Temporal Logics and Model Checking

Francesco Goretti

Alma Mater Studiorum - University of Bologna
Presentation for the course of Logic Methods for Philosophy

26/04/2023

Temporal logics

- Michele has always driven
- Michele drove
- Michele had driven
- Michele will drive
- Michele will always drive

Temporal logics - Syntax

Let $\phi := \{p_0, p_1, p_2, \ldots\}$ be the set of atomic predicates.

The set of temporal formulas F_m^ϕ is defined as follows:

- $p_i \in \phi$ implies $p_i \in F_m^\phi$
- $\perp \in F_m^\phi$
- $A \in F_m^\phi$ implies $\neg A \in F_m^\phi$
- $A, B \in F_m^\phi$ implies $(A \wedge B), (A \vee B), (A \rightarrow B) \in F_m^\phi$
- $A \in F_m^\phi$ implies $\mathrm{H}A, \mathrm{G}A, \mathrm{P}A, \mathrm{F}A \in F_m^\phi$
- F_m^ϕ doesn't contain anything else

Temporal logics - Temporal operators

H: "It was always the case that"

G: "It will be always the case that"

P: "It was the case that"

F: "It will be the case that"

$$\mathrm{H}, \mathrm{G} \quad \sim \quad \Box$$

$$\mathrm{P}, \mathrm{F} \quad \sim \quad \Diamond$$

Duality:

$$\neg \mathrm{H} \neg A = \mathrm{P} A$$
$$\neg \mathrm{G} \neg A = \mathrm{F} A$$

Temporal logics - Examples

$$p := \text{"Michele drives"}$$

- Michele has always driven $\mathrm{H}p$
- Michele drove $\mathrm{P}p$
- Michele had driven $\mathrm{PP}p$
- Michele will drive $\mathrm{F}p$
- Michele will always drive $\mathrm{G}p$

Temporal logics - Semantics

A temporal model M is defined as follows:

$$\mathrm{M} := < \mathrm{T}, \lessdot, \mathrm{I} >$$

where

- $\mathrm{T} := \{t_0, t_1, t_2, ...\}$ non-empty set of instants
- $\lessdot \subseteq \mathrm{T} \times \mathrm{T}$ relation of temporal precedence
- $\mathrm{I} : \phi \rightarrow \mathcal{P}(\mathrm{T})$ valuation function

A temporal frame F is defined as follows:

$$\mathrm{F} := < \mathrm{T}, \lessdot >$$

Temporal Logics - Truth value of a formula

Truth value of a formula A in an instant $t \in \mathrm{T}$ of a model M:

- $\models_t p_i$ iff $t \in \mathrm{I}(p_i)$
- $\not\models_t \bot$
- $\models_t \neg B$ iff $\not\models_t B$
- $\models_t B \wedge C$ iff $\models_t B$ and $\models_t C$
- $\models_t B \vee C$ iff $\models_t B$ or $\models_t C$
- $\models_t B \rightarrow C$ iff $\not\models_t B$ or $\models_t C$

- $\models_t \mathrm{H}B$ iff $\forall t' \in \mathrm{T}(t' < t$ implies $\models_{t'} B)$
- $\models_t \mathrm{G}B$ iff $\forall t' \in \mathrm{T}(t < t'$ implies $\models_{t'} B)$
- $\models_t \mathrm{P}B$ iff $\exists t' \in \mathrm{T}(t' < t$ and $\models_{t'} B)$
- $\models_t \mathrm{F}B$ iff $\exists t' \in \mathrm{T}(t < t'$ and $\models_{t'} B)$

$\mathrm{K_t}$ logic

It's a set of formulas Γ such that:

- $\mathrm{TAUT} \in \Gamma$
- $\mathrm{H}(A \to B) \to (\mathrm{H}A \to \mathrm{H}B) \in \Gamma$
- $\mathrm{G}(A \to B) \to (\mathrm{G}A \to \mathrm{G}B) \in \Gamma$
- $A \to \mathrm{HF}A \in \Gamma$
- $A \to \mathrm{GP}A \in \Gamma$
- $\frac{A \to B \in \Gamma \qquad A \in \Gamma}{B \in \Gamma}$ (modus ponens)
- $\frac{A \in \Gamma}{HA \in \Gamma} \qquad \frac{A \in \Gamma}{GA \in \Gamma}$ (necessitation)

$\mathsf{K4_t}$ logic

$$\mathsf{K4_t} = \mathsf{K_t} + \text{"}\mathrm{H}A \to \mathrm{HH}A\text{"}$$

(transitivity)

if $t<t'$ and $t'<t''$ then $t<t''$

Linear past and future

In $\mathrm{K4_t}$, past and future are branched.

