Modeling and Analysis of Hybrid Systems

Propositional and temporal logics

Prof. Dr. Erika Ábrahám

Informatik 2 - Theory of Hybrid Systems
RWTH Aachen University

SS 2011

Propositional logic

- Abstract syntax:

$$\varphi \ ::= \ a \mid (\varphi \wedge \varphi) \mid (\neg\varphi)$$

  with $a \in AP$.
- Syntactic sugar: *true*, *false*, $\vee, \rightarrow, \leftrightarrow, \ldots$
- Omit parentheses when no confusion
- Semantics:

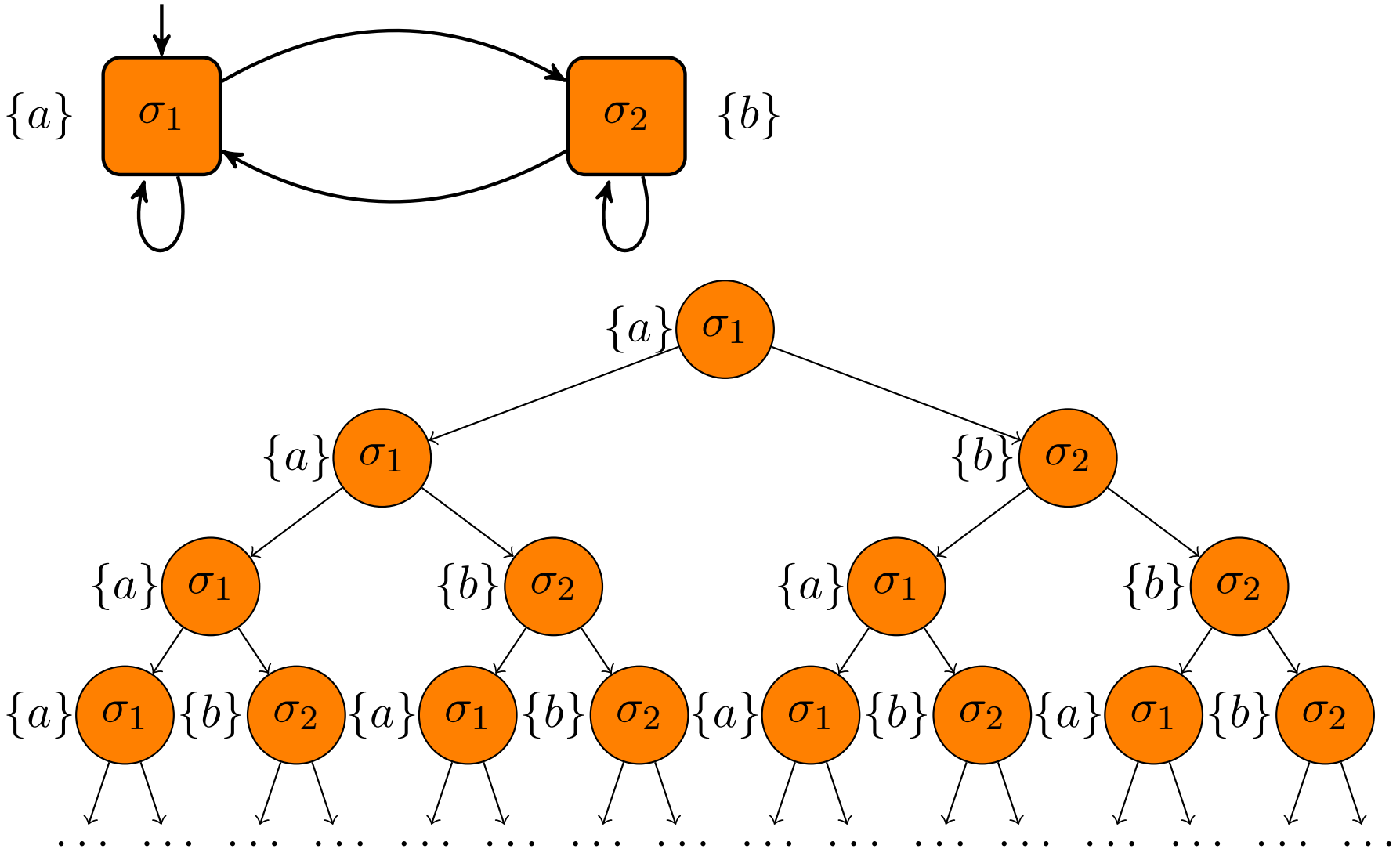
$$\begin{array}{lll} \sigma \models a & \textit{iff} & a \in L(\sigma), \\ \sigma \models (\varphi_1 \wedge \varphi_2) & \textit{iff} & \sigma \models \varphi_1 \textit{ and } \sigma \models \varphi_2, \\ \sigma \models (\neg\varphi) & \textit{iff} & \sigma \not\models \varphi. \end{array}$$

