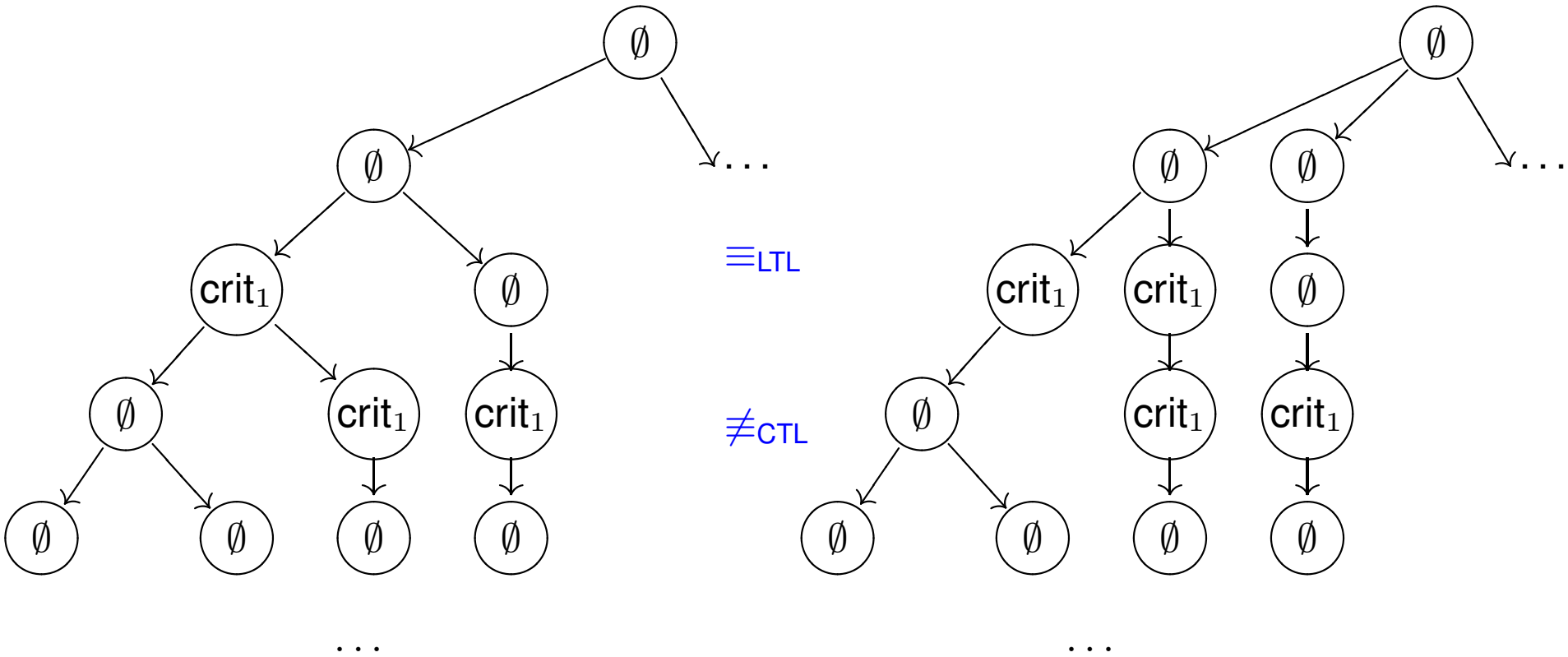
$\mathsf{E}\,\phi\,\mathsf{R}\,\psi \equiv \neg\,\mathsf{A}\,\neg\phi\,\mathsf{U}\,\neg\psi$

Def.: ACTL = CTL_+ without E

CTL vs LTL

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

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



LTL vs CTL

LTL	CTL	comments
$\mathsf{G}\,p, \quad \mathsf{F}\,p$	$\mathsf{AG}\,p, \quad \mathsf{AF}\,p$	$\in$ ACTL
$\mathsf{X}\,\mathsf{X}\,p$	$\mathsf{AX}\,\mathsf{AX}\,p$	$\in$ 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
—	$\mathsf{EF}\,p, \quad \mathsf{EG}\,p$	$M \not\models \mathsf{G}\,\neg p$

LTL vs CTL

LTL	CTL	comments
$\mathsf{G}\,p, \quad \mathsf{F}\,p$	$\mathsf{AG}\,p, \quad \mathsf{AF}\,p$	$\in$ ACTL
$\mathsf{X}\,\mathsf{X}\,p$	$\mathsf{AX}\,\mathsf{AX}\,p$	$\in$ 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
—	$\mathsf{EF}\,p, \quad \mathsf{EG}\,p$	$M \not\models \mathsf{G}\,\neg p$

Question: Is $M \models \mathsf{EF}\,p$ equivalent to $M \not\models \mathsf{G}\,\neg p$?

