Modeling and Analysis of Hybrid Systems

Propositional and temporal logics

Prof. Dr. Erika Ábrahám

Informatik 2 - Theory of Hybrid Systems
RWTH Aachen University

SS 2013

Temporal logics

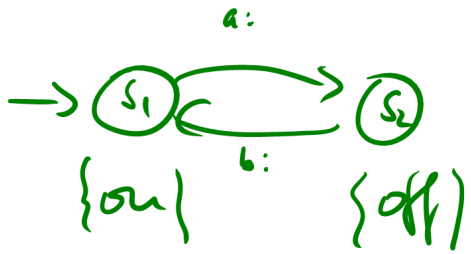
Assume

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

$s_1 \models on$

$s_2 \models off$

$s_1 \not\models on \wedge off$



Temporal logics

Assume

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

- How can we describe properties of this system?

Temporal logics

Assume

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

- How can we describe properties of this system?
- We need a well-suited logic.

Propositional logic

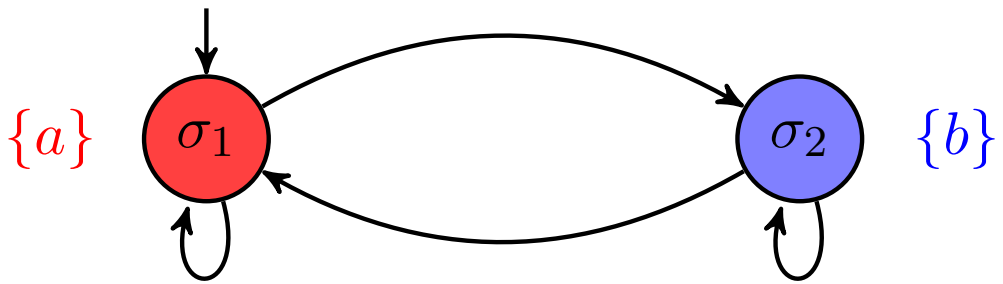
- Abstract syntax:

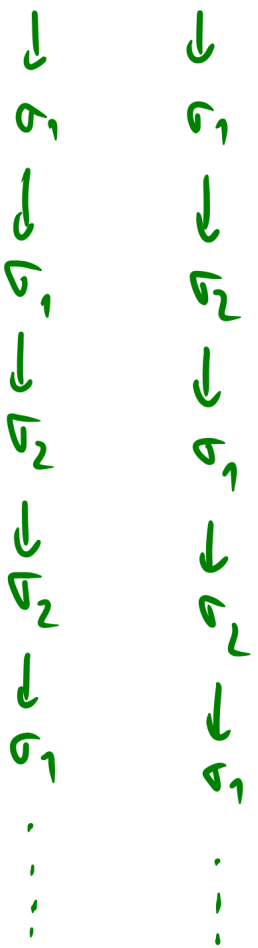
$$\varphi \ ::= \ a \mid (\varphi \wedge \varphi) \mid (\neg\varphi) \quad \mid \forall \psi \mid \exists \psi$$

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

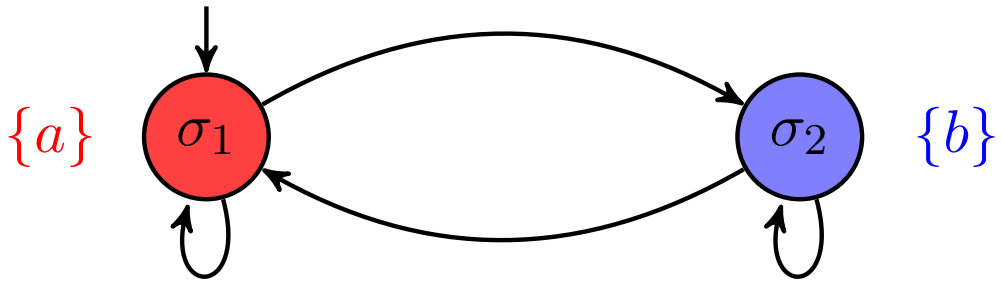
$$\begin{array}{lll} \sigma \models a & \textit{iff} & a \in L(\sigma), \\ \sigma \models (\varphi_1 \wedge \varphi_2) & \textit{iff} & \sigma \models \varphi_1 \textit{ and } \sigma \models \varphi_2, \\ \sigma \models (\neg\varphi) & \textit{iff} & \sigma \not\models \varphi. \end{array}$$