Temporal logics

Assume

- a labeled state transition system $\mathcal{LSTS} = (\Sigma, Lab, Edge, Init)$,
- a set of atomic propositions AP, and
- a labeling function $L : \Sigma \to 2^{AP}$.

Computation tree



LTL syntax

Linear Temporal Logic (LTL) is suited to argue about single (linear) paths in the computation tree.

- Abstract syntax:

$$\varphi \quad ::= \quad a \mid (\varphi \wedge \varphi) \mid (\neg\varphi) \mid (\mathcal{X}\varphi) \mid (\varphi \,\mathcal{U}\, \varphi)$$

  where $a \in AP$.

- Syntactic sugar: $\mathcal{F}$ ("finally" or "eventually"), $\mathcal{G}$ ("globally"), etc.
- We often omit parentheses when no confusion.

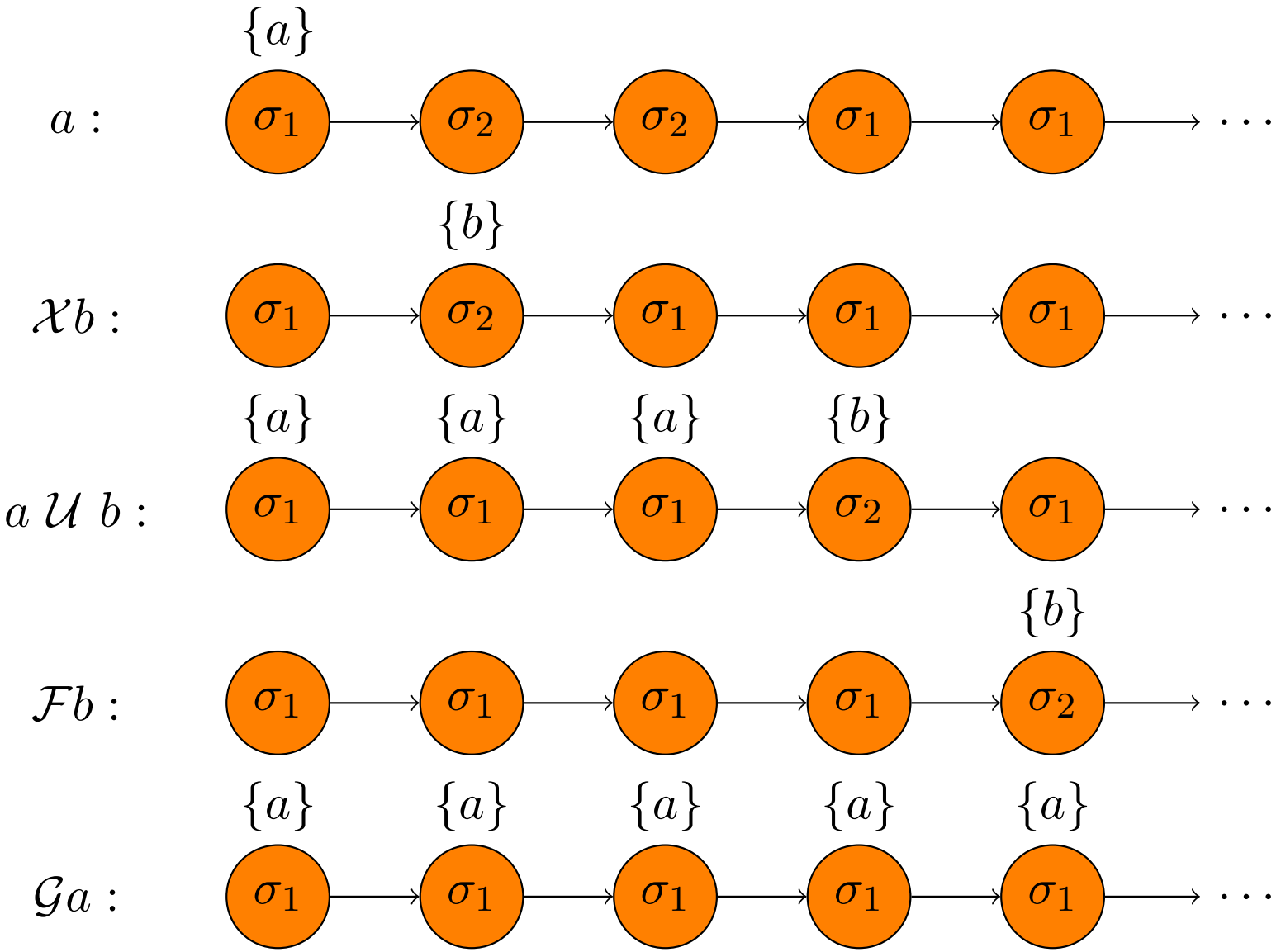
LTL semantics

For a path $\pi = \sigma_0 \to \sigma_1 \to \dots$
let $\pi(i)$ denote σ_i, and
let π^i denote $\sigma_i \to \sigma_{i+1} \to \dots$.

$$
\begin{array}{lll}
\pi \models a & \textit{iff} & a \in L(\pi(0)), \\
\pi \models \varphi_1 \wedge \varphi_2 & \textit{iff} & \pi \models \varphi_1 \textit{ and } \pi \models \varphi_2, \\
\pi \models \neg\varphi & \textit{iff} & \pi \not\models \varphi, \\
\pi \models \mathcal{X}\varphi & \textit{iff} & \pi^1 \models \varphi, \\
\pi \models \varphi_1 \,\mathcal{U}\, \varphi_2 & \textit{iff} & \exists j \geq 0 . \pi^j \models \varphi_2 \wedge \forall 0 \leq i < j . \pi^i \models \varphi_1.
\end{array}
$$

$\mathcal{LSTS} \models \varphi$ iff $\pi \models \varphi$ for all paths π of $\mathcal{LSTS}$.

Example


$\{a\}$
$a:$
σ_1 σ_2 σ_2 σ_1 σ_1 $\cdots$
$\{b\}$
$\mathcal{X}b:$
