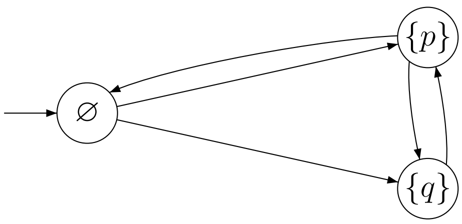
Bernd Finkbeiner Date: July 5, 2011

Automata, Games and Verification: Lecture 13

21 Computation Tree Logic

Example: Examples of CTL* formulas:

- AG($q \to$ F p)
- EF($p \wedge \neg q$)
- AG(EF $\neg p \wedge \neg q$)



Definition 1 *Let AP be a set of atomic propositions. A* Kripke structure *over AP is a tuple $M = (S, R, L)$*

- *S : a set of states*
- *$R \subseteq S \times S$: a transition relation*
- *$L : S \to 2^{AP}$: labels each states with the set of atomic propositions that are assured to be true in S*

Definition 2 *A* pointed Kripke structure *$(\mathcal{M}, s)$ is a Kripke structure $\mathcal{M}$ with an initial state $s \in S$.*

CTL* Syntax (f, g - state formulas, φ, ψ - path formulas):

- State formulas f:
$$f \ ::= \ AP \mid \neg f \mid f \vee g \mid A\varphi \mid E\varphi$$
- Path formulas φ:
$$\varphi ::= \ f \mid \neg\varphi \mid \varphi \vee \psi \mid G\varphi \mid F\varphi \mid \varphi U \psi \mid X\varphi$$

CTL* Semantics ($\mathcal{M}$ - Kripke structure, s - state, π^i - suffix of π starting at i):

- $\mathcal{M}, s \models p$ iff $p \in L(s)$ for $p \in AP$
- $\mathcal{M}, s \models \neg f$ iff $\mathcal{M}, s \not\models f$
- $\mathcal{M}, s \models E\varphi$ iff there is a path π from s such that $\mathcal{M}, \pi \models \varphi$
- $\mathcal{M}, s \models A\varphi$ iff for every path π from s such that $\mathcal{M}, \pi \models \varphi$

- $\mathcal{M}, \pi \models f$ iff $\mathcal{M}, s \models f$ where $\pi = s\pi^1$
- $\mathcal{M}, \pi \models \neg\varphi$ iff $\mathcal{M}, \pi \not\models \varphi$
- $\mathcal{M}, \pi \models \varphi \vee \psi$ iff $\mathcal{M}, \pi \models \varphi$ or $\mathcal{M}, \pi \models \psi$
- $\mathcal{M}, \pi \models G\varphi$ iff for every i $\mathcal{M}, \pi^i \models \varphi$
- $\mathcal{M}, \pi \models F\varphi$ iff there exists i such that $\mathcal{M}, \pi^i \models \varphi$
- $\mathcal{M}, \pi \models \varphi U \psi$ iff there exists i such that for every $j < i$ $\mathcal{M}, \pi^j \models \varphi$ and $\mathcal{M}, \pi^i \models \psi$
- $\mathcal{M}, \pi \models X\varphi$ iff $\mathcal{M}, \pi^1 \models \varphi$

LTL. Special case of CTL* formulas: A φ, where φ is a path formula with only atomic propositions as state subformulas.
CTL. Special case of CTL* formulas where each temporal operator must immediately be preceeded by a path quantifier.

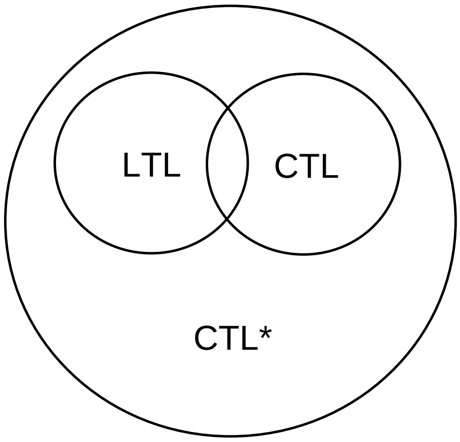
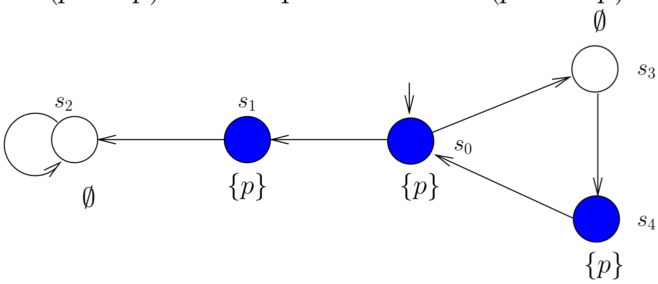