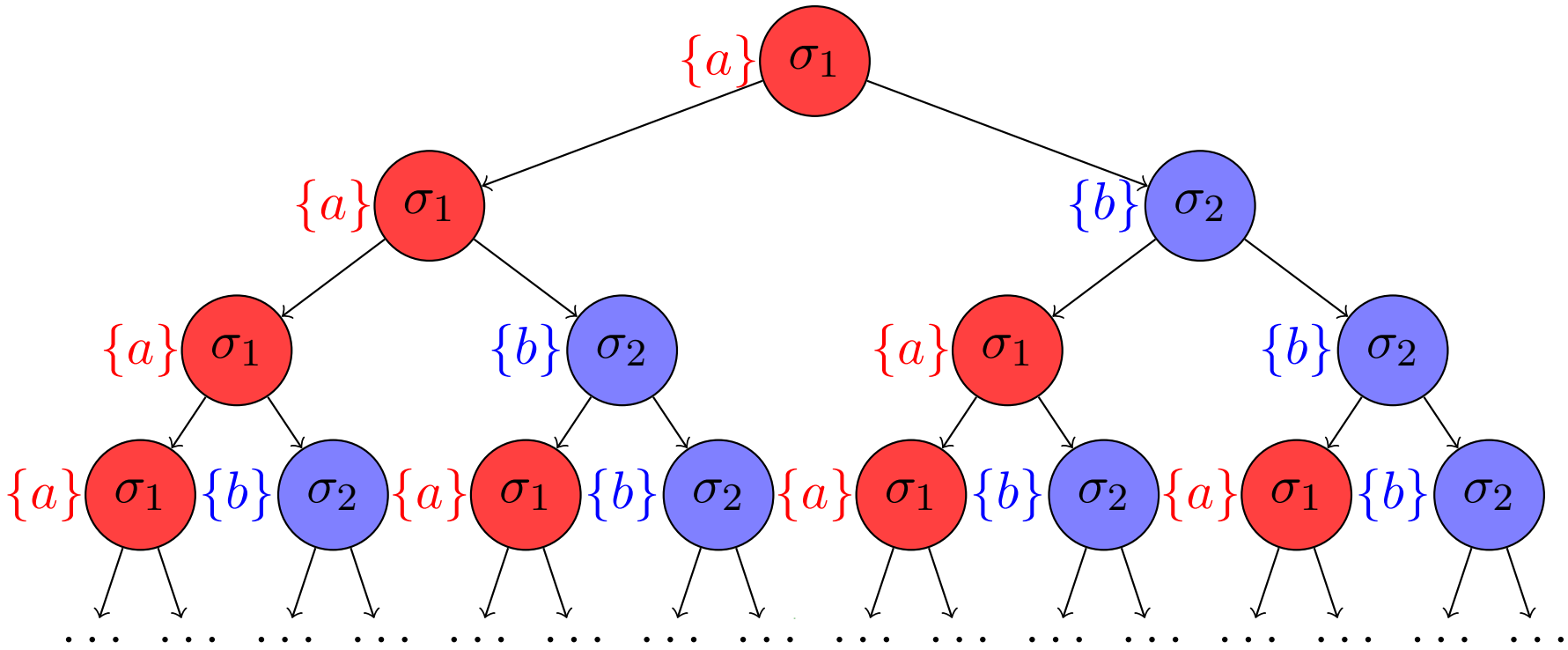
Computation tree





Computation tree

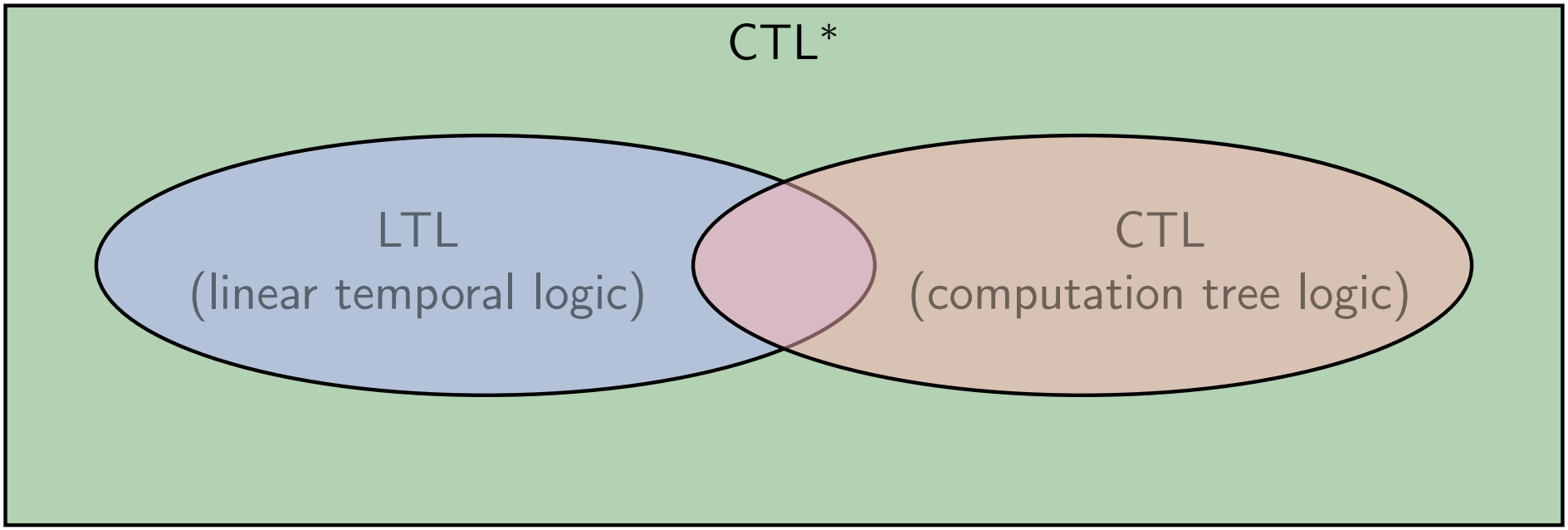




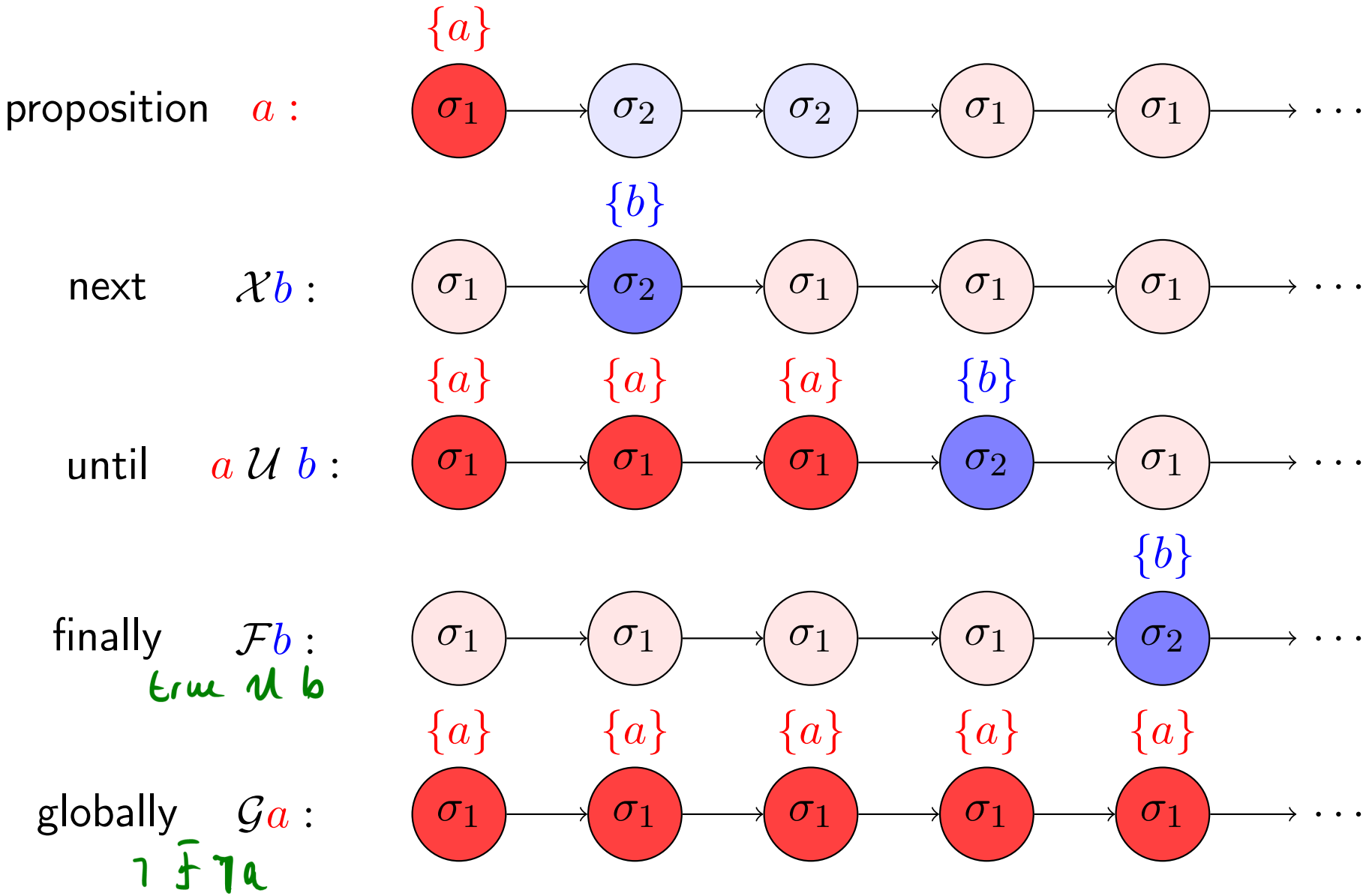
Temporal logics

In the computation tree we can describe

- a given path starting in a state (path formulas, "linear" properties) and
- quantified (universal/existential) properties over all paths starting in a given state (state formulas, "branching" properties).

