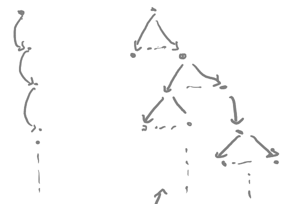
CTL (*)

LTL f.lae implicitely universally quantify on paths

$$s \models \varphi \iff \text{for all } \pi \in Paths(s).\ \pi \models \varphi$$

Natures of (discrete) Time



closer to reactive systems

Example: LTL cannot precisely express

"for all computations it is possible φ"

$\underbrace{\qquad\qquad}_{\forall\square}$ $\underbrace{\quad}_{\exists\lozenge}$ $\underbrace{\quad}_{\varphi}$

$$\boxed{CTL = LTL + \exists \text{path}}$$

(Clarke & Emerson 81, Queille & Sifakis 82-83)

for all paths — for some path

Syntax

STATE F.LAE $\qquad \Phi ::= true \mid \underset{AP}{a} \mid \neg\Phi \mid \Phi \wedge \Phi \mid \forall\varphi \mid \exists\varphi$

path f.lae $\qquad \varphi ::= \circ\Phi \mid \Phi \,\mathsf{U}\, \Phi$

Example Safety $\qquad \forall\square(\neg c_1 \vee \neg c_2) \qquad \forall\square\left(\bigwedge_{1\leq i \neq j \leq n} \neg c_i \vee \neg c_j\right)$

Liveness $\qquad \bigwedge_{1\leq i\leq n} \forall\square\forall\lozenge\, c_i \qquad$ Mutex in CTL

Another CTL liveness f.la: $\forall\square(req \rightarrow \forall\lozenge\, res)$

Obs Temporal operators cannot be immediately preceded by other temporal operators:

- $\exists\square\lozenge\varphi$ ✗
- $\exists\square\forall\lozenge\varphi$ ✓

Also, $\forall(\cdots \wedge \cdots)$ $\exists\neg\cdots$ are not legal!

Semantics $\boxed{TS \models \Phi \iff \forall s \in I.\ s \models \Phi}$

$s \models true$

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

$s \models \neg\Phi \iff$ not $s \models \Phi$

$s \models \Phi \wedge \Psi \iff s \models \Phi$ & $s \models \Psi$

$s \models \exists \varphi \iff$ for a $\pi \in Paths(s)$: $\pi \models \varphi$

$s \models \forall \varphi \iff$ for all $\pi \in Paths(s)$: $\pi \models \varphi$

$\pi \models \circ\Phi \iff \pi[1] \models \Phi$

$\pi \models \Phi \cup \Psi \iff \exists_{j \geq 0} : \pi[j] \models \Psi$ & $\forall_{0 \leq i < j} : \pi[h] \models \Phi$

Eventually $\begin{cases} \exists\Diamond\phi \equiv \exists(true \cup \phi) \\ \forall\Diamond\phi \equiv \forall(true \cup \phi) \end{cases}$

potentially ϕ

inevitably ϕ

Always $\begin{cases} \exists\Box\phi \equiv \neg\forall\Diamond\neg\phi \\ \forall\Box\phi \equiv \neg\exists\Diamond\neg\phi \end{cases}$

potentially invariantly ϕ

invariantly ϕ

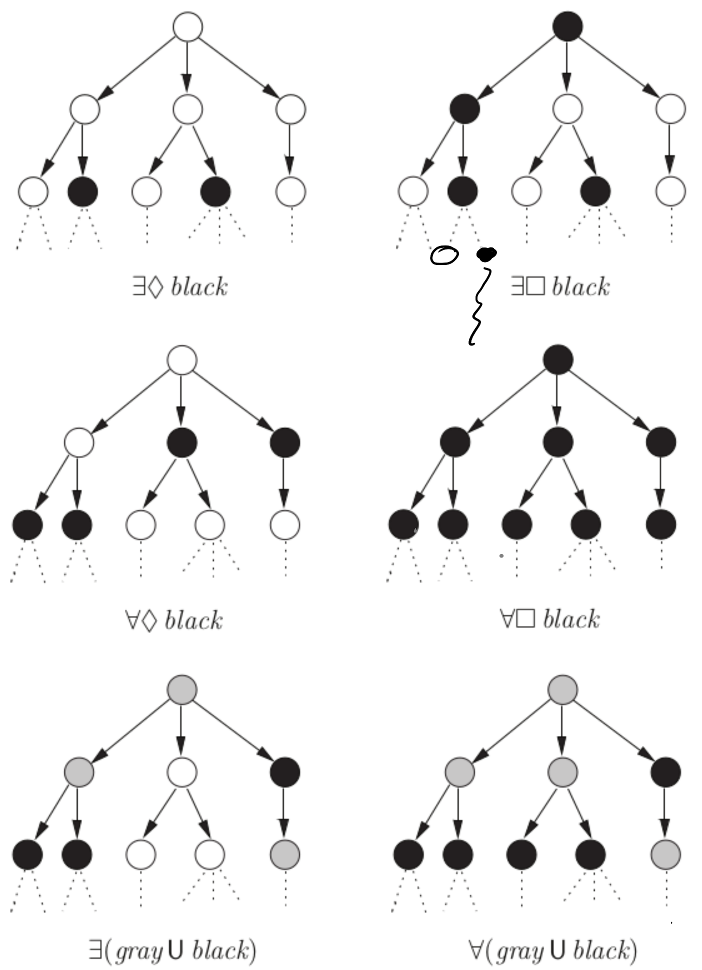


Figure 6.2: Visualization of semantics of some basic CTL formulae.

Fig. 6.2 borrowed from [1]

The syntactic restrictions of CTL forbid writing e.g.

<u>fairness</u> $\bigwedge_{0\le i\le n} (\Box\Diamond w_i \to \Box\Diamond c_i)$ is <u>not</u> a CTL f.la

which is not in CTL because of the consecutive temporal operators.

[Emerson & Halpern 86] propose CTL*

Syntax

$$\Phi ::= true \mid \underset{\in AP}{a} \mid \neg\Phi \mid \Phi\wedge\Phi \mid \exists\varphi \qquad \text{state f.lae}$$

$$\varphi ::= \Phi \mid \varphi\wedge\varphi \mid \neg\varphi \mid \bigcirc\varphi \mid \varphi\, U\, \varphi \qquad \text{path f.lae}$$

<u>Semantics</u> $\boxed{TS \models \Phi \iff \forall s\in I.\ s\models\Phi}$

$$\left.\begin{array}{lll} \forall s\in S\ s\models true & \vdots & s\models a \iff a\in L(s) \\ s\models\neg\Phi & \iff & \text{not } s\models\Phi \\ s\models\Phi\wedge\Psi & \iff & s\models\Phi \ \&\ s\models\Psi \\ s\models\exists\varphi & \iff & \exists\pi\in Paths(s): \pi\models\varphi \end{array}\right\} \text{as for CTL}$$

$$\pi\models\Phi \iff \pi[0]\models\Phi$$

$$\pi\models\varphi_1\wedge\varphi_2 \iff \pi\models\varphi_1 \ \&\ \pi\models\varphi_2$$

$$\pi\models\neg\varphi \iff \pi\not\models\varphi$$

$$\pi\models\bigcirc\varphi \iff \pi_{\geq 1}\models\varphi$$

$$\pi\models\varphi_1 U\varphi_2 \iff \exists j\geq 0: \pi_{\geq j}\models\varphi_2 \ \&\ (\forall 0\le h<j: \pi_{\geq h}\models\varphi_1)$$