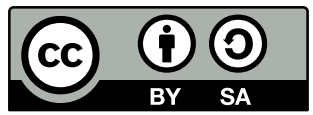
Logiche Temporali e Model Checking

Francesco Goretti

Alma Mater Studiorum - Università di Bologna
Presentazione per il corso di Metodi Logici per la Filosofia

26/04/2023



Logiche temporali

- Michele ha sempre guidato
- Michele guidò
- Michele aveva guidato
- Michele guiderà
- Michele guiderà sempre

Logiche temporali - Sintassi

Sia $\phi := \{p_0, p_1, p_2, ...\}$ l'insieme delle variabili enunciative.

L'insieme delle formule temporali F_m^ϕ è definito come segue:

- $p_i \in \phi$ implica $p_i \in F_m^\phi$
- $\bot \in F_m^\phi$
- $A \in F_m^\phi$ implica $\neg A \in F_m^\phi$
- $A, B \in F_m^\phi$ implica $(A \wedge B), (A \vee B), (A \rightarrow B) \in F_m^\phi$
- $A \in F_m^\phi$ implica $\mathrm{H}A, \mathrm{G}A, \mathrm{P}A, \mathrm{F}A \in F_m^\phi$
- Nient'altro appartiene a F_m^ϕ

Logiche temporali - Operatori temporali

H: "Si è sempre dato il caso che"

G: "Si darà sempre il caso che"

P: "Si è dato il caso che"

F: "Si darà il caso che"

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

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

Dualità:

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

Logiche temporali - Esempi

$p :=$ "Michele guida"

- Michele ha sempre guidato $\mathrm{H}p$
- Michele guidò $\mathrm{P}p$
- Michele aveva guidato $\mathrm{PP}p$
- Michele guiderà $\mathrm{F}p$
- Michele guiderà sempre $\mathrm{G}p$

Logiche temporali - Semantica

Un modello temporale M è definito come segue:

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

dove

- $\mathrm{T} := \{t_0, t_1, t_2, ...\}$ insieme non vuoto di istanti
- $< \subseteq \mathrm{T} \times \mathrm{T}$ relazione di precedenza temporale
- $\mathrm{I} : \phi \rightarrow \mathcal{P}(\mathrm{T})$ funzione di valutazione

Una struttura temporale F è definita come segue:

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

Logiche temporali - Verità di una formula

Verità di una formula A in un istante $t \in \mathrm{T}$ di un modello M:

- $\models_t p_i$ sse $t \in \mathrm{I}(p_i)$
- $\not\models_t \bot$
- $\models_t \neg B$ sse $\not\models_t B$
- $\models_t B \wedge C$ sse $\models_t B$ e $\models_t C$
- $\models_t B \vee C$ sse $\models_t B$ oppure $\models_t C$
- $\models_t B \rightarrow C$ sse $\not\models_t B$ oppure $\models_t C$

- $\models_t \mathrm{H}B$ sse $\forall t' \in \mathrm{T}(t'<t$ implica $\models_{t'} B)$
- $\models_t \mathrm{G}B$ sse $\forall t' \in \mathrm{T}(t<t'$ implica $\models_{t'} B)$
- $\models_t \mathrm{P}B$ sse $\exists t' \in \mathrm{T}(t'<t$ e $\models_{t'} B)$
- $\models_t \mathrm{F}B$ sse $\exists t' \in \mathrm{T}(t<t'$ e $\models_{t'} B)$

Logica K_t

È un insieme di formule Γ tale che:

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

Logica $K4_t$

$$K4_t = K_t + "\mathrm{H}A \rightarrow \mathrm{HH}A"$$

(transitività)

se $t<t'$ e $t'<t''$ allora $t<t''$

Passato e futuro lineare

In $\mathsf{K4_t}$, passato e futuro sono ramificati.

Per avere un passato lineare si aggiunge la seguente clausola alla definizione di Γ:

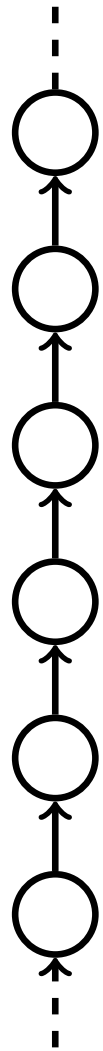
$$\mathrm{FP}A \to \mathrm{P}A \vee A \vee \mathrm{F}A \in \Gamma$$

che corrisponde alla tricotomia:

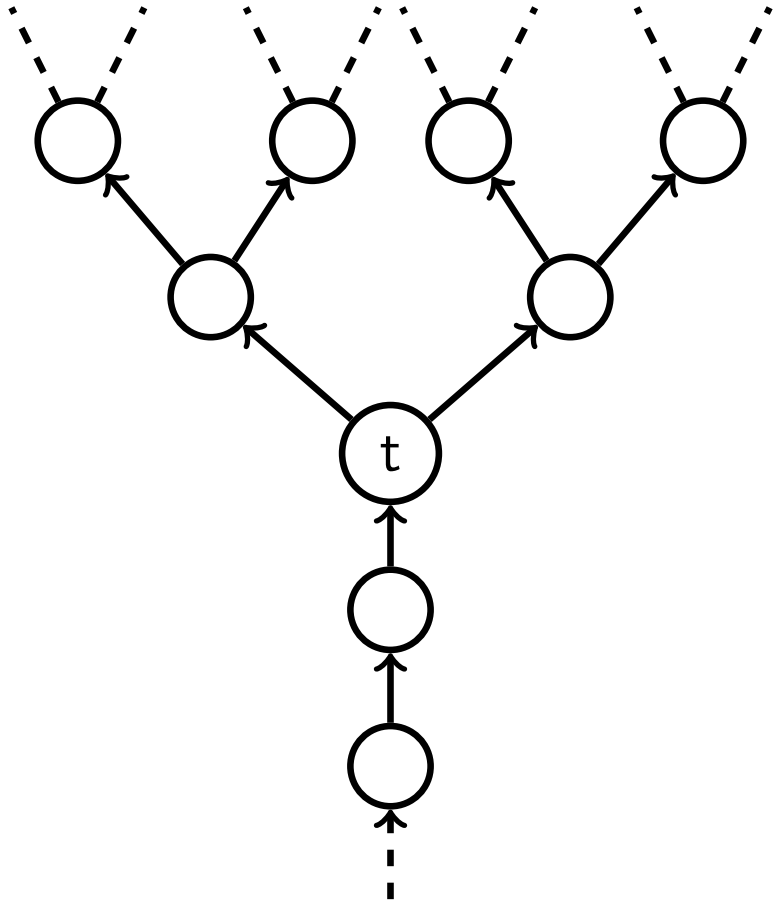
$t<t''$ e $t'<t''$ implica $t<t'$ oppure $t = t'$ oppure $t'<t$

Per avere un futuro lineare, invece, si aggiunge la seguente clausola:

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

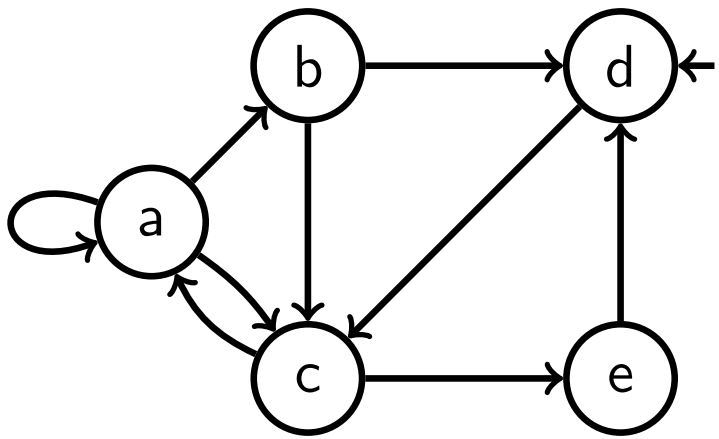


Futuro ramificato



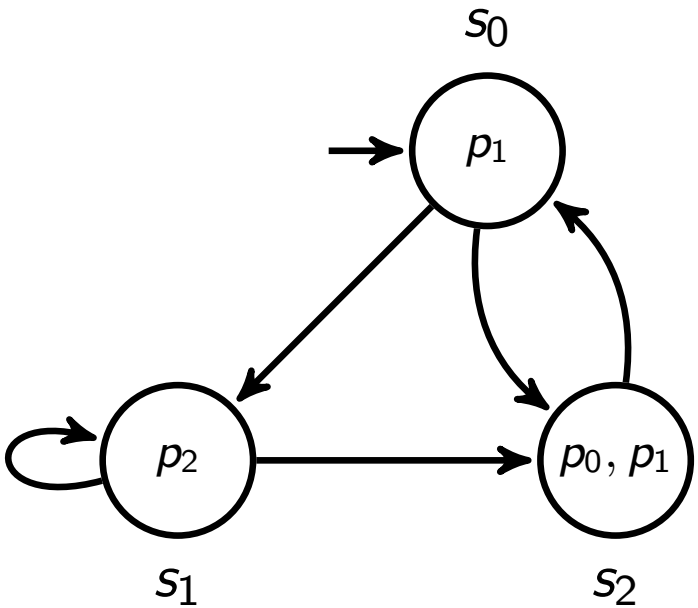
Model Checking

Il model checking è un metodo di verifica automatico di proprietà su un modello a stati finiti.