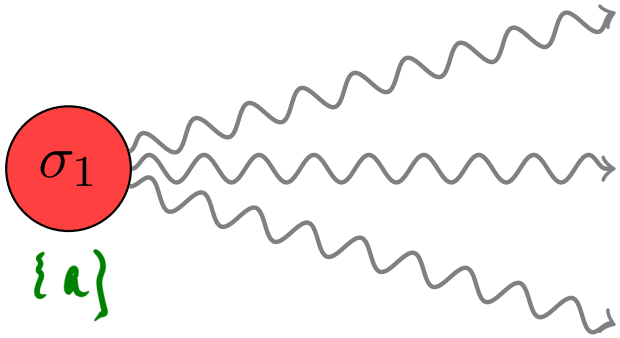


Examples for path formulas



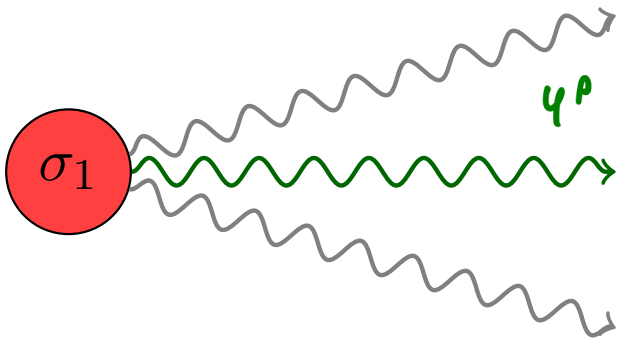
Examples for state formulas

proposition a :



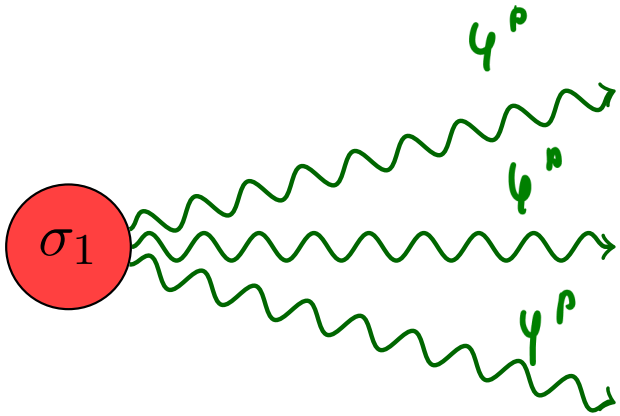
path : φ^p

exists $\mathbf{E}\ \varphi^p$:



state : φ^s

for all $\mathbf{A}\ \varphi^p$:



CTL* syntax

CTL* state formulae:

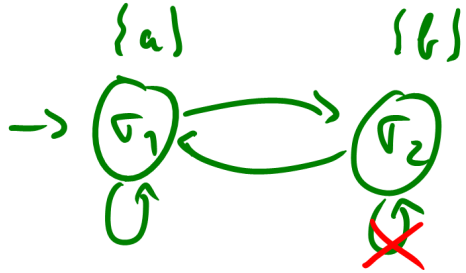
$$\psi^s \quad ::= \quad a \mid (\psi^s \wedge \psi^s) \mid (\neg\psi^s) \mid (\mathbf{E}\varphi^p)$$

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

CTL* path formulae:

$$\varphi^p \quad ::= \quad \psi^s \mid (\varphi^p \wedge \varphi^p) \mid (\neg\varphi^p) \mid (\mathcal{X}\varphi^p) \mid (\varphi^p \,\mathcal{U}\, \varphi^p) \mid \mathcal{G}\,\varphi^p \mid \mathcal{F}\,\varphi^p$$

where ψ^s are CTL* state formulae.



$\sigma_1 \models_{CTL^*}$

(1) $E\,G\,a$

$\sigma_1 \models$

(2) $E\,X\,X\,X\,b$

$\sigma_1 \not\models$

(3) $A\,F\,b \equiv \neg E \neg F b$

$\sigma_1 \models$

(4) $A\,a\,\mathcal{U}\,(b\,\mathcal{U}\,a)$

$\sigma_1 \models$

(5) a

(6) $A\,G\,F\,b$

(7) $A\,G\,E\,F\,b$

(8) $A\,G\,b \rightarrow F\,a$

CTL*

LTL

A (path formulas)

A a U (G b)

CTL

Q O_p^{path} Q O_p^{path} ....

A G E F a

CTL* syntax

CTL* state formulae:

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

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

CTL* path formulae:

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

where ψ^s are CTL* state formulae.

CTL* formulae are CTL* state formulae.

CTL* syntax

CTL* state formulae:

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

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

CTL* path formulae:

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

where ψ^s are CTL* state formulae.

CTL* formulae are CTL* state formulae. $LSTS \models \psi^s$ iff $LSTS, s_0 \models \varphi^s$

We often omit parentheses. Syntactic sugar:
$\mathbf{A}$ ("for all"), $\mathcal{F}$ ("finally" or "eventually"), $\mathcal{G}$ ("globally" or "always"), $\mathcal{R}$ ("releases")

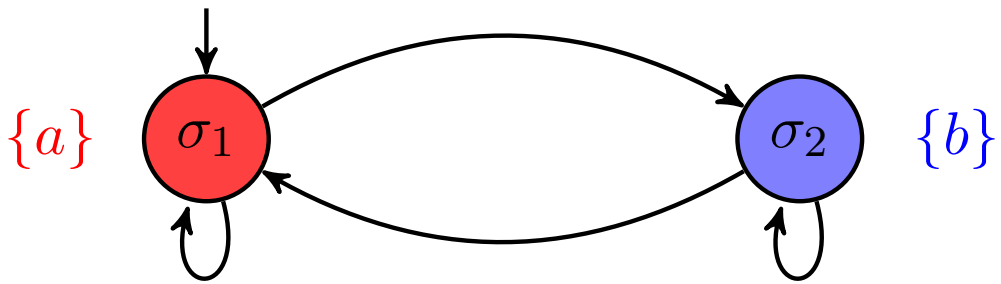
CTL* semantics

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

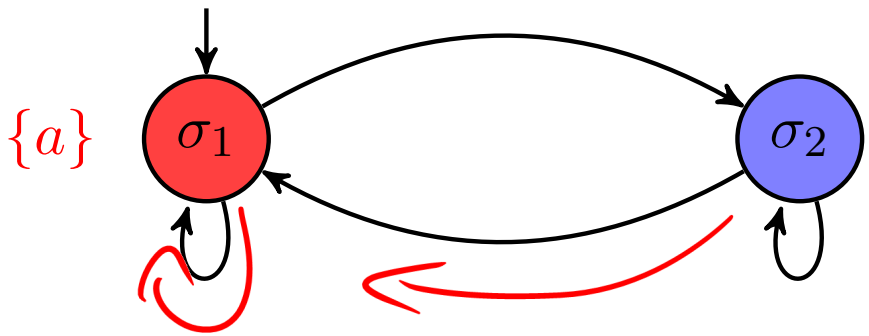
$$
\begin{array}{lll}
\sigma \models a & \textit{iff} & a \in L(\sigma) \\
\sigma \models \psi_1^s \wedge \psi_2^s & \textit{iff} & \sigma \models \psi_1^s \textit{ and } \sigma \models \psi_2^s \\
\sigma \models \neg\psi^s & \textit{iff} & \sigma \not\models \psi^s \\
\sigma \models \mathbf{E}\varphi^p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