LTL vs CTL

LTL	CTL	comments
$\mathsf{G}\,p, \quad \mathsf{F}\,p$	$\mathsf{AG}\,p, \quad \mathsf{AF}\,p$	$\in$ ACTL
$\mathsf{X}\,\mathsf{X}\,p$	$\mathsf{AX}\,\mathsf{AX}\,p$	$\in$ 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
—	$\mathsf{EF}\,p, \quad \mathsf{EG}\,p$	$M \not\models \mathsf{G}\,\neg p$

Question: Is $M \models \mathsf{EF}\,p$ equivalent to $M \not\models \mathsf{G}\,\neg p$?

$M, s \models \mathsf{EF}\,p$ is equivalent to $M_s \not\models \mathsf{G}\,\neg p$

LTL vs CTL

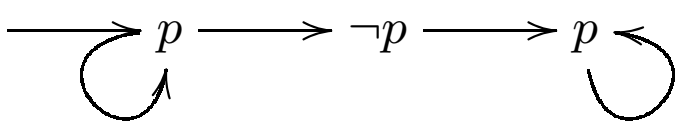
LTL	CTL	comments
$\mathsf{FG}\, r \Rightarrow \mathsf{GF}\, g$	—	
$\mathsf{GF}\, r \Rightarrow \mathsf{GF}\, g$	—	
—	$\mathsf{EX}\, \mathsf{AX}\, \mathsf{EX}\, p$	
—	$\mathsf{AG}\, \mathsf{EF}\, \texttt{start}$	

LTL vs CTL

LTL	CTL	comments
—	AF AX p	$\in$ ACTL
F X p	AX AF p	
—	AF $(p \wedge$ AX $p)$	$\in$ ACTL
F $(p \wedge$ X $p)$	—	
—	AF AG p	$\in$ ACTL
FG p	—	

LTL vs CTL

LTL	CTL	comments
—	AF AX p	$\in$ ACTL
F X p	AX AF p	
—	AF $(p \wedge$ AX $p)$	$\in$ ACTL
F $(p \wedge$ X $p)$	—	
—	AF AG p	$\in$ ACTL
FG p	—	

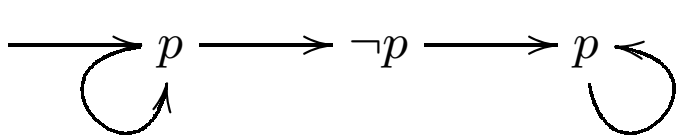


$\models$ FG p $\not\models$ AF AG p

AF AG p $\notin$ LTL

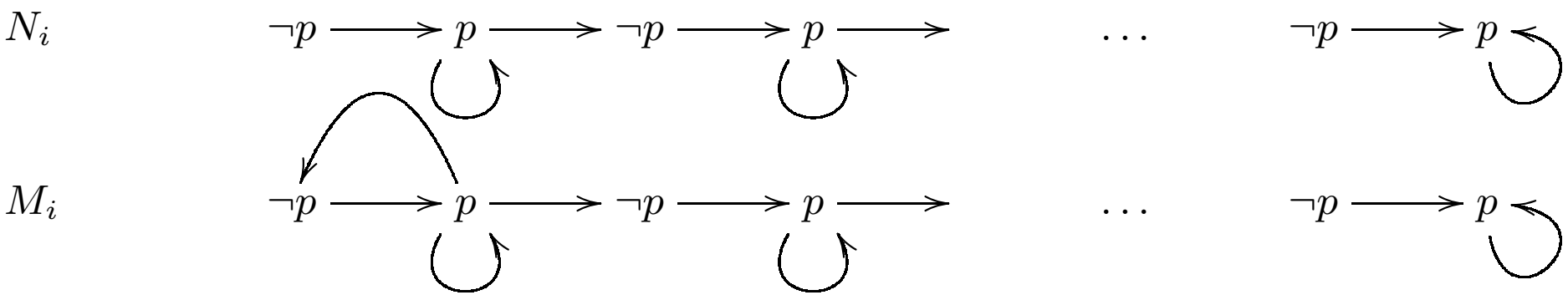
Thm.: $\mathrm{CTL} \ni \phi \longmapsto \psi \in \mathrm{LTL}$ (removing path quantifiers)