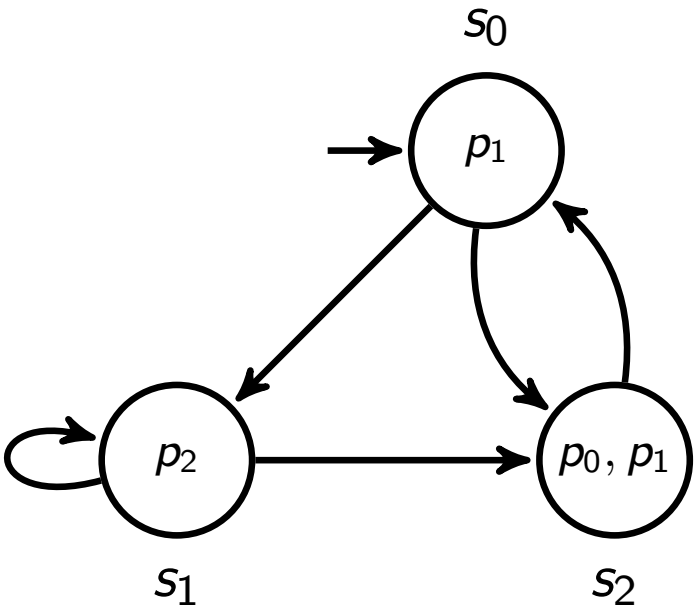
Struttura di Kripke

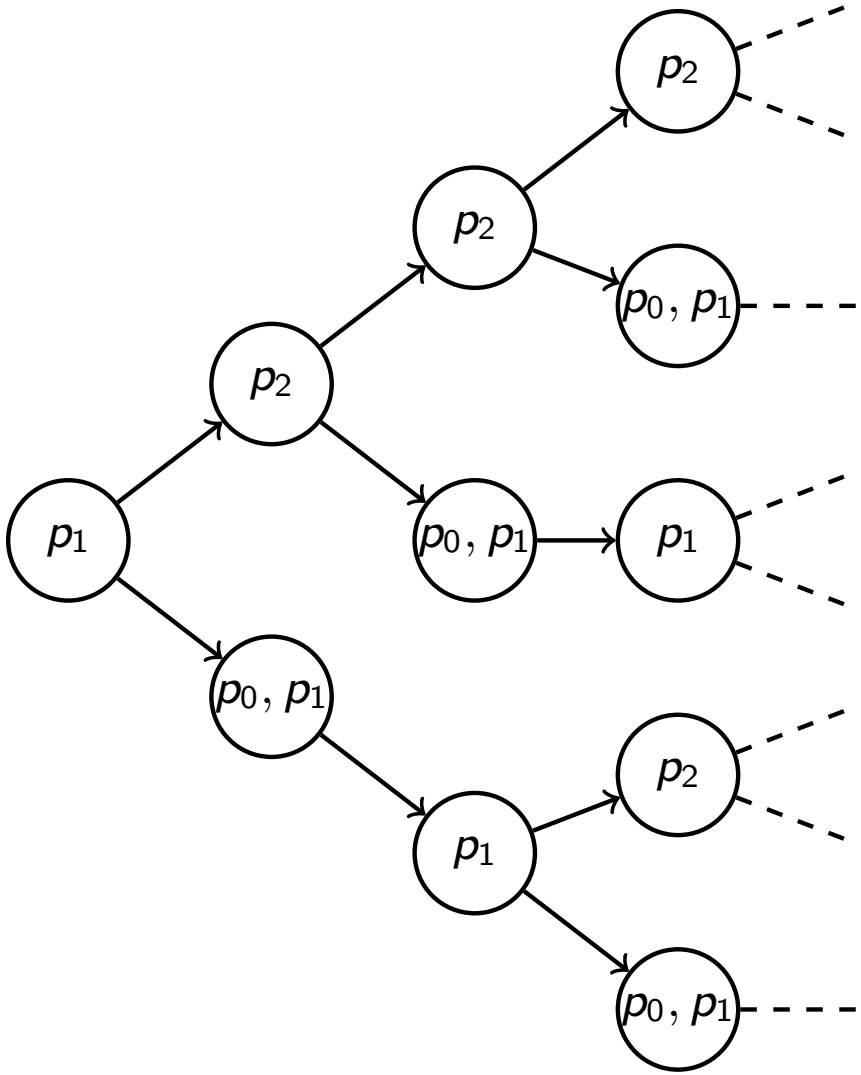
Una struttura di Kripke è una quadrupla $< \mathrm{S}, \mathrm{S}_0, \mathrm{R}, \mathrm{I} >$ dove:



- $\mathrm{S} = \{s_0, s_1, s_2\}$ insieme di stati
- $\mathrm{S}_0 = s_0$ stato iniziale
- $\mathrm{R} \subseteq \mathrm{S} \times \mathrm{S}$ relazione di transizione
- $\mathrm{I} : \Phi \to \mathcal{P}(\mathrm{S})$ funzione di interpretazione

Computation tree logic (CTL)





CTL - Sintassi

L'insieme delle formule di CTL F_m^ϕ è definito come segue:

- Contiene tutte le formule proposizionali
- $B, C \in F_m^\phi$ implica $\mathrm{AX}B, \mathrm{AF}B, \mathrm{AG}B, \mathrm{A}(B\mathrm{U}C) \in F_m^\phi$
- $B, C \in F_m^\phi$ implica $\mathrm{EX}B, \mathrm{EF}B, \mathrm{EG}B, \mathrm{E}(B\mathrm{U}C) \in F_m^\phi$
- Nient'altro appartiene a F_m^ϕ

Quantificatori:

All
Exists

Operatori:

ne**X**t
Future
Globally
Until

CTL - Esempi di formule

$B \wedge C$

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

$\mathrm{EX}\ B$

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

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

~~E~~

~~F~~

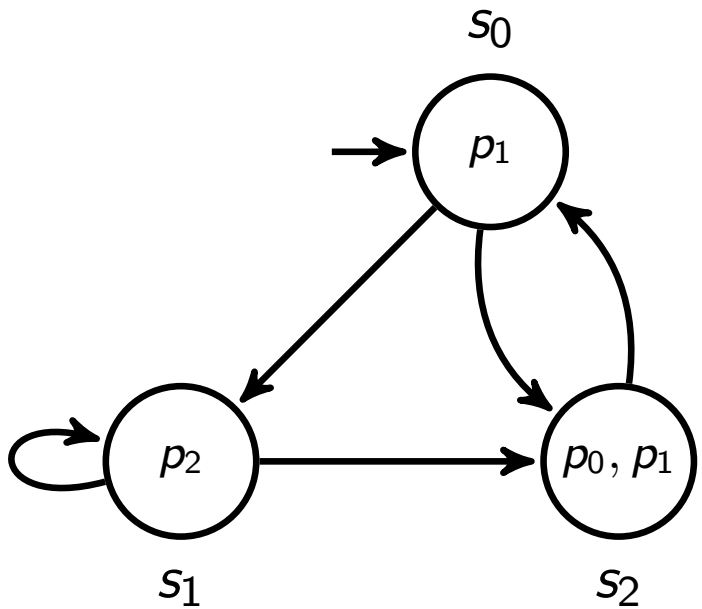
~~$\mathrm{A}\ B$~~

~~$\mathrm{AE}\ B$~~

~~$\mathrm{A}\ (B \rightarrow C)\mathrm{X}$~~

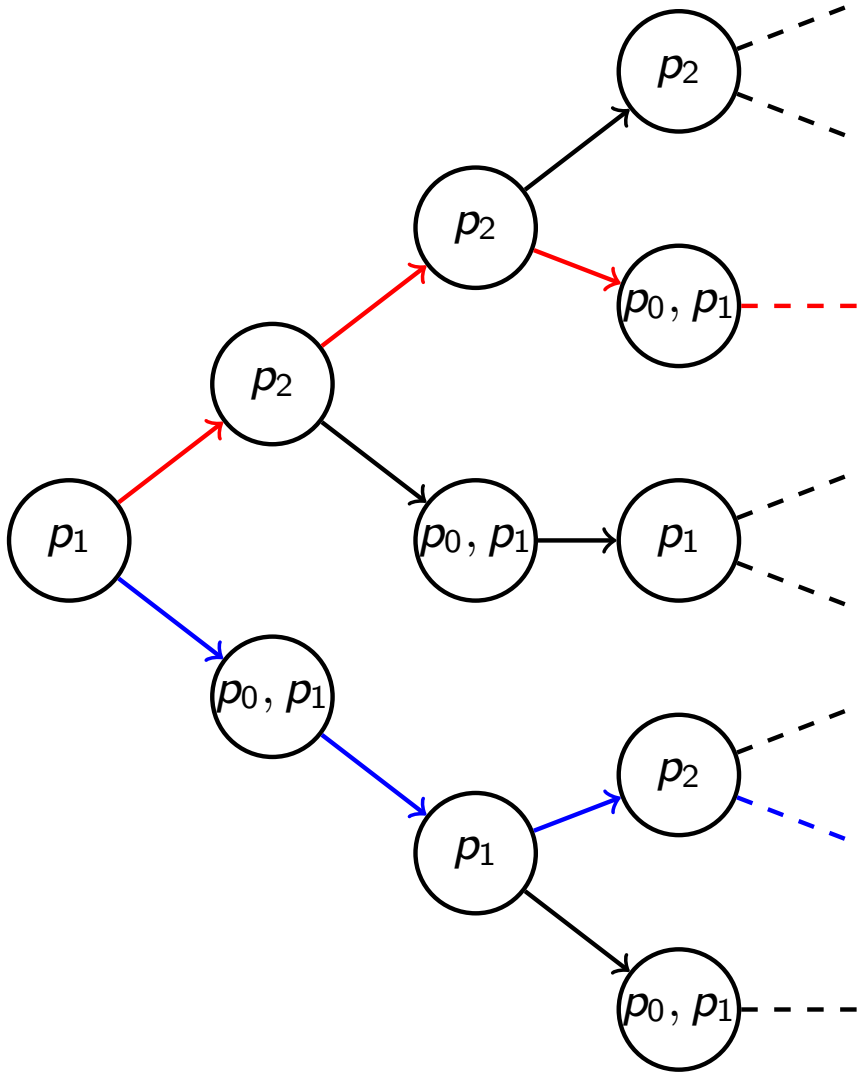
Percorso

Un percorso è una sequenza non vuota di stati tra cui esistono transizioni.



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

Percorso



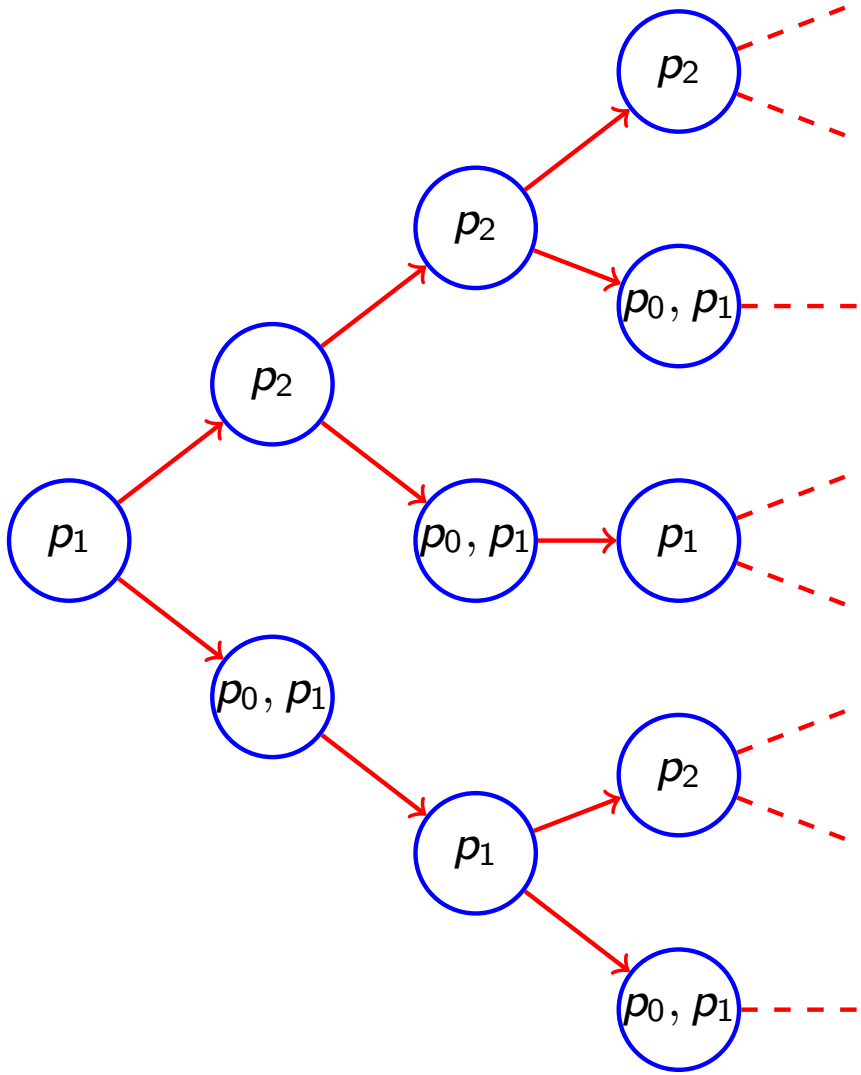
CTL - Semantica

Verità di una formula CTL in uno stato $s_0 \in \mathrm{S}$ di una struttura di Kripke (casi temporali):