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

Computation tree



Computation tree



LTL ⇒ CTL

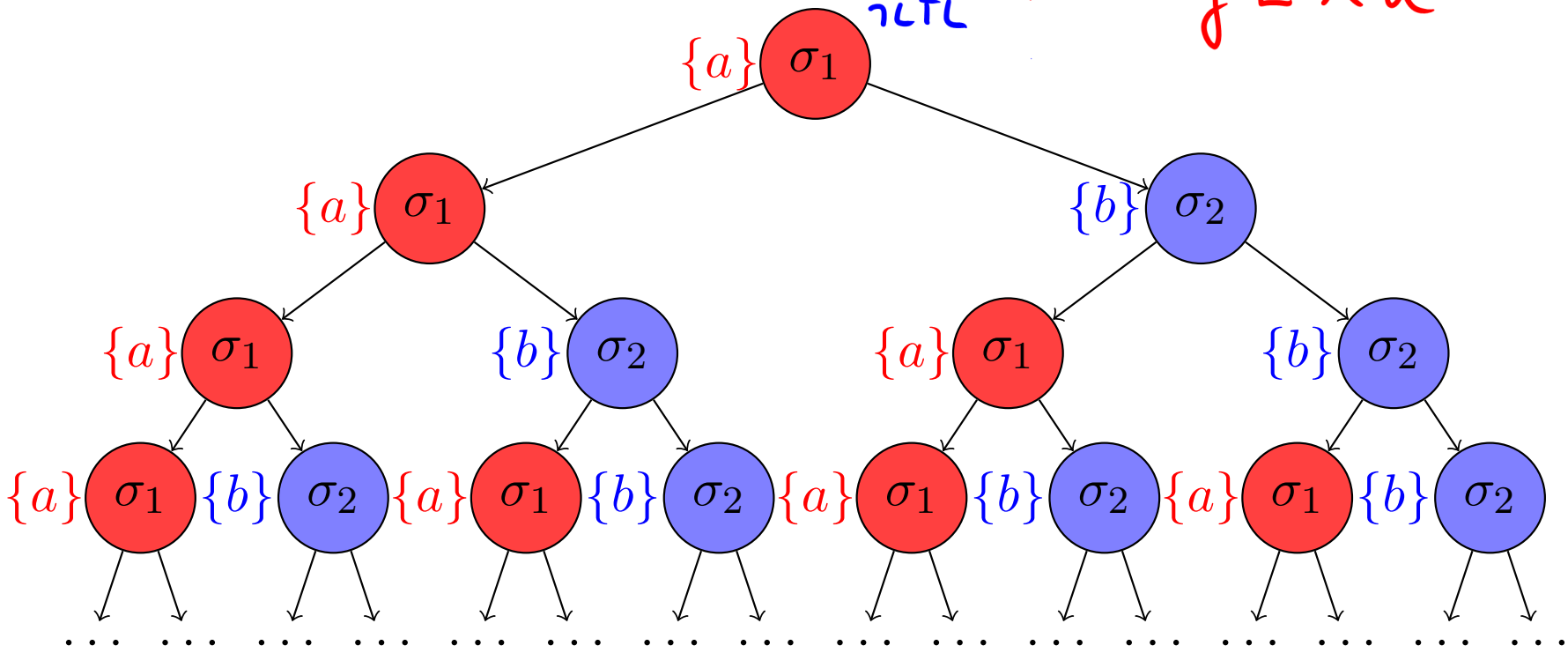
$\sigma_1 \models A\,F\,a$

LTL ⇒ ¬CTL

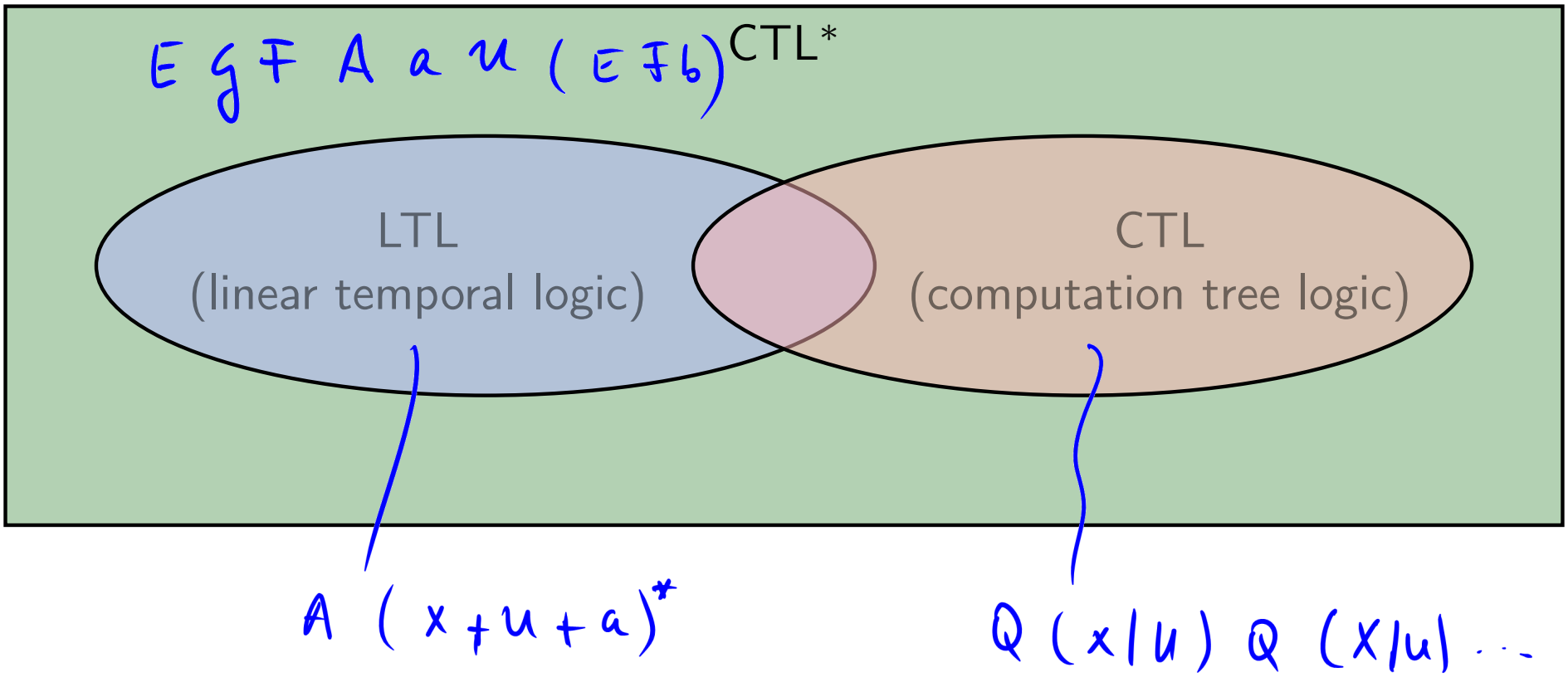
$\sigma_1 \models A\,F\,a\;U\,(b \vee ga)$