σ_1 σ_2 σ_1 σ_1 σ_1 $\cdots$
$\{a\}$ $\{a\}$ $\{a\}$ $\{b\}$
$a\ \mathcal{U}\ b:$
σ_1 σ_1 σ_1 σ_2 σ_1 $\cdots$
$\{b\}$
$\mathcal{F}b:$
σ_1 σ_1 σ_1 σ_1 σ_2 $\cdots$
$\{a\}$ $\{a\}$ $\{a\}$ $\{a\}$ $\{a\}$
$\mathcal{G}a:$
σ_1 σ_1 σ_1 σ_1 σ_1 $\cdots$

CTL syntax

CTL state formulae:

$$\psi \quad ::= \quad a \mid (\psi \wedge \psi) \mid (\neg\psi) \mid (\mathbf{E}\varphi) \mid (\mathbf{A}\varphi)$$

with $a \in AP$ and φ are CTL path formulae.

CTL path formulae:

$$\varphi \quad ::= \quad \mathcal{X}\psi \mid \psi \,\mathcal{U}\, \psi$$

where ψ are CTL state formulae.

CTL formulae are CTL state formulae.

We omit parentheses when causing no confusion.

CTL semantics

$$
\begin{array}{lll}
\sigma \models a & \textit{iff} & a \in L(\sigma) \\
\sigma \models \psi_1 \wedge \psi_2 & \textit{iff} & \sigma \models \psi_1 \textit{ and } \sigma \models \psi_2 \\
\sigma \models \neg\psi & \textit{iff} & \sigma \not\models \psi \\
\sigma \models \mathbf{E}\varphi & \textit{iff} & \pi \models \varphi \textit{ for some } \pi = \sigma_0 \to \sigma_1 \to \ldots \textit{ with } \sigma_0 = \sigma \\
\sigma \models \mathbf{A}\varphi & \textit{iff} & \pi \models \varphi \textit{ for all } \pi = \sigma_0 \to \sigma_1 \to \ldots \textit{ with } \sigma_0 = \sigma \\
 & & \\
\pi \models \mathcal{X}\psi & \textit{iff} & \pi(1) \models \psi \\
\pi \models \psi_1 \,\mathcal{U}\, \psi_2 & \textit{iff} & \textit{exists } 0 \leq j \textit{ with } \pi(j) \models \psi_2 \textit{ and} \\
 & & \pi(i) \models \psi_1 \textit{ for all } 0 \leq i < j.
\end{array}
$$