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

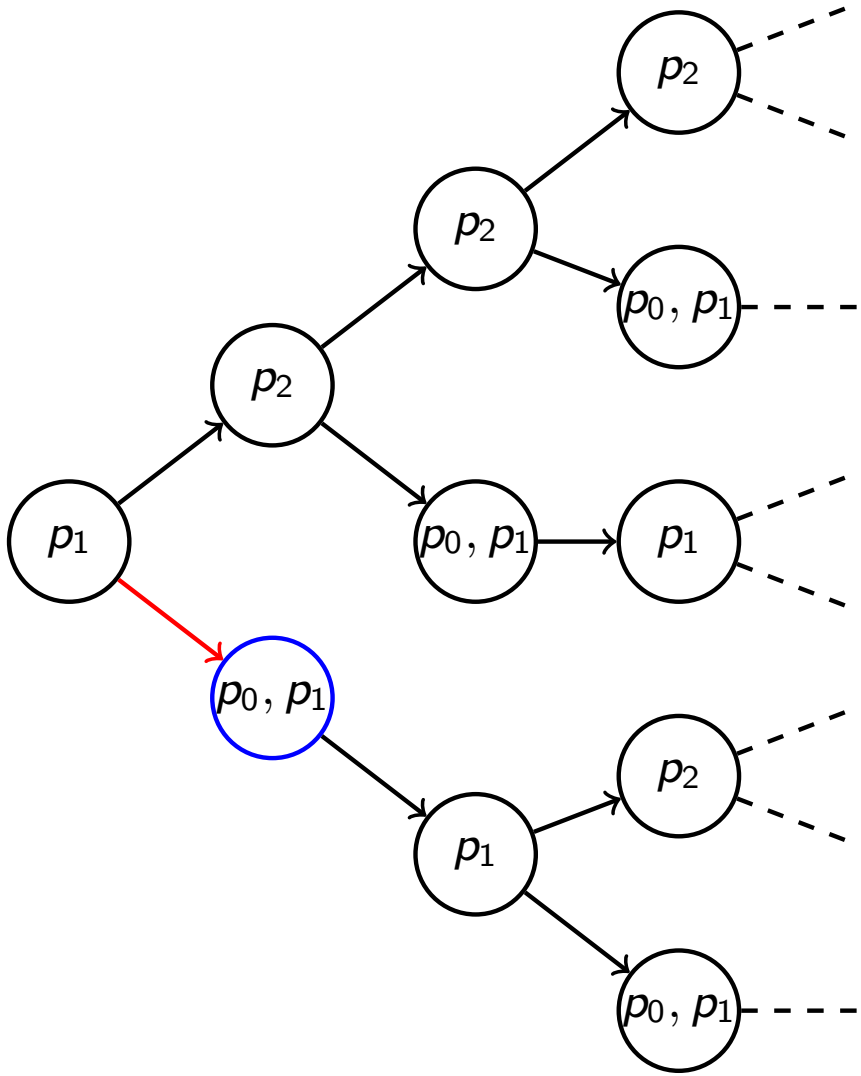
CTL - Esempi

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



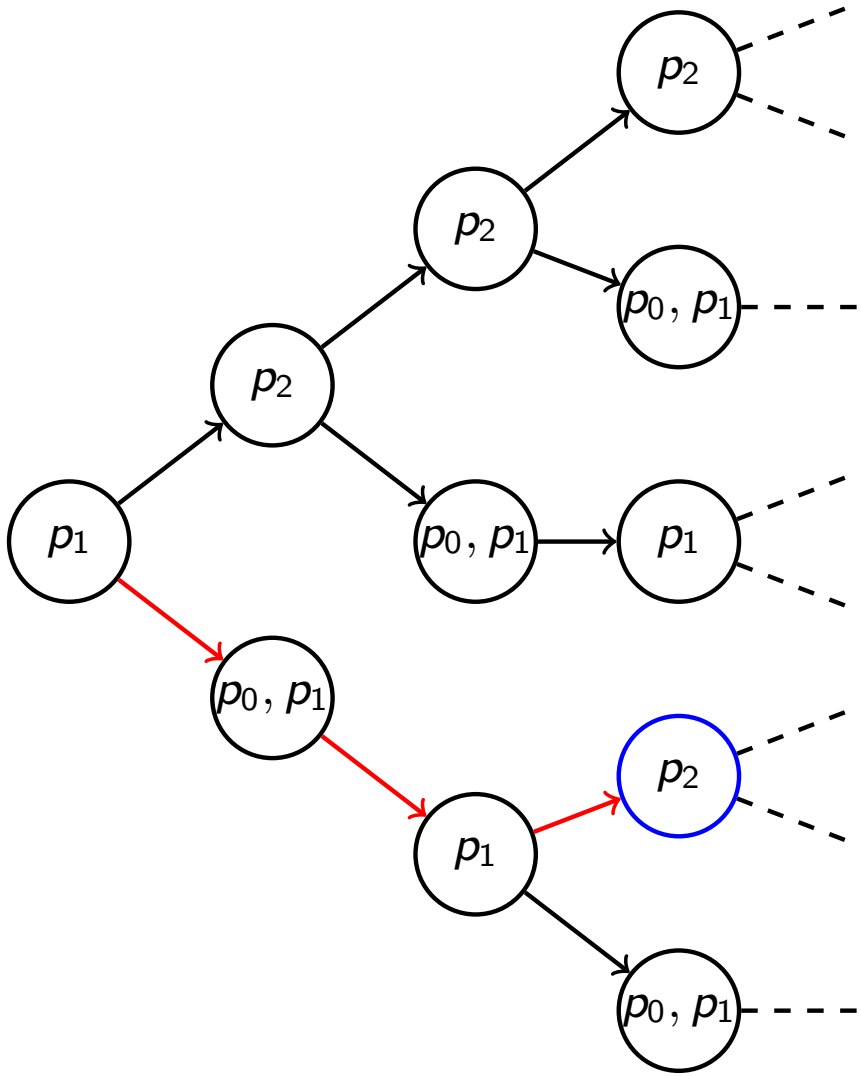
CTL - Esempi

