Linear and branching temporal logic

- **Linear** temporal logic:

  "statements about (all) paths starting in a state"

  $s \models \mathsf{G}(x \leq 20)$ iff for all possible paths starting in s always $x \leq 20$

- **Branching** temporal logic:

  "statements about all or some paths starting in a state"

  $s \models \mathsf{AG}\,(x \leq 20)$ iff for **all** paths starting in s always $x \leq 20$
  $s \models \mathsf{EG}\,(x \leq 20)$ iff for **some** path starting in s always $x \leq 20$
  nesting of path quantifiers is allowed

- Checking $\mathsf{E}\,\varphi$ in LTL can be done using $\mathsf{A}\,\neg\varphi$
  - (but this does not work for nested formulas such as $\mathsf{AG}\,\mathsf{EF}\,a$)

Linear versus branching temporal logic

- Semantics is based on a branching notion of time
  - an infinite tree of states obtained by unfolding transition system
  - one "time instant" may have several possible successor "time instants"
- Incomparable expressiveness
  - there are properties that can be expressed in LTL, but not in CTL
  - there are properties that can be expressed in CTL, but not in LTL
- Different model checking algorithms and complexities
- Different treatment of fairness assumptions
- Different equivalences (pre-orders) on transition systems

Linear and branching temporal logic

- **Linear** temporal logic:

  "statements about (all) paths starting in a state"

  $s \models \Box(x \leq 20)$ iff for all possible paths starting in s always $x \leq 20$

- **Branching** temporal logic:

  "statements about all or some paths starting in a state"

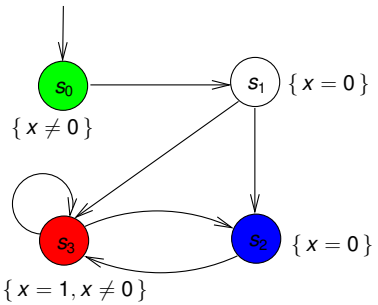
  $s \models \mathrm{AG}\,(x \leq 20)$ iff for **all** paths starting in s always $x \leq 20$
  $s \models \mathrm{EG}\,(x \leq 20)$ iff for **some** path starting in s always $x \leq 20$
  nesting of path quantifiers is allowed

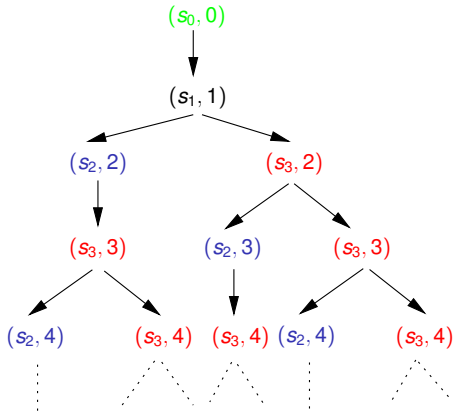
- Checking $\mathrm{E}\,\varphi$ in LTL can be done using $\mathrm{A}\,\neg\varphi$
  - (but this does not work for nested formulas such as $\mathrm{AG}\,\mathrm{EF}\,a$)

Linear versus branching temporal logic

- Semantics is based on a branching notion of time
  - an infinite tree of states obtained by unfolding transition system
  - one "time instant" may have several possible successor "time instants"
- Incomparable expressiveness
  - there are properties that can be expressed in LTL, but not in CTL
  - there are properties that can be expressed in CTL, but not in LTL
- Different model checking algorithms and complexities
- Different treatment of fairness assumptions
- Different equivalences (pre-orders) on transition systems

Transition systems and trees





CTL

Computation Tree Logic

Computation tree logic

modal logic over infinite trees [Clarke & Emerson 1981]

- State formulas Φ
  - $a \in AP$ — atomic proposition
  - $\neg\Phi$ and $\Phi \wedge \Psi$ — negation and conjunction
  - $\mathsf{E}\,\varphi$ — there **exists** a path fulfilling φ
  - $\mathsf{A}\,\varphi$ — **all** paths fulfill φ
- Path formulas φ
  - $\mathsf{X}\,\Phi$ — the next state fulfills Φ
  - $\Phi\,\mathsf{U}\,\Psi$ — Φ holds until a Ψ-state is reached