$\mathcal{LSTS} \models \psi$ iff $\sigma_0 \models \psi$ for all initial states σ_0 of $\mathcal{LSTS}$.

CTL* syntax

CTL* state formulae:

$$\psi \quad ::= \quad a \mid (\psi \wedge \psi) \mid (\neg\psi) \mid (\mathbf{E}\varphi)$$

with $a \in AP$ and φ are CTL* path formulae.

CTL* path formulae:

$$\varphi \quad ::= \quad \psi \mid (\varphi \wedge \varphi) \mid (\neg\varphi) \mid (\mathcal{X}\varphi) \mid (\varphi \,\mathcal{U}\, \varphi)$$

where ψ are CTL* state formulae.

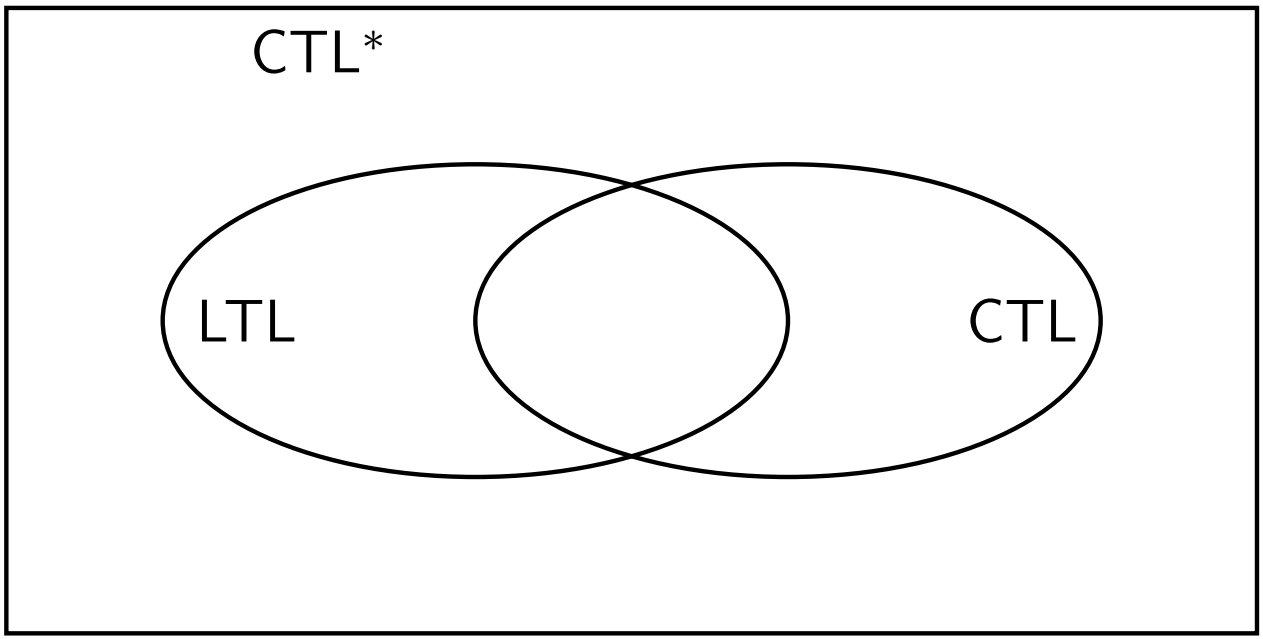
CTL* formulae are CTL* state formulae.
We often omit parentheses.