$\models_{s_0} \mathrm{EX}\ p_0$



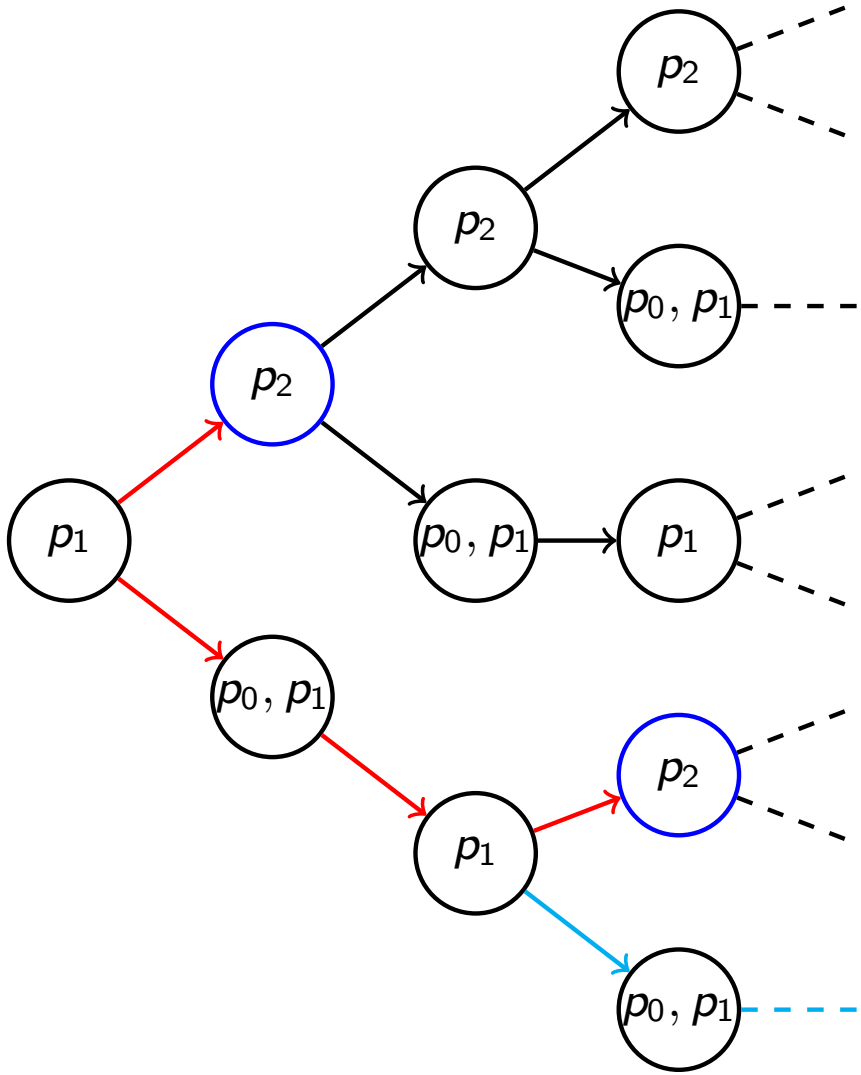
CTL - Esempi

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

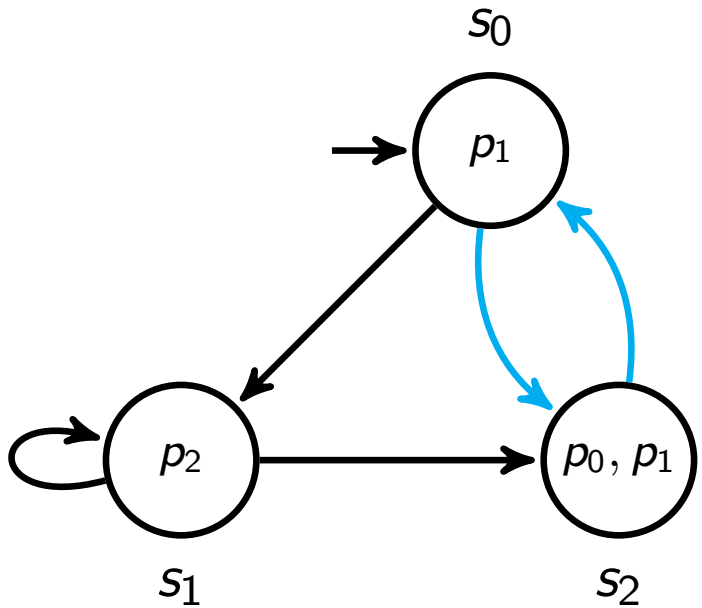


CTL - Esempi

