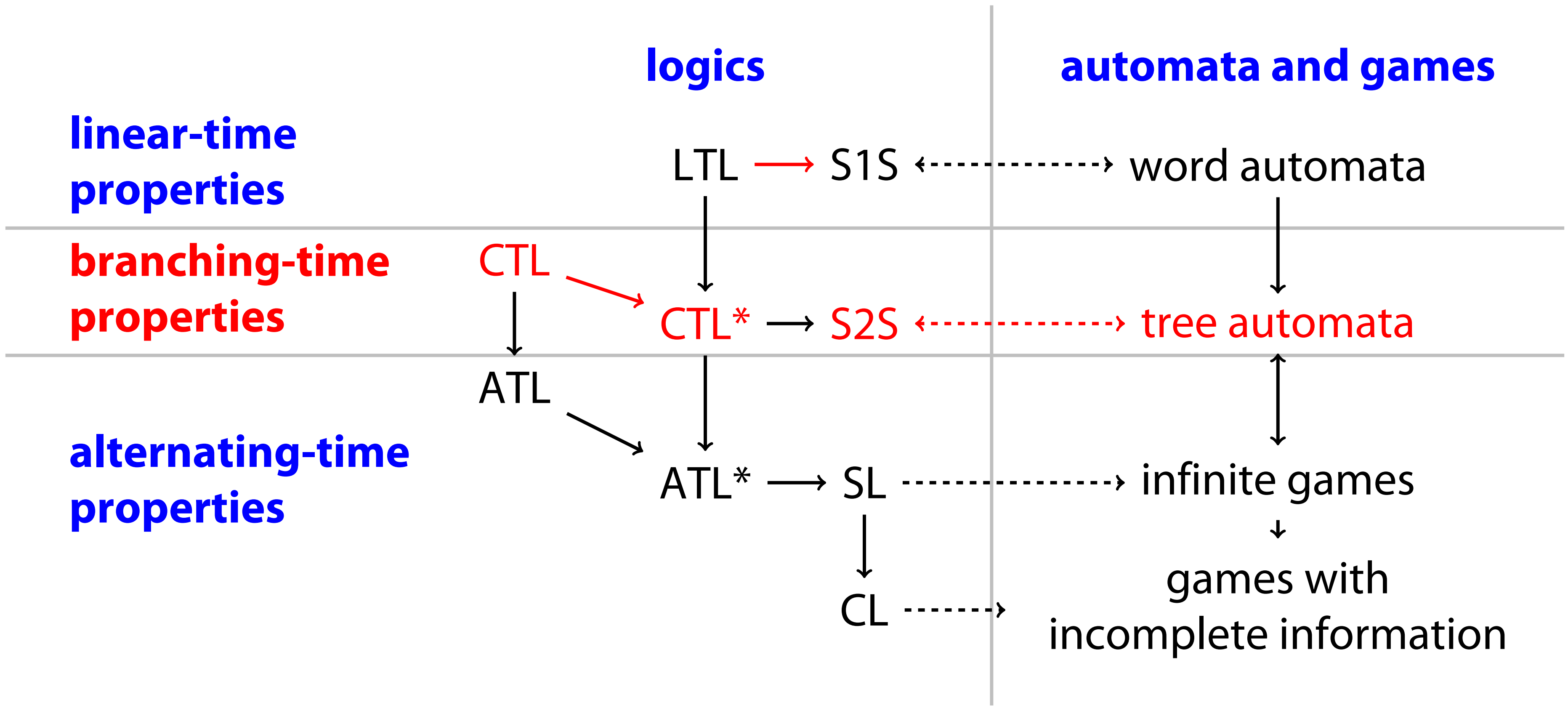
Automata, Games & Verification

#14


logics
automata and games
linear-time properties
LTL
S1S
word automata
branching-time properties
CTL
CTL*
S2S
tree automata
ATL
alternating-time properties
ATL*
SL
infinite games
CL
games with incomplete information

Monadic Second-Order Theory of Two Successors (S2S)

Syntax:

- first-order variable set $V_1 = \{x_0, x_1, \ldots\}$
- second-order variable set $V_2 = \{X_0, X_1, \ldots\}$
- Terms: $t ::= \varepsilon \mid x \mid t0 \mid t1$
- Formulas $\varphi ::= t \in X \mid t_1 = t_2 \mid \neg\varphi \mid \varphi_0 \vee \varphi_1 \mid \exists x.\varphi \mid \exists X.\varphi$

Semantics:

- first-order valuation $\sigma_1 : V_1 \to \mathbb{B}^*$
- second-order valuation $\sigma_2 : V_2 \to 2^{\mathbb{B}^*}$
- terms: $[\![\varepsilon]\!] = \varepsilon$, $[\![t0]\!]_{\sigma_1} = [\![t]\!]_{\sigma_1}0$, etc.
- formulas: $\sigma_1, \sigma_2 \models \exists x_i.\varphi$ iff there is a $a \in \mathbb{B}^*$ s.t.

$$\sigma_1'(y) = \begin{cases} \sigma_1(y) & \text{if } x \neq y, \\ a & \text{otherwise;} \end{cases} \qquad \text{and } \sigma_1', \sigma_2 \models \varphi$$

etc.