CTL* semantics

$$
\begin{array}{lll}
\sigma \models a & \textit{iff} & a \in L(\sigma) \\
\sigma \models \psi_1 \wedge \psi_2 & \textit{iff} & \sigma \models \psi_1 \textit{ and } \sigma \models \psi_2 \\
\sigma \models \neg\psi & \textit{iff} & \sigma \not\models \psi \\
\sigma \models \mathbf{E}\varphi & \textit{iff} & \pi \models \varphi \textit{ for some } \pi = \sigma_0 \to \sigma_1 \to \ldots \textit{ with } \sigma_0 = \sigma \\
 & & \\
\pi \models \psi & \textit{iff} & \pi(0) \models \psi \\
\pi \models \varphi_1 \wedge \varphi_2 & \textit{iff} & \pi \models \varphi_1 \textit{ and } \pi \models \varphi_2 \\
\pi \models \neg\varphi & \textit{iff} & \pi \not\models \varphi \\
\pi \models \mathcal{X}\varphi & \textit{iff} & \pi^1 \models \varphi \\
\pi \models \varphi_1 \,\mathcal{U}\, \varphi_2 & \textit{iff} & \textit{exists } 0 \leq j \textit{ with } \pi^j \models \varphi_2 \textit{ and} \\
 & & \pi^i \models \varphi_1 \textit{ for all } 0 \leq i < j.
\end{array}
$$

$\mathcal{LSTS} \models \psi$ iff $\sigma_0 \models \psi$ for all initial states σ_0 of $\mathcal{LSTS}$.

The relation of LTL, CTL, and CTL*



- The LTL formula $\mathcal{F}\mathcal{G}a$ is not expressible in CTL.
- The CTL formula $\mathbf{A}\mathcal{F}\mathbf{A}\mathcal{G}a$ is not expressible in LTL.

CTL model checking

Given a state transition system and a CTL formula ψ, CTL model checking labels the states recursively with the sub-formulae of ψ inside-out.

- The labeling with atomic propositions $a \in AP$ is given by a labeling function.
- Given the labelings for ψ_1 and ψ_2, we label a state with $\psi_1 \wedge \psi_2$ iff the state is labeled with both ψ_1 and ψ_2.
- Given the labeling for ψ, we label a state with $\neg\psi$ iff the state is not labeled with ψ.

CTL model checking

- Given the labeling for ψ, we label a state with $\mathbf{E}\mathcal{X}\psi$ iff there is a successor state labeled with ψ.
- Given the labeling for ψ_1 and ψ_2, we
  - label all with ψ_2 labeled states additionally with $\mathbf{E}\psi_1\ \mathcal{U}\ \psi_2$, and
  - label all states that have the label ψ_1 and have a successor state with the label $\mathbf{E}\psi_1\ \mathcal{U}\ \psi_2$ also with $\mathbf{E}\psi_1\ \mathcal{U}\ \psi_2$ iteratively until a fixed point is reached.
- Given the labeling for ψ, we label a state with $\mathbf{A}\mathcal{X}\psi$ iff all successor states are labeled with ψ.
- Given the labeling for ψ_1 and ψ_2, we
  - label all with ψ_2 labeled states additionally with $\mathbf{A}\psi_1\ \mathcal{U}\ \psi_2$, and
  - label all states that have the label ψ_1 and all of their successor states have the label $\mathbf{A}\psi_1\ \mathcal{U}\ \psi_2$ also with $\mathbf{A}\psi_1\ \mathcal{U}\ \psi_2$ iteratively until a fixed point is reached.

Discrete-time LTL

$$\mathcal{X}^k \varphi =$$

$$\begin{cases} \varphi & \text{if } k = 0 \\ \mathcal{X}\mathcal{X}^{k-1}\varphi & \text{else.} \end{cases}$$

$$\varphi_1 \; \mathcal{U}^{[k_1,k_2]} \; \varphi_2 =$$

$$\begin{cases} \varphi_1 \; \mathcal{U} \; \varphi_2 & \text{for } [k_1,k_2] = [0,\infty] \\ \varphi_2 & \text{for } [k_1,k_2] = [0,0] \\ \varphi_1 \wedge \mathcal{X}(\varphi_1 \; \mathcal{U}^{[k_1-1,k_2-1]} \; \varphi_2) & \text{for } k_1 > 0 \\ \varphi_2 \vee (\varphi_1 \wedge \mathcal{X}(\varphi_1 \; \mathcal{U}^{[0,k_2-1]} \; \varphi_2)) & \text{for } k_1 = 0, k_2 > 0 \end{cases}$$