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

LTL	CTL	comments
—	AF AG p	
FG p	—	

(FG p $\neq$ AF AG p)

FG p $\notin$ CTL

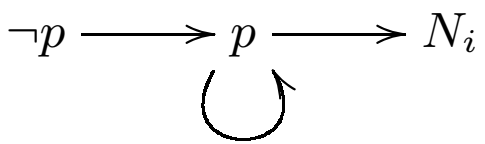


Fact: $N_i \models \mathsf{FG}\, p, \quad M_i \not\models \mathsf{FG}\, p.$

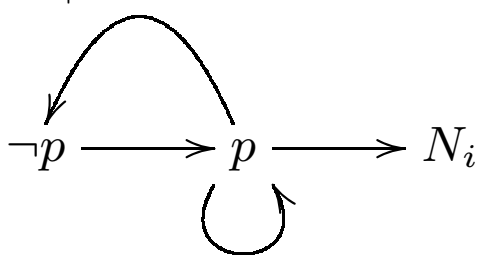
Let $\phi \in$ CTL.

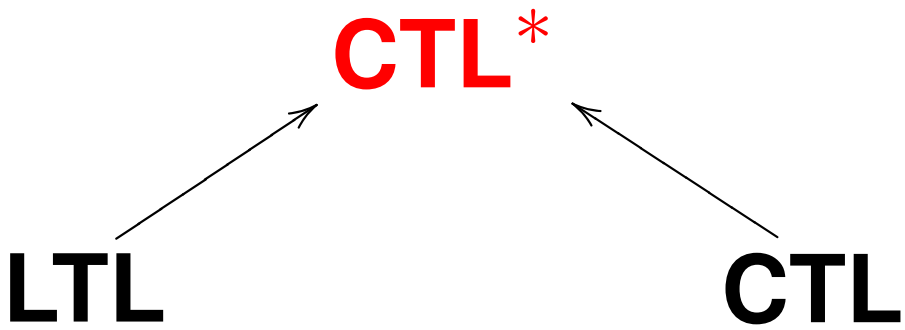
Lem.: If $i \geq \mathrm{size}(\phi)$, $N_i \models \phi \iff M_i \models \phi$.

N_{i+1}:



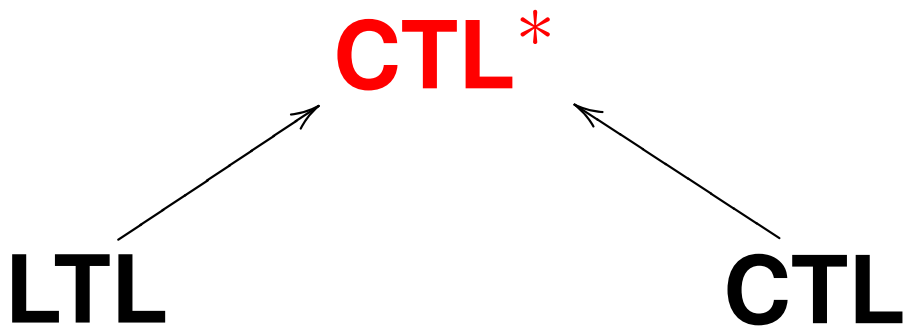
M_{i+1}:





Example: A F G p $\vee$ AG EF p $\notin$ LTL $\cup$ CTL

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



Example: A F G p $\vee$ AG EF p $\notin$ LTL $\cup$ CTL

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: $\Pi \models \psi$

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

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:

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

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:

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

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:

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

Example:

$$\mathsf{E}\,\mathsf{GF}\,p \notin \mathsf{LTL} \cup \mathsf{CTL}$$

Semantics

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

$s \models \phi$

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

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

$\Pi \models \psi$ $\qquad \Pi =$ 

$\Pi \models \phi$ 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: A ψ, where ψ "pure path formula" (without E , A)

CTL $\subset$ CTL*

restriction: occurrences of path quantifiers and temporal operators paired

LTL $\subset$ **CTL***

restriction: A ψ, where ψ "pure 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 $\phi \notin$ CTL*

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

Fairness

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

I. reachability

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

II. safety

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

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

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

Exercise: Write $\mathsf{A}\,(\neg\mathtt{start}\,\mathsf{U}\,\mathtt{key} \vee\ \mathsf{G}\,\neg\mathtt{start})$ in CTL.