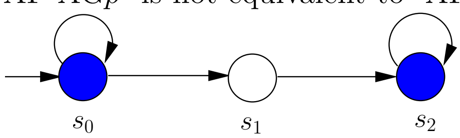
Figure 1: Relative expressiveness of LTL, CTL and CTL*

- AF$(p \wedge \mathrm{X}p)$ is not equivalent to AF$(p \wedge \mathrm{AX}p)$



$s_0 \models \mathrm{AF}(p \wedge \mathrm{X}p)$ but $\underbrace{s_0 \not\models \mathrm{AF}(p \wedge \mathrm{AX}p)}_{\text{path } s_0\, s_1\, (s_2)^\omega \text{ violates it}}$

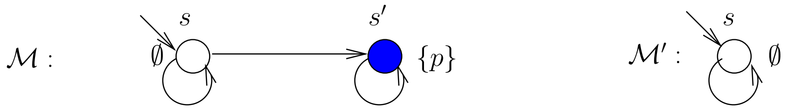
- AF AGp is not equivalent to AF Gp



$s_0 \models \text{AF G}p$ but $\underbrace{s_0 \not\models \text{AF AG } p}_{\text{path } s_0^\omega \text{ violates it}}$

- The CTL-formula AG EF p cannot be expressed in LTL

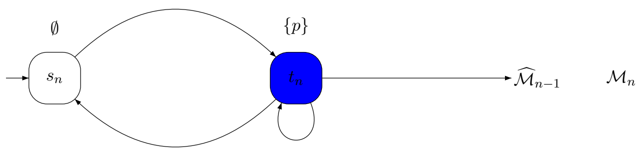
  Proof by contradiction: assume $\varphi \equiv$ AG EFp; let:

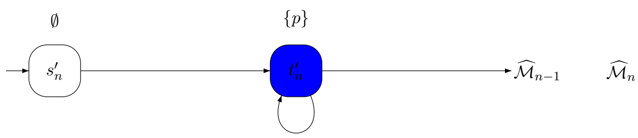


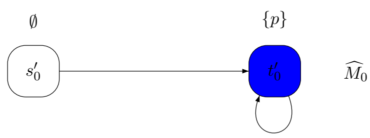
  - $\mathcal{M}, s \models$ AG EFp, and thus—by assumption—$\mathcal{M}, s \models \varphi$
  - Every path in $\mathcal{M}'$ is also a path in $\mathcal{M}$; hence, $\mathcal{M}', s \models \varphi$
  - But $\mathcal{M}', s \not\models$ AG EF p.

- The LTL-formula AFGp cannot be expressed in CTL

  - Provide two series of Kripke structures $\mathcal{M}_n$ and $\widehat{\mathcal{M}}_n$
  - such that $\mathcal{M}_n, s_n \not\models$ AFGp and $\widehat{\mathcal{M}}_n, s_n \models$ AFGp, and
  - for any CTL formula Φ with $|\Phi| \leq n$:
    $\mathcal{M}_n, s_n \models \Phi$ iff $\widehat{\mathcal{M}}_n, s_n \models \Phi$
    (proof is by induction on n; omitted here)







only difference: $\mathcal{M}_n$ includes $t_n \to s_n$, while $\widehat{\mathcal{M}}_n$ does not

Theorem 1 *For every CTL* formula Φ, the following are equivalent:*

1. there is an LTL formula $A\varphi$ that is equivalent to Φ

2. *Φ is equivalent to $A(remove_{E,A}(\Phi))$, where $remove_{E,A}(\Phi)$ is obtained from Φ by deleting all path quantifiers.*

Proof:

$$
\begin{array}{rcl}
\mathcal{M}, s \models \Phi & \Leftrightarrow & \mathcal{M}, s \models \mathrm{A}\varphi \\
& \Leftrightarrow & \forall \text{ paths } \pi \text{ from } s : \pi \models \varphi \\
& \Leftrightarrow & \forall \text{ paths } \pi \text{ from } s : \mathcal{M}_\pi \models \varphi \\
& & \text{where } \mathcal{M}_\pi \text{ is the restriction of } \mathcal{M} \text{ to } \pi \\
& \Leftrightarrow & \forall \text{ paths } \pi \text{ from } s : \mathcal{M}_\pi, s \models \mathrm{A}\varphi \\
& \Leftrightarrow & \forall \text{ paths } \pi \text{ from } s : \mathcal{M}_\pi, s \models \Phi \\
& \Leftrightarrow & \forall \text{ paths } \pi \text{ from } s : \mathcal{M}_\pi, s \models A(\text{remove}_{\mathrm{E,A}}(\Phi)) \\
& & \text{(because there is only a single path)} \\
& \Leftrightarrow & \forall \text{ paths } \pi \text{ from } s : \pi \models \text{remove}_{\mathrm{E,A}}(\Phi) \\
& \Leftrightarrow & \mathcal{M}, s \models \mathrm{A}(\text{remove}_{\mathrm{E,A}}(\Phi))
\end{array}
$$

