

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”

$s \models \text{AG}(x \leq 20)$ iff for **all** paths starting in s always $x \leq 20$

$s \models \text{EG}(x \leq 20)$ iff for **some** path starting in s always $x \leq 20$

nesting of path quantifiers is allowed

- ▶ Checking $E\varphi$ in LTL can be done using $A\neg\varphi$

- ▶ (but this does not work for nested formulas such as $\text{AGEF } a$)

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**

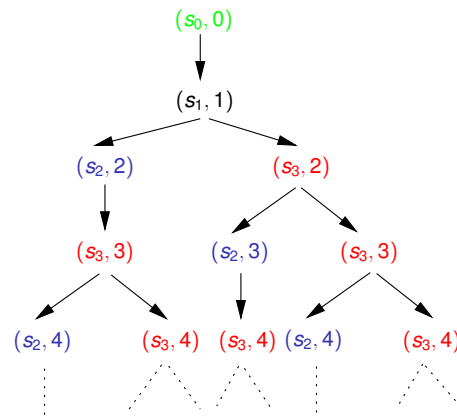
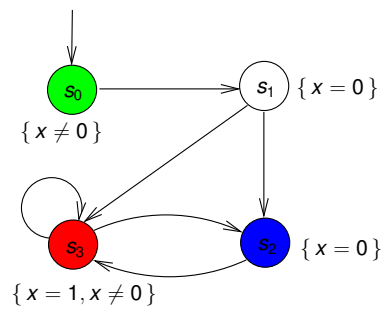
- ▶ there are properties that can be expressed in LTL, but not in CTL
- ▶ there are properties that can be expressed in CTL, but not in LTL

- ▶ Different **model checking algorithms** and complexities

- ▶ Different treatment of **fairness assumptions**

- ▶ Different **equivalences** (pre-orders) on transition systems

Transition systems and trees



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
- ▶ $E\varphi$ there **exists** a path fulfilling φ
- ▶ $A\varphi$ **all** paths fulfill φ

▶ Path formulas φ

- ▶ $X\phi$ the next state fulfills ϕ
- ▶ $\phi U \psi$ ϕ holds until a ψ -state is reached

⇒ note that X and U **alternate** with A and E

- ▶ $AXX\phi$ and $AEX\phi \notin \text{CTL}$, but $AXAX\phi$ and $AXEX\phi \in \text{CTL}$

Alternative syntax: $E \approx \exists$, $A \approx \forall$, $X \approx \bigcirc$, $G \approx \square$, $F \approx \diamond$.

Derived operators

potentially ϕ : $EF\phi = E(\text{true} U \phi)$

inevitably ϕ : $AF\phi = A(\text{true} U \phi)$

potentially always ϕ : $EG\phi := \neg AF\neg\phi$

invariantly ϕ : $AG\phi = \neg EF\neg\phi$

weak until: $E(\phi W \psi) = \neg A((\phi \wedge \neg\psi) U (\neg\phi \wedge \neg\psi))$

$A(\phi W \psi) = \neg E((\phi \wedge \neg\psi) U (\neg\phi \wedge \neg\psi))$

the boolean connectives are derived as usual

Semantics of CTL path-formulas

Defined by a relation \models such that

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

$$\pi \models X\Phi \quad \text{iff } \pi[1] \models \Phi$$

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

where $\pi[j]$ denotes the state s_j in the path $\pi = s_0 s_1 s_2 \dots$

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:

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

- ▶ 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. $s_0 \models EG\Phi$ and $s'_0 \not\models EG\Phi$)

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

$$AX\phi \equiv \neg EX\neg\phi$$

$$EX\phi \equiv \neg AX\neg\phi$$

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

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

$$A(\phi U \psi) \equiv \neg E((\phi \wedge \neg\psi) W (\neg\phi \wedge \neg\psi))$$

Expansion laws

$$A(\Phi \cup \Psi) \equiv \Psi \vee (\Phi \wedge AXA(\Phi \cup \Psi))$$

$$AF\Phi \equiv \Phi \vee AXAF\Phi$$

$$AG\Phi \equiv \Phi \wedge AXAG\Phi$$

$$E(\Phi \cup \Psi) \equiv \Psi \vee (\Phi \wedge EXE(\Phi \cup \Psi))$$

$$EF\Phi \equiv \Phi \vee EXEF\Phi$$

$$EG\Phi \equiv \Phi \wedge EXEG\Phi$$

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
 $AF(\Phi \vee \Psi) \not\equiv AF\Phi \vee AF\Psi$

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

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

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