Classification of properties

III. liveness

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

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

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

IV. deadlock freeness

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

Classification of properties

V. fairness

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

$$\mathsf{A}\,(\mathsf{GF}\,\texttt{head} \wedge \mathsf{GF}\,\texttt{tail})$$

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

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

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

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

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

Fair CTL

Semantics:

$M = \langle S, S_{\text{init}}, \rightarrow, L, \mathbf{F} \rangle$ $\qquad \mathbf{F} = \{X_1, \ldots, X_n\} \subseteq \mathcal{P}(S)$

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

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

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

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

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

Fair CTL

Semantics:

$M = \langle S, S_{\text{init}}, \rightarrow, L, \mathbf{F} \rangle$ $\qquad \mathbf{F} = \{X_1, \ldots, X_n\} \subseteq \mathcal{P}(S)$

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

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

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

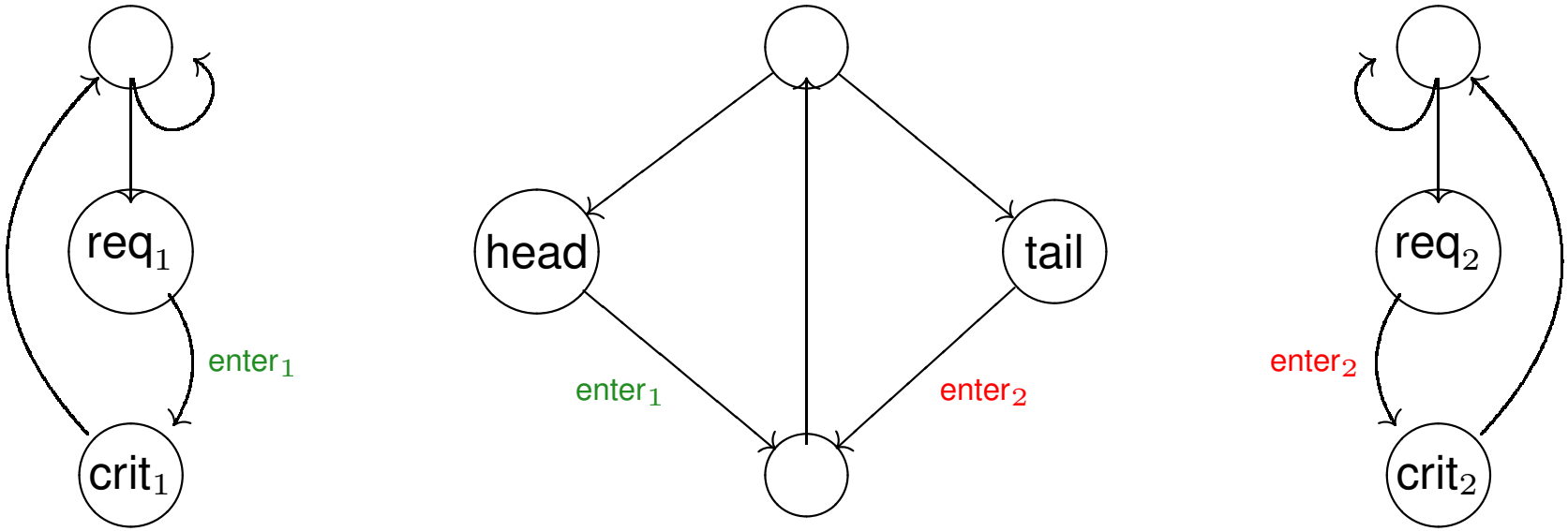
$$s \models_{\mathbf{F}} \mathsf{E}\,\psi \iff \exists \Pi.\ \Pi \text{ fair and starts in } s \text{ and } \Pi \models \psi$$