To have a linear past the following clause is added to the definition of Γ:

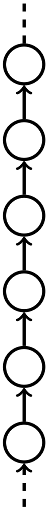
$$\mathrm{FP}A \to \mathrm{P}A \vee A \vee \mathrm{F}A \in \Gamma$$

which corresponds to trichotomy:

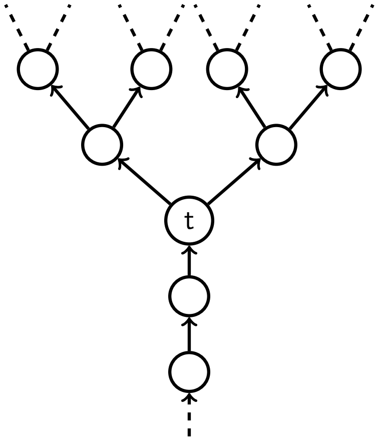
$$t{<}t'' \text{ and } t'{<}t'' \text{ implies } t{<}t' \text{ or } t = t' \text{ or } t'{<}t$$

Instead, to have a linear future the following clause is added:

$$\mathrm{PF}A \to \mathrm{P}A \vee A \vee \mathrm{F}A \in \Gamma$$

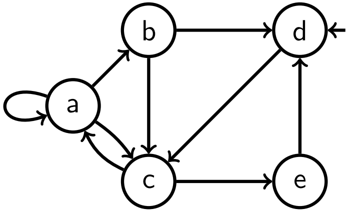


Branched future



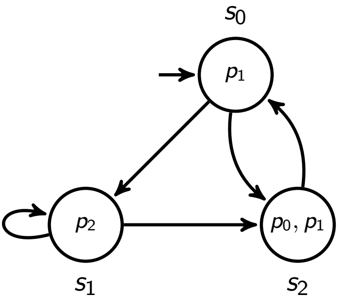
Model Checking

Model checking is an automated method of verification of properties on a finite-state model.



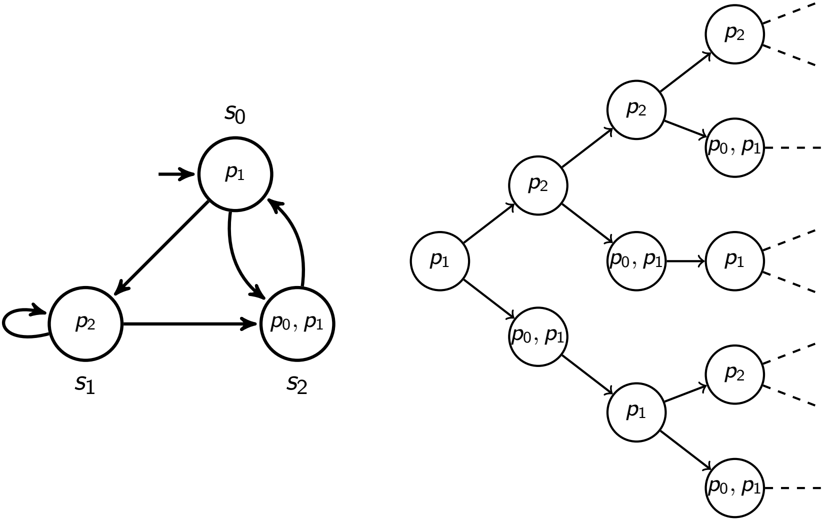
Kripke structure

A Kripke structure is a quadruple $< \mathrm{S}, \mathrm{S}_0, \mathrm{R}, \mathrm{I} >$ where:



- $\mathrm{S} = \{s_0, s_1, s_2\}$ set of states
- $\mathrm{S}_0 = s_0$ initial state
- $\mathrm{R} \subseteq \mathrm{S} \times \mathrm{S}$ transition relation
- $\mathrm{I} : \Phi \rightarrow \mathcal{P}(\mathrm{S})$ interpretation function

Computation tree logic (CTL)