$\Rightarrow$ note that X and U **alternate** with A and E

- $\mathsf{AX}\,\mathsf{X}\,\Phi$ and $\mathsf{A}\,\mathsf{EX}\,\Phi \notin$ CTL, but $\mathsf{AX}\,\mathsf{AX}\,\Phi$ and $\mathsf{AX}\,\mathsf{EX}\,\Phi \in$ CTL

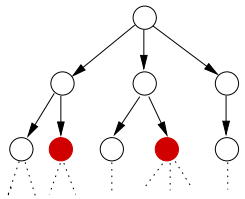
Alternative syntax: $\mathsf{E} \approx \exists$, $\mathsf{A} \approx \forall$, $\mathsf{X} \approx \bigcirc$, $\mathsf{G} \approx \Box$, $\mathsf{F} \approx \Diamond$.

Derived operators

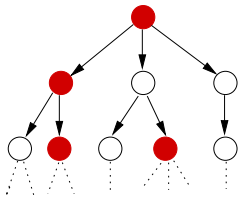
potentially Φ:	$\mathsf{E}\,\mathsf{F}\,\Phi$	$=$	$\mathsf{E}\,(\mathsf{true}\,\mathsf{U}\,\Phi)$
inevitably Φ:	$\mathsf{A}\,\mathsf{F}\,\Phi$	$=$	$\mathsf{A}\,(\mathsf{true}\,\mathsf{U}\,\Phi)$
potentially always Φ:	$\mathsf{E}\,\mathsf{G}\,\Phi$	$:=$	$\neg\mathsf{A}\,\mathsf{F}\,\neg\Phi$
invariantly Φ:	$\mathsf{A}\,\mathsf{G}\,\Phi$	$=$	$\neg\mathsf{E}\,\mathsf{F}\,\neg\Phi$
weak until:	$\mathsf{E}\,(\Phi\,\mathsf{W}\,\Psi)$	$=$	$\neg\mathsf{A}\,((\Phi \wedge \neg\Psi)\,\mathsf{U}\,(\neg\Phi \wedge \neg\Psi))$
	$\mathsf{A}\,(\Phi\,\mathsf{W}\,\Psi)$	$=$	$\neg\mathsf{E}\,((\Phi \wedge \neg\Psi)\,\mathsf{U}\,(\neg\Phi \wedge \neg\Psi))$

the boolean connectives are derived as usual

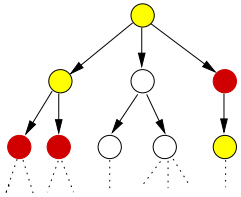
Visualization of semantics



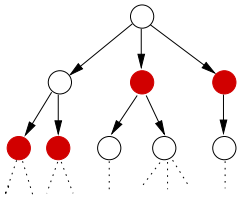
EF *red*



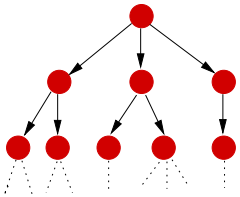
EG *red*



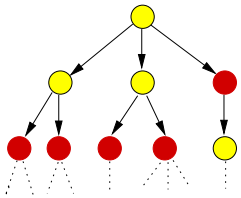
E (*yellow* U *red*)



AF *red*



AG *red*



A (*yellow* U *red*)

Semantics of CTL state-formulas

Defined by a relation $\models$ such that

$s \models \Phi$ if and only if formula Φ holds in state s

$s \models a$	iff	$a \in L(s)$
$s \models \neg\Phi$	iff	$\neg(s \models \Phi)$
$s \models \Phi \wedge \Psi$	iff	$(s \models \Phi) \wedge (s \models \Psi)$
$s \models \mathrm{E}\,\varphi$	iff	$\pi \models \varphi$ for some path π that starts in s
$s \models \mathrm{A}\,\varphi$	iff	$\pi \models \varphi$ for all paths π that start in s