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

This setting is compatible with strong fairness

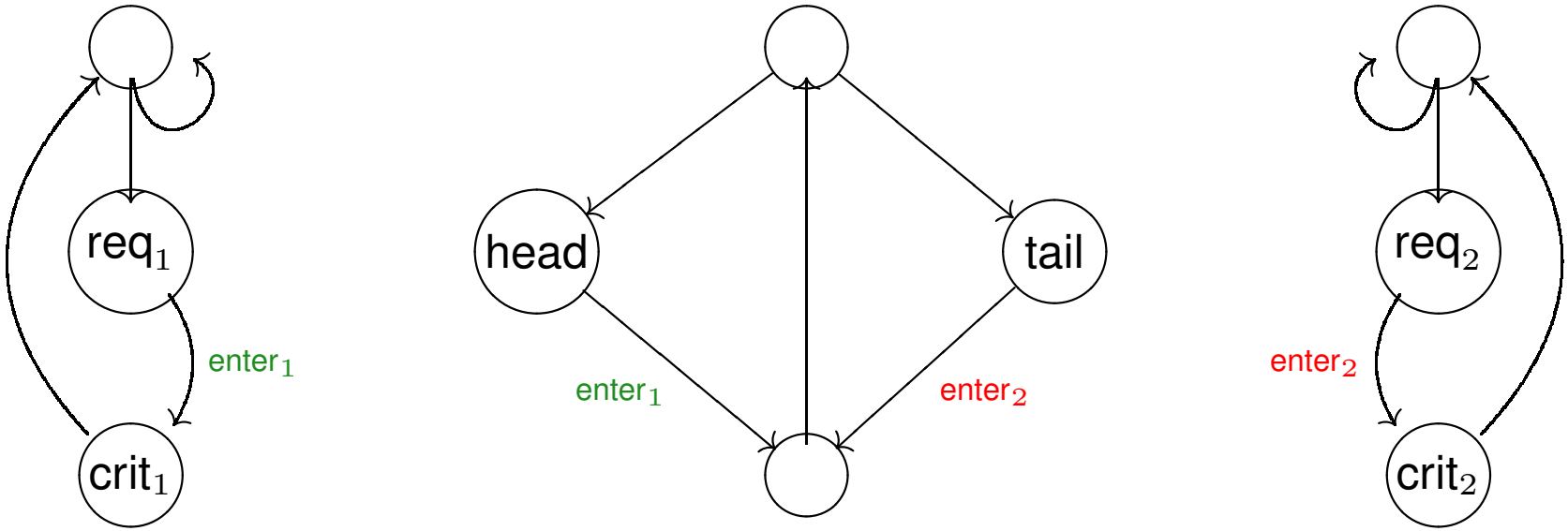
Example

randomized arbiter:



Example

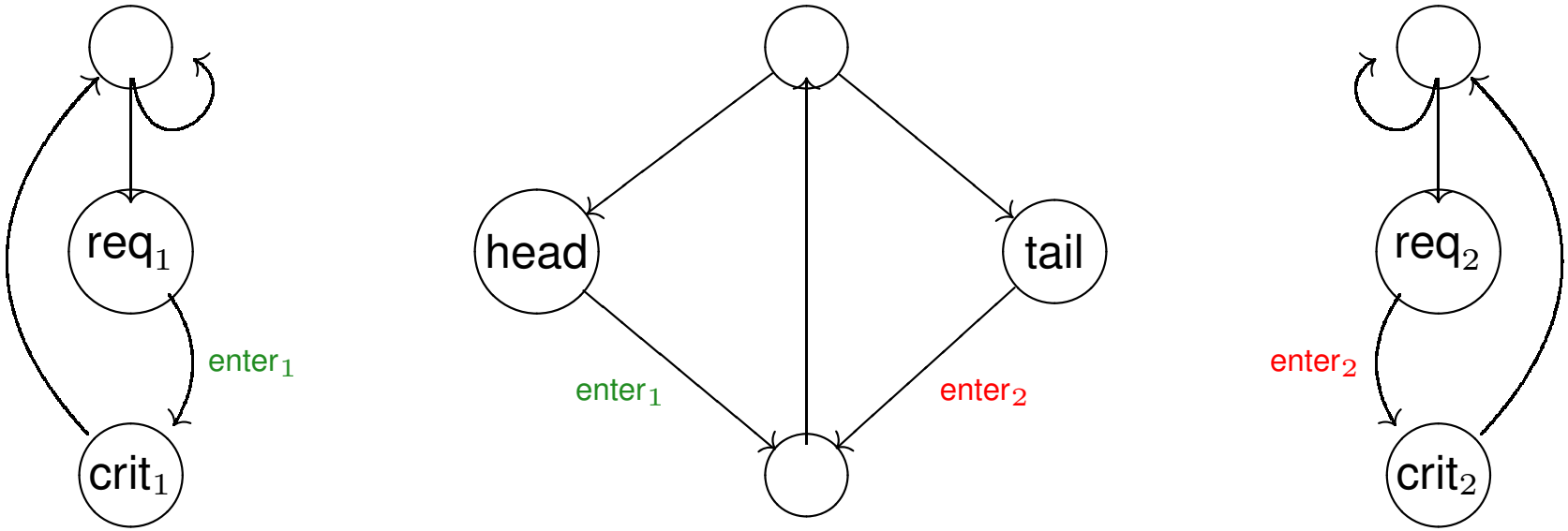
randomized arbiter:



$\not\models \mathsf{AG}\,(\mathsf{req}_1 \implies \mathsf{AF}\,\mathsf{crit}_1)$

Example

randomized arbiter:



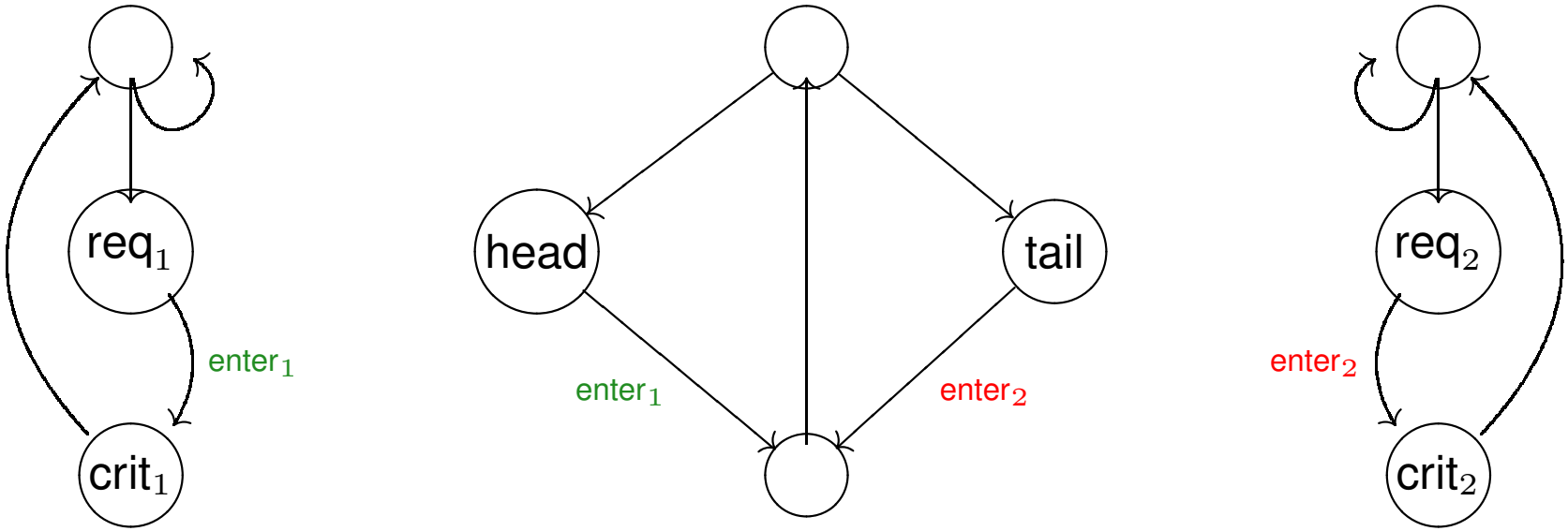
$\not\models$ AG (req$_1$ $\Longrightarrow$ AF crit$_1$)

$\models_{\mathbf{F}}$ AG (req$_1$ $\Longrightarrow$ AF crit$_1$)

$\mathbf{F} = \{$ GF head, GF tail$\}$

Example

randomized arbiter:



$\not\models$ AG (req$_1$ $\Longrightarrow$ AF crit$_1$)

$\models_{\mathbf{F}}$ AG (req$_1$ $\Longrightarrow$ AF crit$_1$)