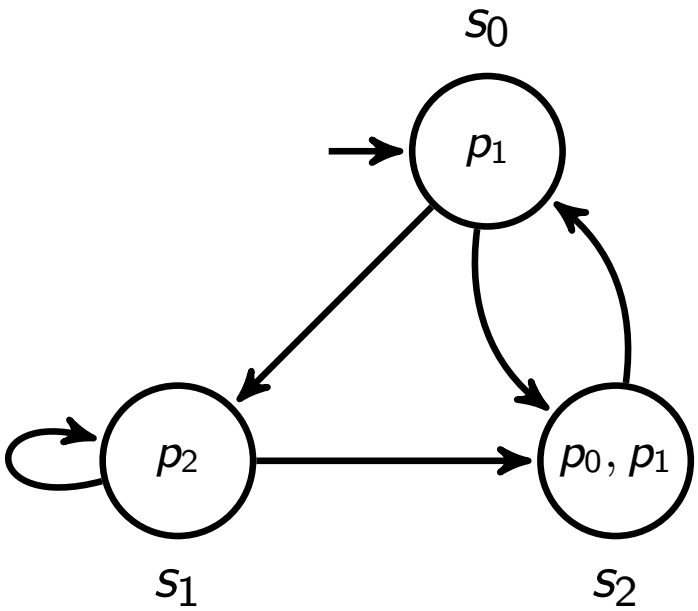
$\not\models_{s_0} \mathrm{A}((p_0 \vee p_1)\mathrm{U}p_2)$

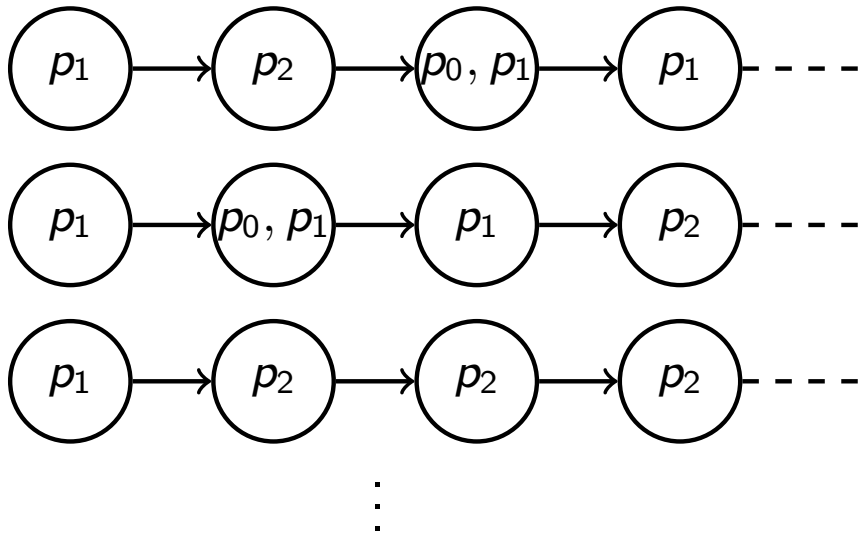


CTL - Esempi



Linear temporal logic (LTL)





Conclusioni

LTL vs CTL vs CTL* vs μ-calcolo