Semantics of CTL path-formulas

Defined by a relation $\models$ such that

$\pi \models \varphi$ *if and only if path* π *satisfies* φ

$\pi \models \mathsf{X}\,\Phi$ iff $\pi[1] \models \Phi$

$\pi \models \Phi\,\mathsf{U}\,\Psi$ iff $(\exists\, j \geq 0.\, \pi[j] \models \Psi \ \wedge\ (\forall\, 0 \leq k < j.\, \pi[k] \models \Phi))$

where $\pi[i]$ denotes the state s_i in the path $\pi = s_0 s_1 s_2 \ldots$

Transition system semantics

- For CTL-state-formula Φ, the **satisfaction set** $Sat(\Phi)$ is defined by:

$$Sat(\Phi) = \{\, s \in S \mid s \models \Phi \,\}$$

- *TS* satisfies CTL-formula Φ iff Φ holds in all its initial states:

$$TS \models \Phi \quad \text{if and only if} \quad \forall s_0 \in I.\, s_0 \models \Phi$$

  - this is equivalent to $I \subseteq Sat(\Phi)$

- Note: It is possible that both $TS \not\models \Phi$ and $TS \not\models \neg\Phi$
  - (because of several initial states, e.g. $s_0 \models \mathsf{EG}\,\Phi$ and $s_0' \not\models \mathsf{EG}\,\Phi$)

CTL equivalence

CTL-formulas Φ and Ψ (over AP) are **equivalent**, denoted $\Phi \equiv \Psi$

if and only if $Sat(\Phi) = Sat(\Psi)$
for all transition systems TS over AP

$\Phi \equiv \Psi$ iff ($TS \models \Phi$ if and only if $TS \models \Psi$)

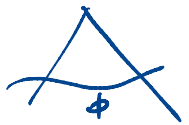
Duality laws

$$\begin{aligned}
AX\Phi &\equiv \neg EX\neg\Phi \\
EX\Phi &\equiv \neg AX\neg\Phi \\
AF\Phi &\equiv \neg EG\neg\Phi \\
EF\Phi &\equiv \neg AG\neg\Phi \\
A(\Phi U \Psi) &\equiv \neg E((\Phi \wedge \neg\Psi) W (\neg\Phi \wedge \neg\Psi))
\end{aligned}$$

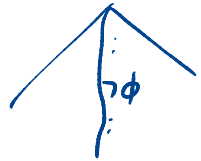
LTL:
$\varphi W \psi \equiv G\varphi \vee (\varphi U \psi)$
(weak until)
$\neg(\varphi U \psi) \equiv (\varphi \wedge \neg\psi) W (\neg\varphi \wedge \neg\psi)$

$s \models AX\phi$ iff $\forall\, s \to s' : s' \models \phi$

$s \models AF\phi$



$s \models EG(\neg\phi)$



Expansion laws

$$A(\Phi U \Psi) \equiv \Psi \vee (\Phi \wedge AXA(\Phi U \Psi))$$
$$AF\Phi \equiv \Phi \vee AXAF\Phi$$
$$AG\Phi \equiv \Phi \wedge AXAG\Phi$$

$$E(\Phi U \Psi) \equiv \Psi \vee (\Phi \wedge EXE(\Phi U \Psi))$$
$$EF\Phi \equiv \Phi \vee EXEF\Phi$$
$$EG\Phi \equiv \Phi \wedge EXEG\Phi$$

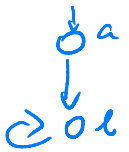
Distributive laws

$$AG(\Phi \wedge \Psi) \equiv AG\Phi \wedge AG\Psi$$
$$EF(\Phi \vee \Psi) \equiv EF\Phi \vee EF\Psi$$

note that $EG(\Phi \wedge \Psi) \not\equiv EG\Phi \wedge EG\Psi$ and
$AF(\Phi \vee \Psi) \not\equiv AF\Phi \vee AF\Psi$