$\mathbf{F} = \{$ GF head, GF tail$\}$

$\models$ A (fair $\Longrightarrow$ G (req$_1$ $\Longrightarrow$ A (fair $\Longrightarrow$ F crit$_1$)))

fair $\equiv$ GF head $\wedge$ GF tail

Examples

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

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

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

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

$$\ldots$$

Examples

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

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

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

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

$$\ldots$$

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

Conclusions

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

CTL model checking

Complexity

$\phi \in \ldots$	$M \models \phi$	satisfability ϕ
LTL	PSPACE $\quad \lvert M\rvert \cdot 2^{\mathcal{O}(\lvert\phi\rvert)}$	PSPACE
CTL	P $\quad \mathcal{O}(\lvert M\rvert \cdot \lvert\phi\rvert)$	EXPTIME
CTL_F	P $\quad \mathcal{O}(\lvert M\rvert \cdot (\lvert\phi\rvert + \lvert F\rvert))$	EXPTIME
CTL^*	PSPACE $\quad \lvert M\rvert \cdot 2^{\mathcal{O}(\lvert\phi\rvert)}$	2-EXPTIME
$L\mu$	NP $\cap$ co-NP $\quad \lvert M\rvert^{\mathcal{O}(\lvert\phi\rvert)}$	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!: LTL may be exponentially more succinct.

$$\mathsf{E}\,(\mathsf{F}\,a_1 \;\wedge\; \ldots \;\wedge\; \mathsf{F}\,a_n)$$

$$\bigvee_{\pi} \mathsf{EF}\,(a_{\pi(1)} \wedge \mathsf{EF}\,(a_{\pi(2)} \wedge \ldots \wedge \mathsf{EF}\,a_{\pi(n)})\ldots)$$

CTL model-checking

$M \models \phi$?

Algorithm labels states of M by subformulas of ϕ (global algorithm)

CTL ($\neg$, $\wedge$, **EX**, **E_U_**, **EG**) (these connectives are sufficient, prove it!)

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

EX ϕ: one step

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

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

Fair CTL model-checking

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

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

EG ϕ: $\quad S' := \{s \in S \mid s \models \phi\},\ F' := \{F_1 \cap S', \ldots, F_n \cap S'\} \quad \mapsto \quad M'$

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

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

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

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

Question: This setting is compatible with strong fairness.

How to adapt it to weak one?

Counterexamples

– a counterexample for $\mathsf{AF}\,(\,\mathsf{AX}\,a \vee\ \mathsf{AG}\,b)$ is...

Counterexamples

– a counterexample for $\mathsf{AF}\,(\,\mathsf{AX}\,a \vee\ \mathsf{AG}\,b)$ is...

  an example for $\mathsf{EG}\,(\,\mathsf{EX}\,\neg a \wedge\ \mathsf{EF}\,\neg b)$

Counterexamples

– a counterexample for $\mathsf{AF}\,(\,\mathsf{AX}\,a \vee\ \mathsf{AG}\,b)$ is...

  an example for $\mathsf{EG}\,(\,\mathsf{EX}\,\neg a \wedge\ \mathsf{EF}\,\neg b)$

– fair countexample for $\mathsf{AF}\,(\,\mathsf{AX}\,a \vee\ \mathsf{AG}\,b)$ is...

Counterexamples

– a counterexample for $\mathsf{AF}\,(\,\mathsf{AX}\,a \vee \mathsf{AG}\,b)$ is...

  an example for $\mathsf{EG}\,(\,\mathsf{EX}\,\neg a \wedge \mathsf{EF}\,\neg b)$

– fair countexample for $\mathsf{AF}\,(\,\mathsf{AX}\,a \vee \mathsf{AG}\,b)$ is...

  an example for $\mathsf{E}\,(\texttt{fair} \wedge \mathsf{G}\,(\,\mathsf{EX}\,(\neg a \wedge \texttt{fair}) \wedge \mathsf{EF}\,(\neg b \wedge \texttt{fair})))$

Counterexamples

– a counterexample for $\mathsf{AF}\,(\,\mathsf{AX}\,a \vee\ \mathsf{AG}\,b)$ is...

  an example for $\mathsf{EG}\,(\,\mathsf{EX}\,\neg a \wedge\ \mathsf{EF}\,\neg b)$

– fair countexample for $\mathsf{AF}\,(\,\mathsf{AX}\,a \vee\ \mathsf{AG}\,b)$ is...

  an example for $\mathsf{E}\,(\mathtt{fair} \wedge\ \mathsf{G}\,(\,\mathsf{EX}\,(\neg a \wedge \mathtt{fair}) \wedge\ \mathsf{EF}\,(\neg b \wedge \mathtt{fair})))$

– this works for ACTL