CTL ⇒ ¬LTL

$\sigma_1 \models A\,G\,E\,X\,a$



The relation of LTL, CTL, and CTL*



LTL syntax

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

- Abstract syntax:

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

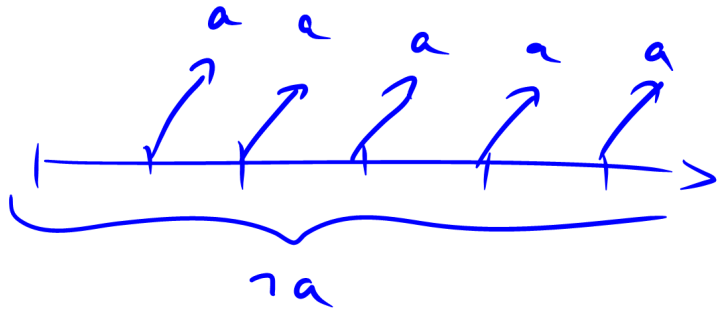
  where $a \in AP$.

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

$\mathcal{F}a \equiv \mathrm{true}\,\mathcal{U}\,a$ $\qquad$ $\mathcal{G}a \equiv \neg(\mathcal{F}(\neg a))$

LTL semantics

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

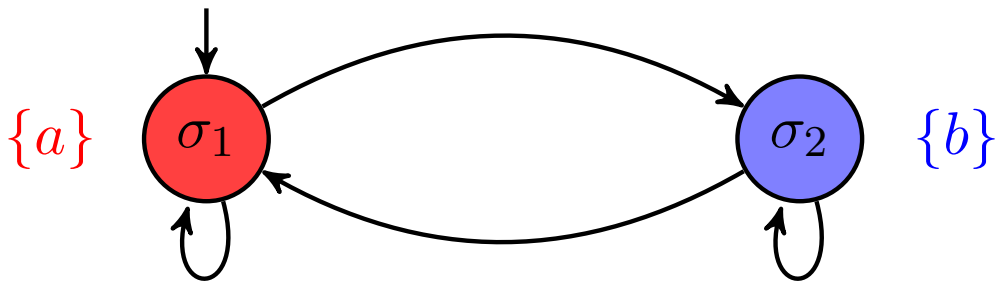


(A) G F a

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

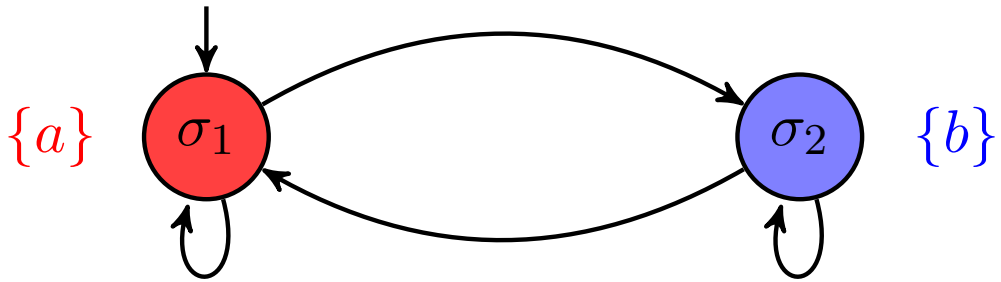
$\mathcal{LSTS} \models \varphi^p$ iff $\pi \models \varphi^p$ for all paths π of $\mathcal{LSTS}$.

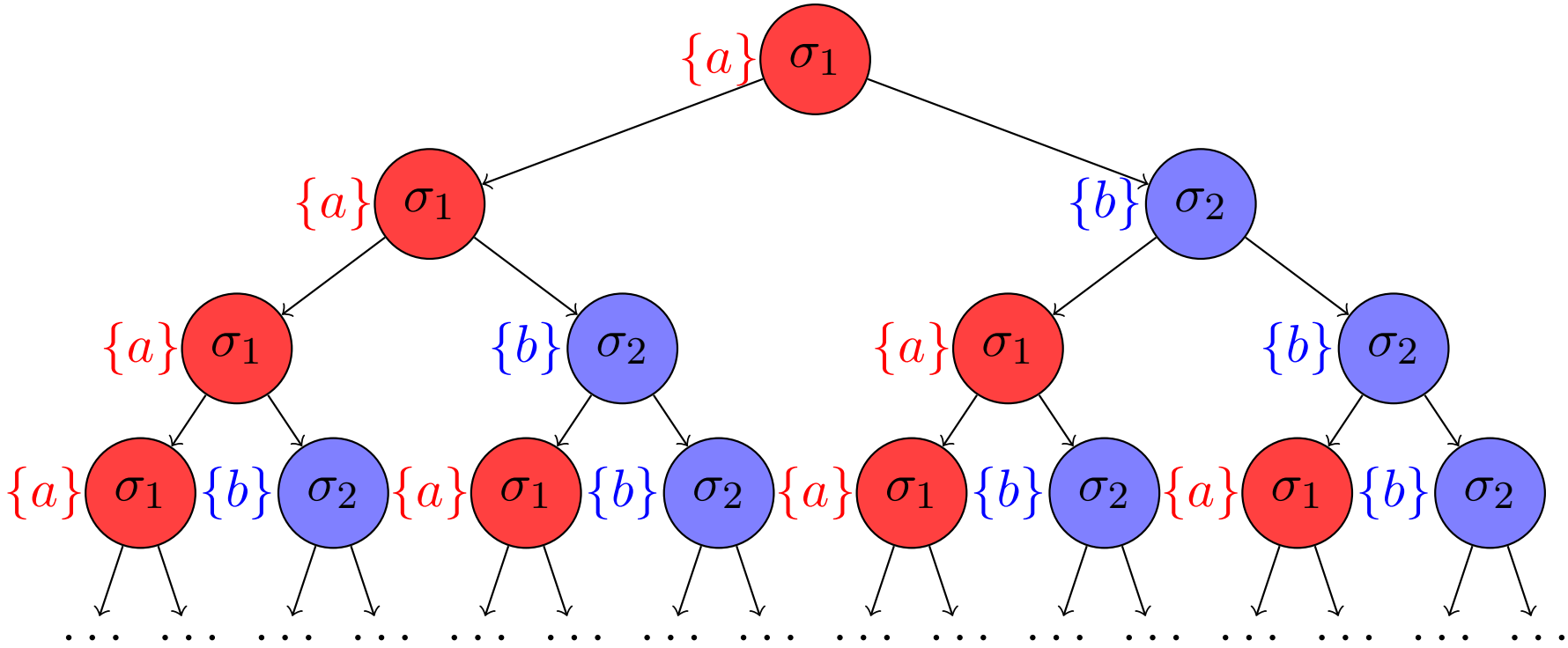
Computation tree



Computation tree

$(A)\ a\ \mathcal{U}\ (\neg a \vee \neg b)$





CTL syntax

CTL state formulae:

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

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

CTL path formulae:

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

where ψ^s are CTL state formulae.