$\phi \equiv a$
$\psi \equiv b$

$AF(\phi \wedge \psi) \not\equiv AF\phi \wedge AF\psi$



$ST \not\models AFa, AFb$

$ST \not\models AF(a \wedge b)$

$EG(\phi \vee \psi) \not\equiv EG\phi \vee EG(\psi)$

Existential normal form (ENF)

The set of CTL formulas in **existential normal form** (ENF) is given by:

$$\Phi \;::=\; \text{true} \;\Big|\; a \;\Big|\; \Phi_1 \wedge \Phi_2 \;\Big|\; \neg\Phi \;\Big|\; \mathsf{EX}\,\Phi \;\Big|\; \mathsf{E}\,(\Phi_1\,\mathsf{U}\,\Phi_2) \;\Big|\; \mathsf{EG}\,\Phi$$

For each CTL formula, there exists an equivalent CTL formula in ENF

$$\begin{aligned}
\mathsf{AX}\,\Phi &\equiv \neg\mathsf{EX}\,\neg\Phi \\
\mathsf{A}\,(\Phi\,\mathsf{U}\,\Psi) &\equiv \neg\mathsf{E}\,(\neg\Psi\,\mathsf{U}\,(\neg\Phi \wedge \neg\Psi)) \wedge \neg\mathsf{EG}\,\neg\Psi
\end{aligned}$$

Existential normal form (ENF)

The set of CTL formulas in **existential normal form** (ENF) is given by:

$$\Phi \;::=\; \text{true} \;\Big|\; a \;\Big|\; \Phi_1 \wedge \Phi_2 \;\Big|\; \neg\Phi \;\Big|\; \mathsf{EX}\,\Phi \;\Big|\; \mathsf{E}\,(\Phi_1\,\mathsf{U}\,\Phi_2) \;\Big|\; \mathsf{EG}\,\Phi$$

For each CTL formula, there exists an equivalent CTL formula in ENF

$$\begin{aligned}
\mathsf{AX}\,\Phi &\equiv \neg\mathsf{EX}\,\neg\Phi \\
\mathsf{A}\,(\Phi\,\mathsf{U}\,\Psi) &\equiv \neg\mathsf{E}\,(\neg\Psi\,\mathsf{U}\,(\neg\Phi \wedge \neg\Psi)) \wedge \neg\mathsf{EG}\,\neg\Psi
\end{aligned}$$

Existential normal form (ENF)

The set of CTL formulas in **existential normal form** (ENF) is given by:

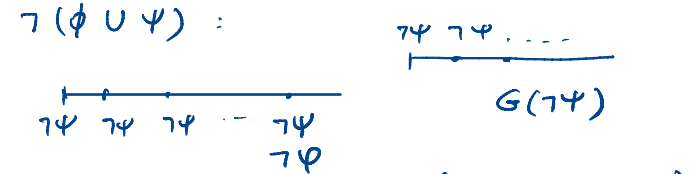
$$\Phi ::= \text{true} \mid a \mid \Phi_1 \wedge \Phi_2 \mid \neg\Phi \mid \text{EX}\,\Phi \mid \text{E}\,(\Phi_1\,\text{U}\,\Phi_2) \mid \text{EG}\,\Phi$$

For each CTL formula, there exists an equivalent CTL formula in ENF

$$\text{AX}\,\Phi \equiv \neg\text{EX}\,\neg\Phi$$

$$\text{A}\,(\Phi\,\text{U}\,\Psi) \equiv \neg\text{E}\,(\neg\Psi\,\text{U}\,(\neg\Phi \wedge \neg\Psi)) \wedge \neg\text{EG}\,\neg\Psi$$

$\neg(\phi\,U\,\psi)$:



$\neg(\phi\,U\,\psi) \equiv G(\neg\psi) \vee (\neg\psi\,U(\neg\psi \wedge \neg\phi))$

$E(\phi_1 \vee \phi_2) \equiv E(\phi_1) \vee E(\phi_2)$