CTL - Syntax

The set of CTL formulas F_m^ϕ is defined as follows:

- It contains every propositional formula
- $B, C \in F_m^\phi$ implies $\mathrm{AX}B, \mathrm{AF}B, \mathrm{AG}B, \mathrm{A}(B\mathrm{U}C) \in F_m^\phi$
- $B, C \in F_m^\phi$ implies $\mathrm{EX}B, \mathrm{EF}B, \mathrm{EG}B, \mathrm{E}(B\mathrm{U}C) \in F_m^\phi$
- F_m^ϕ doesn't contain anything else

Quantifiers:	Operators:
All	ne**X**t
Exists	**F**uture
	Globally
	Until

CTL - Examples of formulas

$B \wedge C$

$\mathrm{AG}(B \wedge C)$

$\mathrm{EX}\ B$

$\mathrm{AG}\ \mathrm{EF}\ B$

$B \vee \mathrm{AG}(C \wedge \mathrm{E}(\mathrm{BUD}))$

$\cancel{\mathrm{E}}$

$\cancel{\mathrm{F}}$

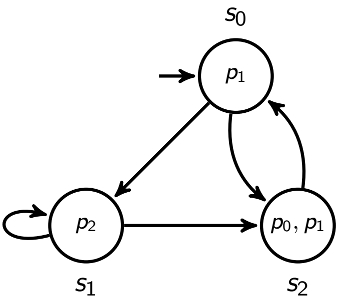
$\cancel{\mathrm{A}\ B}$

$\cancel{\mathrm{AE}\ B}$

$\cancel{\mathrm{A}\ (B \to C)\mathrm{X}}$

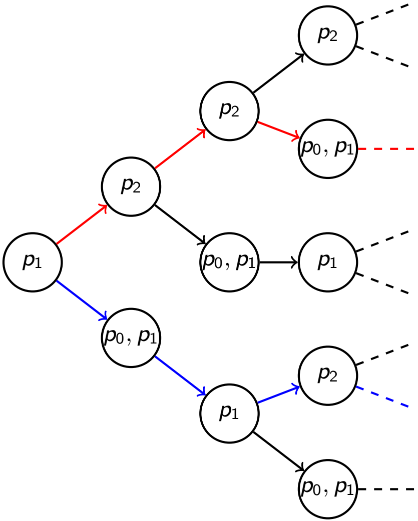
Path

A path is a non-empty sequence of states such that there always exists a transitions between them.



$$s_0 \to s_1 \to s_1 \to s_2 \to s_0 \to \dots$$

Path



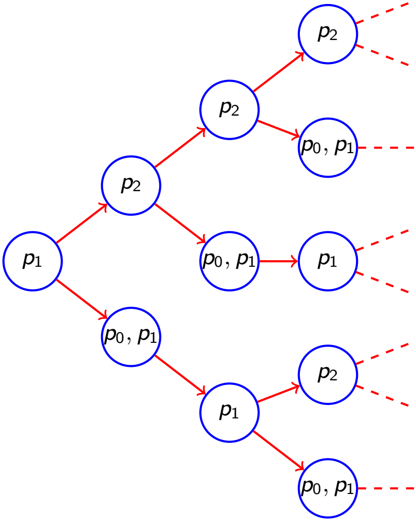
CTL - Semantics

Truth value of a CTL formula in a state $s_0 \in \mathrm{S}$ of a Kripke structure (temporal cases):

- $\models_{s_0} \mathrm{AX}B$ iff $\forall s_0 \to s_1 (\models_{s_1} B)$
- $\models_{s_0} \mathrm{EX}B$ iff $\exists s_0 \to s_1 (\models_{s_1} B)$
- $\models_{s_0} \mathrm{AG}B$ iff $\forall s_0 \to s_1 \to s_2 \to \dots (\forall i (\models_{s_i} B))$
- $\models_{s_0} \mathrm{EG}B$ iff $\exists s_0 \to s_1 \to s_2 \to \dots (\forall i (\models_{s_i} B))$
- $\models_{s_0} \mathrm{AF}B$ iff $\forall s_0 \to s_1 \to s_2 \to \dots (\exists i (\models_{s_i} B))$
- $\models_{s_0} \mathrm{EF}B$ iff $\exists s_0 \to s_1 \to s_2 \to \dots (\exists i (\models_{s_i} B))$
- $\models_{s_0} \mathrm{A}(B \mathrm{U} C)$ iff
  $\forall s_0 \to s_1 \to s_2 \to \dots (\exists i (\models_{s_i} C \text{ and } \forall j < i (\models_{s_j} B)))$
- $\models_{s_0} \mathrm{E}(B \mathrm{U} C)$ iff
  $\exists s_0 \to s_1 \to s_2 \to \dots (\exists i (\models_{s_i} C \text{ and } \forall j < i (\models_{s_j} B)))$