CTL formulae are CTL state formulae.

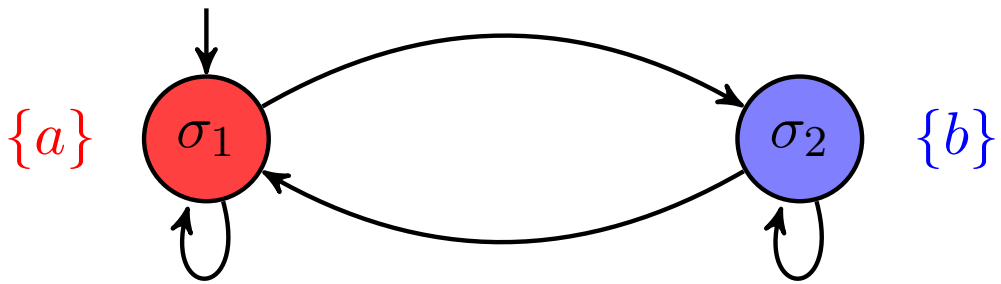
We omit parentheses when causing no confusion.

CTL semantics

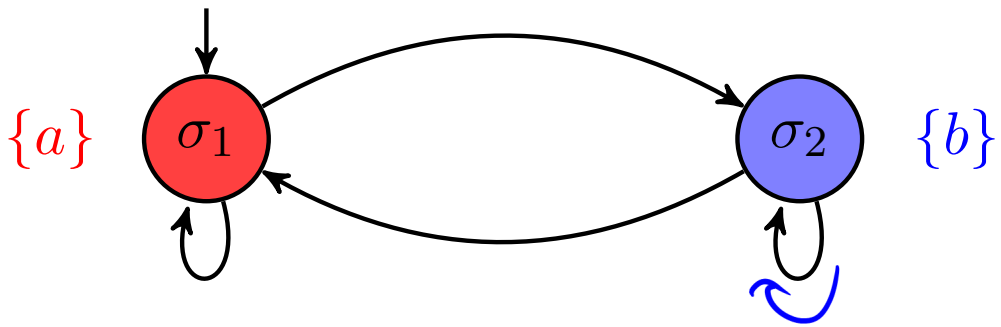
$$
\begin{array}{lll}
\sigma \models a & \textit{iff} & a \in L(\sigma) \\
\sigma \models \psi_1^s \wedge \psi_2^s & \textit{iff} & \sigma \models \psi_1^s \textit{ and } \sigma \models \psi_2^s \\
\sigma \models \neg\psi^s & \textit{iff} & \sigma \not\models \psi^s \\
\sigma \models \mathbf{E}\varphi^p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