Theorem 1. *For each Muller tree automaton* $\mathcal{A} = (S, s_0, M, \mathcal{F})$ *over* $\Sigma = 2^{V_2}$ *there is a S2S formula* φ *over* V_2 *s.t.* $t \in \mathcal{L}(\mathcal{A})$ *iff* $\sigma_2 \vDash \varphi$ *where* $\sigma_2(P) = \{q \in \{0,1\}^* \mid P \in t(q)\}$.

Theorem 2. *For every S2S formula* φ *over* V_1, V_2 *there is a Muller tree automaton* $\mathcal{A}$ *over* $\Sigma = 2^{V_1 \cup V_2}$ *such that* $t \in \mathcal{L}(\mathcal{A})$ *iff* $\sigma_1, \sigma_2 \vDash \varphi$ *where*

$$\begin{aligned} \sigma_1(x) &= q \text{ iff } x \in t(q); \\ \sigma_2(X) &= \{q \in \{0,1\}^* \mid X \in t(q)\}. \end{aligned}$$

Definition 1. *A transition system* $(AP, S, s_0, \rightarrow, L)$ *consists of*

- AP: *atomic propositions*
- S: *finite set of states*
- $s_0 \in S$: *initial state*
- $\rightarrow \subseteq S \times S$: *transition relation*
- $L : S \rightarrow 2^{AP}$: *labeling function*

Computation tree logic (CTL)

- CTL state formulas.

  -- $a \in AP$ atomic proposition
  -- $\neg\Phi$ and $\Phi \wedge \Psi$ negation and conjunction
  -- E φ there *exists* a path fulfilling φ
  -- A φ *all* paths fulfill φ

- CTL path formulas.

  -- X Φ the next state fulfills Φ
  -- $\Phi \,\mathcal{U}\, \Psi$ Φ holds until a Ψ-state is reached

Semantics

CTL state formulas. Semantics 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	$(s \models \Phi) \wedge (s \models \Psi)$
$s \models \mathsf{E}\,\varphi$	iff	$\pi \models \varphi$ for some path π that starts in s
$s \models \mathsf{A}\,\varphi$	iff	$\pi \models \varphi$ for all paths π that start in s

CTL path formulas. Semantics defined by a relation $\models$ such that $\pi \models \varphi$ if and only if path π satisfies φ.

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

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

Satisfaction of a CTL formula over a transition system: $\mathcal{T} \models \Phi$ iff $s_0 \models \Phi$.

CTL*

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):

- $\mathcal{M}, s \vDash p$ iff $p \in L(s)$ for $p \in AP$
- $\mathcal{M}, s \vDash \neg f$ iff $\mathcal{M}, s \nvDash f$
- $\mathcal{M}, s \vDash \mathrm{E}\varphi$ iff there is a path π from s such that $\mathcal{M}, \pi \vDash \varphi$
- $\mathcal{M}, s \vDash \mathrm{A}\varphi$ iff for every path π from s such that $\mathcal{M}, \pi \vDash \varphi$

- $\mathcal{M}, \pi \vDash f$ iff $\mathcal{M}, s \vDash f$ where $\pi = s\pi^1$
- $\mathcal{M}, \pi \vDash \neg\varphi$ iff $\mathcal{M}, \pi \nvDash \varphi$
- $\mathcal{M}, \pi \vDash \varphi \vee \psi$ iff $\mathcal{M}, \pi \vDash \varphi$ or $\mathcal{M}, \pi \vDash \psi$
- $\mathcal{M}, \pi \vDash \varphi \,\mathcal{U}\, \psi$ iff there exists i such that for every $j < i$
  $\mathcal{M}, \pi^j \vDash \varphi$ and $\mathcal{M}, \pi^i \vDash \psi$
- $\mathcal{M}, \pi \vDash \mathrm{X}\varphi$ iff $\mathcal{M}, \pi^1 \vDash \varphi$

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.