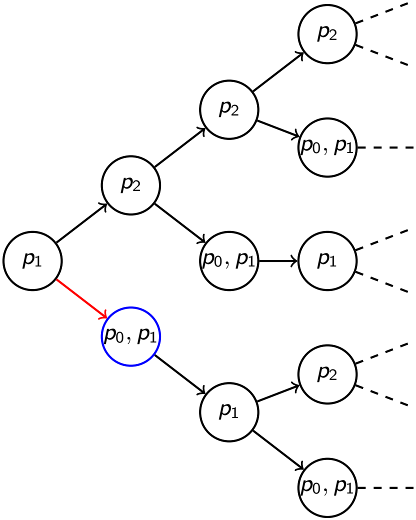
CTL - Examples

$\models_{s_0} \mathrm{AG}(p_1 \vee p_2)$



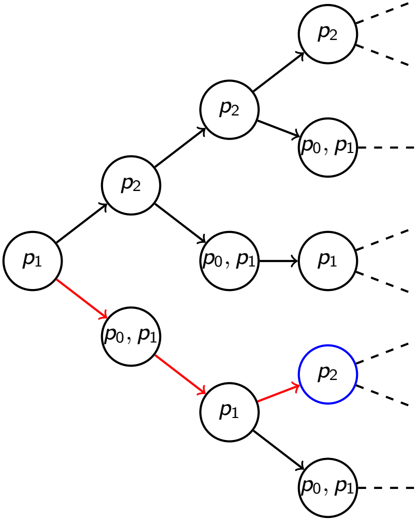
CTL - Examples

$\models_{s_0}$ EX p_0



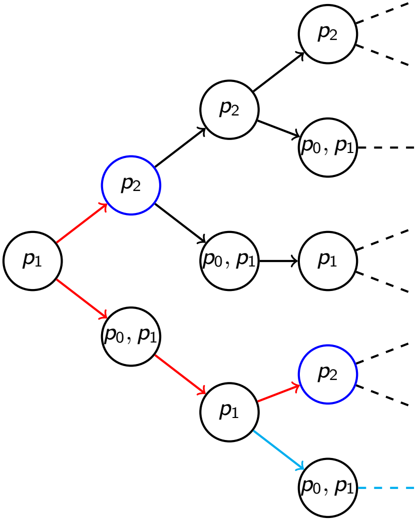
CTL - Examples

$\vDash_{s_0} \mathrm{EF}\ p_2$

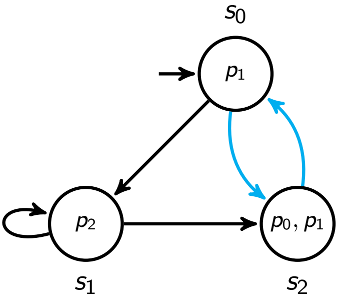


CTL - Examples

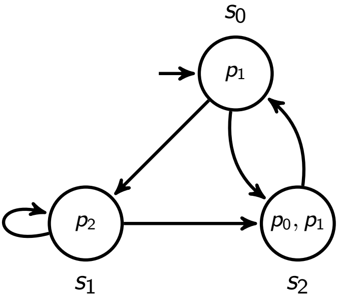
$\not\models_{s_0} \mathrm{A}((p_0 \vee p_1)\mathrm{U}\, p_2)$

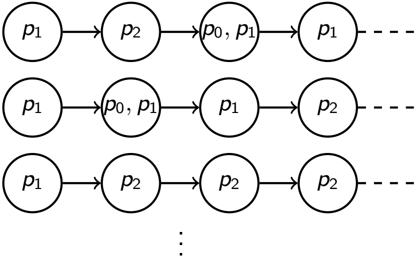


CTL - Examples



Linear temporal logic (LTL)





Conclusions

LTL vs CTL vs CTL* vs μ-calculus