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

Computation tree



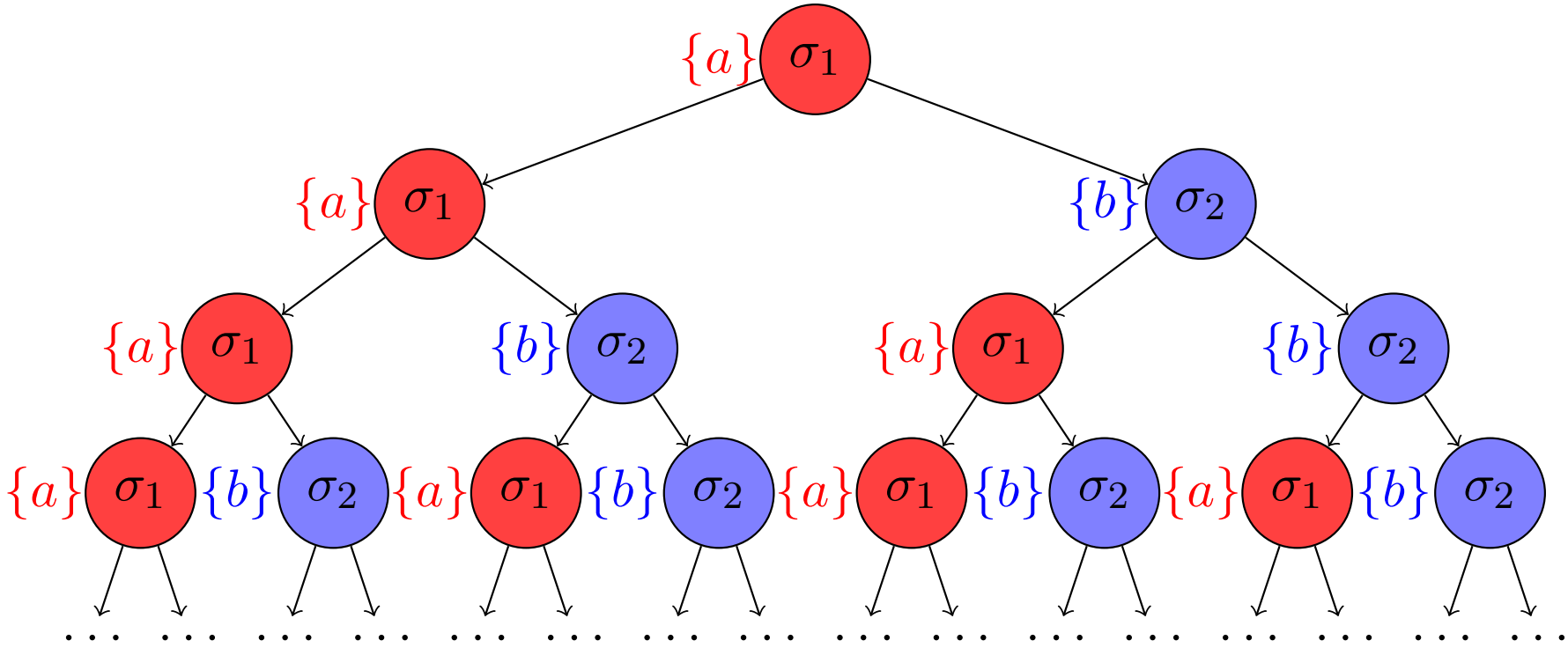
Computation tree



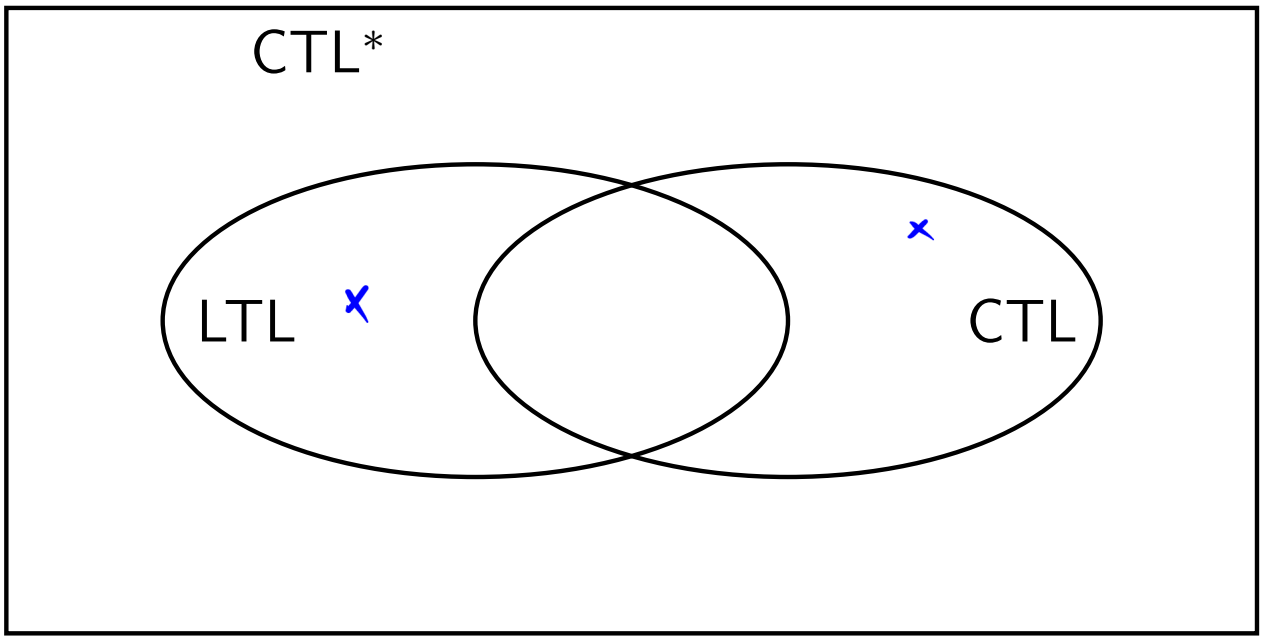
$\sigma_1 \models AGEXb$

$\sigma_2 \models ?$ -11-

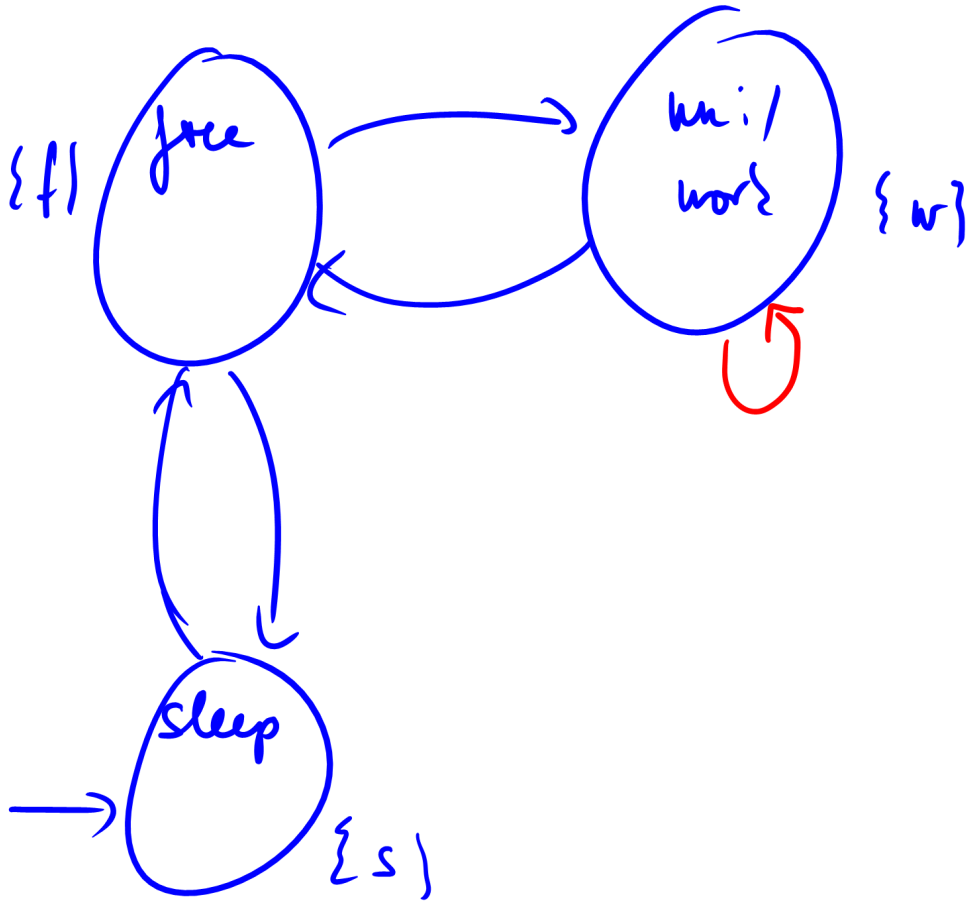
$\sigma_1 \models EXAGb$



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.