Discrete-time CTL

$$\mathbf{E}\mathcal{X}^k\psi =$$

$$\begin{cases} \psi & \textit{if } k = 0 \\ \mathbf{E}\mathcal{X}\mathbf{E}\mathcal{X}^{k-1}\psi & \textit{else.} \end{cases}$$

$$\mathbf{E}\psi_1\ \mathcal{U}^{[k_1,k_2]}\ \psi_2 =$$

$$\begin{cases} \mathbf{E}\psi_1\ \mathcal{U}\ \psi_2 & \textit{for } [k_1,k_2] = [0,\infty] \\ \psi_2 & \textit{for } [k_1,k_2] = [0,0] \\ \psi_1 \wedge \mathbf{E}\mathcal{X}\mathbf{E}(\psi_1\ \mathcal{U}^{[k_1-1,k_2-1]}\ \psi_2) & \textit{for } k_1 > 0 \\ \psi_2 \vee (\psi_1 \wedge \mathbf{E}\mathcal{X}\mathbf{E}(\psi_1\ \mathcal{U}^{[0,k_2-1]}\ \psi_2)) & \textit{for } k_1 = 0, k_2 > 0 \end{cases}$$

Syntactic sugar

We also write

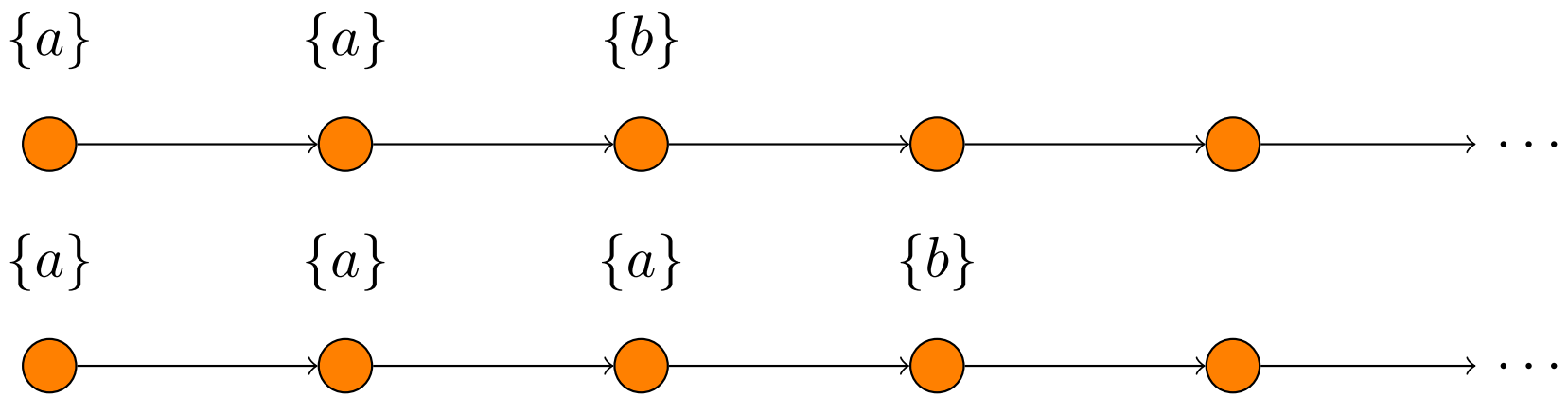
- $\mathcal{U}^{\leq k}$ instead of $\mathcal{U}^{[0,k]}$,
- $\mathcal{U}^{\geq k}$ for $\mathcal{U}^{[k,\infty]}$,
- $\mathcal{U}^{=k}$ for $\mathcal{U}^{[k,k]}$, and
- $\mathcal{U}$ for $\mathcal{U}^{[0,\infty]}$.

Example

The discrete-time LTL formula $a \, \mathcal{U}^{[2,3]} \, b$ is defined as

$$a \wedge \mathcal{X}(a \wedge \mathcal{X}(b \vee (a \wedge \mathcal{X}b))).$$

It is satisfied by paths of the following form:



Discrete-time model checking

As the discrete-time temporal operators are defined as syntactic sugar, LTL model checking can be applied to check the validity of discrete-time LTL formulae for state transition systems.