■

22 The Modal μ-calculus

Syntax: given a set of atomic propositions AP, the set of formulas is defined inductively as follows (where φ and ψ are formulas)

- $\bot, \top$
- $p, \neg p$ for every $p \in AP$
- $\varphi \wedge \psi$, $\varphi \vee \psi$
- $\Box\varphi$, $\Diamond\varphi$ *(Note: the meaning of $\Box$ and $\Diamond$ used here are different from the Box and Diamond operators of LTL.)*
- $\mu p\ \varphi$, $\nu p\ \varphi$, where $p \in AP$ and p only occurs positively in φ.

Note: negation only allowed for atomic propositions. However arbitrary negation can be expressed as follows:

- $\varphi \vee \psi \equiv \neg(\neg\varphi \wedge \neg\psi)$
- $\Diamond\varphi \equiv \neg\Box\neg\psi$
- $\mu p\ \varphi \equiv \neg\nu p \neg\psi[p/\neg p]$

Normal form: every $p \in AP$ is quantified at most once and all occurrances of p are in the scope of the quantifier. Let φ_p be the unique subformula starting with this quantifier.

Semantics: Formulas are interpreted as sets of states.

- $\|\bot\|_{\mathcal{M}} = \emptyset$
- $\|\top\|_{\mathcal{M}} = S$
- $\|p\|_{\mathcal{M}} = \{s|p \in L(s)\}$
- $\|\neg p\|_{\mathcal{M}} = \{s|p \notin L(s)\}$
- $\|\varphi \vee \psi\|_{\mathcal{M}} = \|\varphi\|_{\mathcal{M}} \cup \|\psi\|_{\mathcal{M}}$, $\|\varphi \wedge \psi\|_{\mathcal{M}} = \|\varphi\|_{\mathcal{M}} \cap \|\psi\|_{\mathcal{M}}$
- $\|\Box\varphi\|_{\mathcal{M}} = \{s|\forall t.(s,t) \in R \rightarrow t \in \|\varphi\|_{\mathcal{M}}\}$
- $\|\Diamond\varphi\|_{\mathcal{M}} = \{s|\exists t.(s,t) \in R \wedge t \in \|\varphi\|_{\mathcal{M}}\}$
- $\|\mu p.\varphi\|_{\mathcal{M}} = \bigcap\{S' \subseteq S \mid \|\psi\|_{\mathcal{M}[p\mapsto S]} \subseteq S'\}$
- $\|\nu p.\varphi\|_{\mathcal{M}} = \bigcup\{S' \subseteq S \mid \|\psi\|_{\mathcal{M}[p\mapsto S]} \supseteq S'\}$

where $\mathcal{M}[p \mapsto S'] = (S, R, L[p \mapsto S'])$, $L[p \mapsto S'](n) = \begin{cases} L(n) \cup \{p\} & \text{if } n \in S' \\ L(n) \setminus \{p\} & \text{if } p \notin S' \end{cases}$

Direct evaluation algorithm:
$eval(\varphi, \mathcal{M})$:

- if $\varphi = \bot$ then return $\emptyset$
- ...
- if $\varphi = \mu p.\varphi'$ then
  - $S' = \emptyset$
  - repeat
    - $S'_{old} = S'$
    - $S' = eval(\varphi', \mathcal{M}[p \mapsto S'])$
  - until $S'_{old} = S'$
  - return S'
- if $\varphi = \nu p.\varphi'$ then
  - $S' = S$
  - repeat
    - $S'_{old} = S'$
    - $S' = eval(\varphi', \mathcal{M}[p \mapsto S'])$
  - until $S'_{old} = S'$
  - return S'

Examples:

- $\mu q.(p \vee \Diamond q)$ contains every state s such that there is a path from s to a state where p holds
- Attractor set (Let p_0 be an atomic propositions such that $p_0 \in L(n)$ iff $n \in V_0$.):

$$\mu p'(p \vee ((p_0 \wedge \Diamond p') \vee (\neg p_0 \wedge \Box p')))$$

- Translating CTL:
  - $p' = p$
  - $(f \wedge g)' = f' \wedge g'$
  - $(EXf)' = \Diamond f'$
  - $(E(fUg))' = \mu q.(g' \vee (f' \wedge \Diamond q))$
  - $(EGf)' = \nu q.(f' \wedge \Diamond Q)$