$\{x=0\}$

$\langle x := x+1 \rangle \parallel \langle x := 2 \rangle$

$\{ x=2 \cup x=3 \cup (x=1) \}$

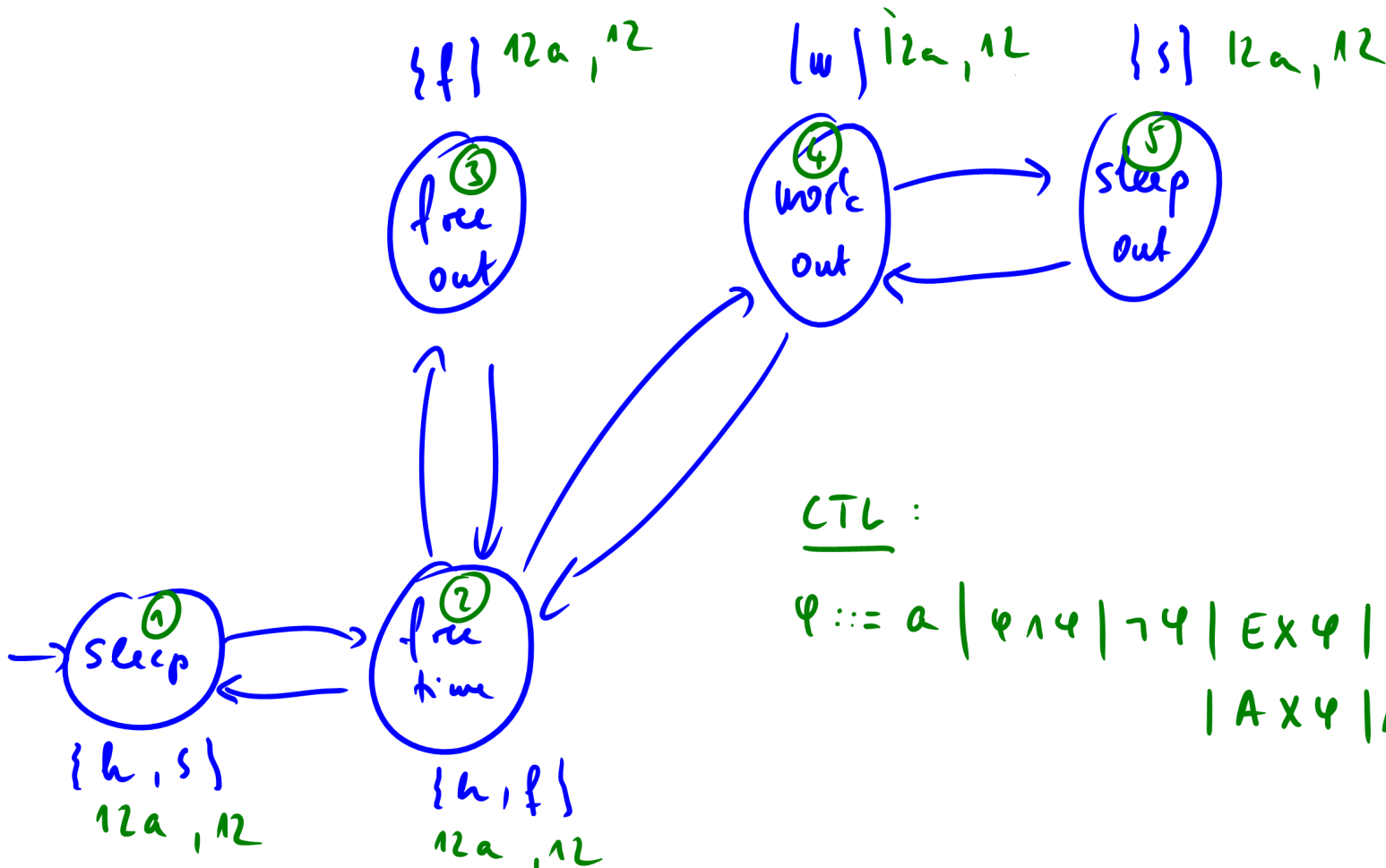
$sleep \models \bar{E}\, X\, x\, G\, w$

$sleep \models \neg E\, X\, X\, G\, w$

$s \rightarrow \bar{F}\, f$

$s \rightarrow F(\neg s)$

$G\, f \rightarrow (\neg s\ U\ w)$



CTL:

$\varphi ::= a \mid \varphi \wedge \varphi \mid \neg\varphi \mid EX\varphi \mid E\varphi U \varphi$
$\mid AX\varphi \mid A\varphi U \varphi$

0) $\neg w$

1) h

2) s

3) $h \wedge s$ (w 1, w 2)

4) $\neg(h \wedge s)$ (↓)

5) $EX\, h$ (w 1)

6) $E f U s$

7) $AX\, w$

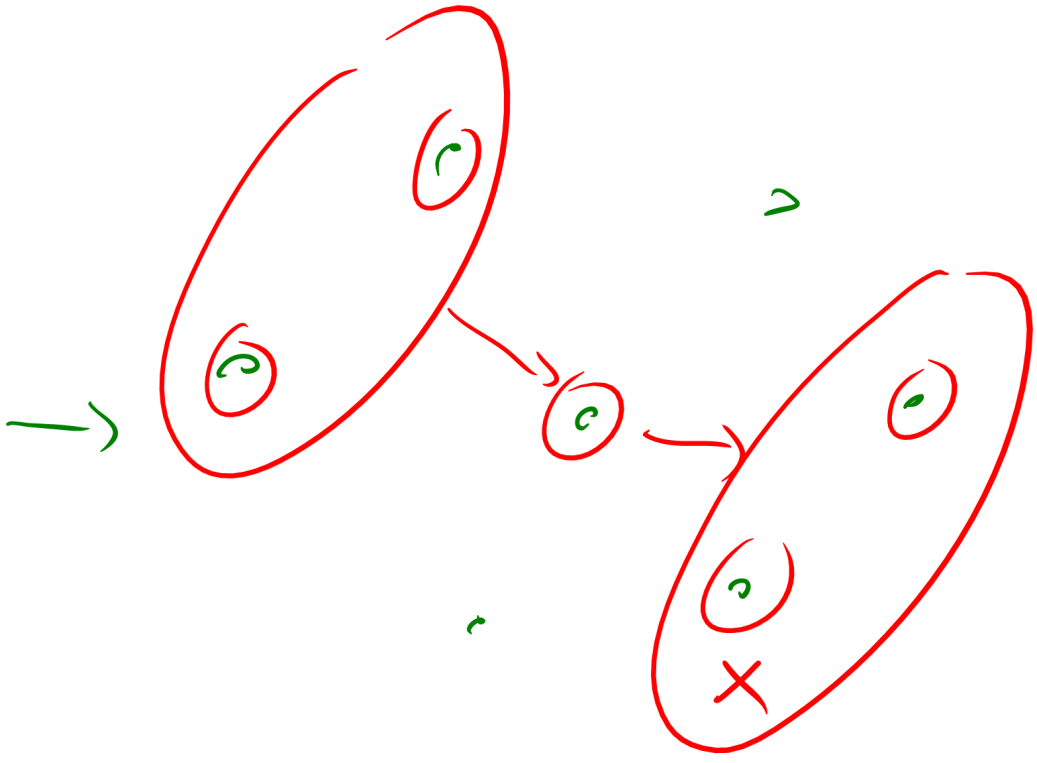
8) $A\, \neg w\, U\, h$

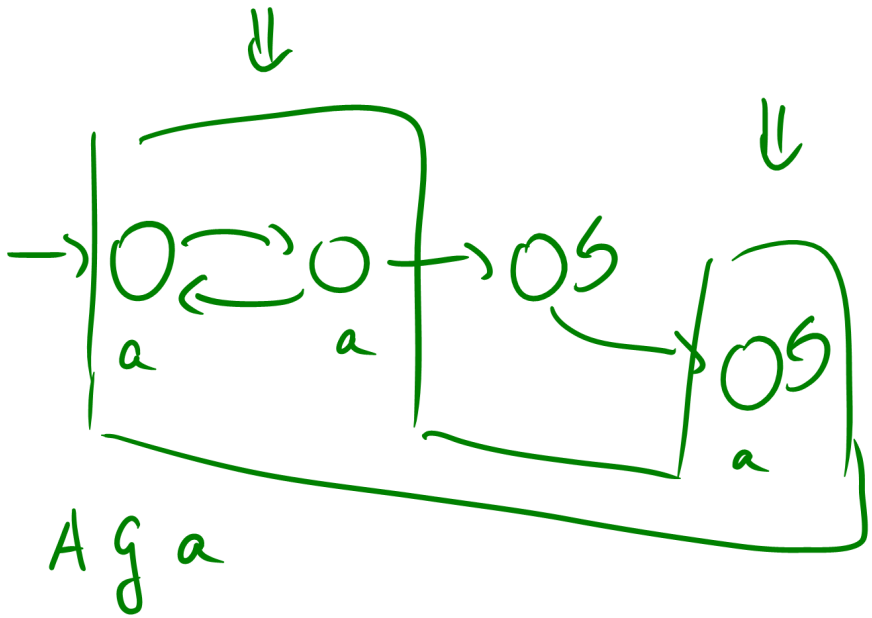
9) $EF(\neg s \wedge E f U s)$

=> 10) $EG\, \neg s$

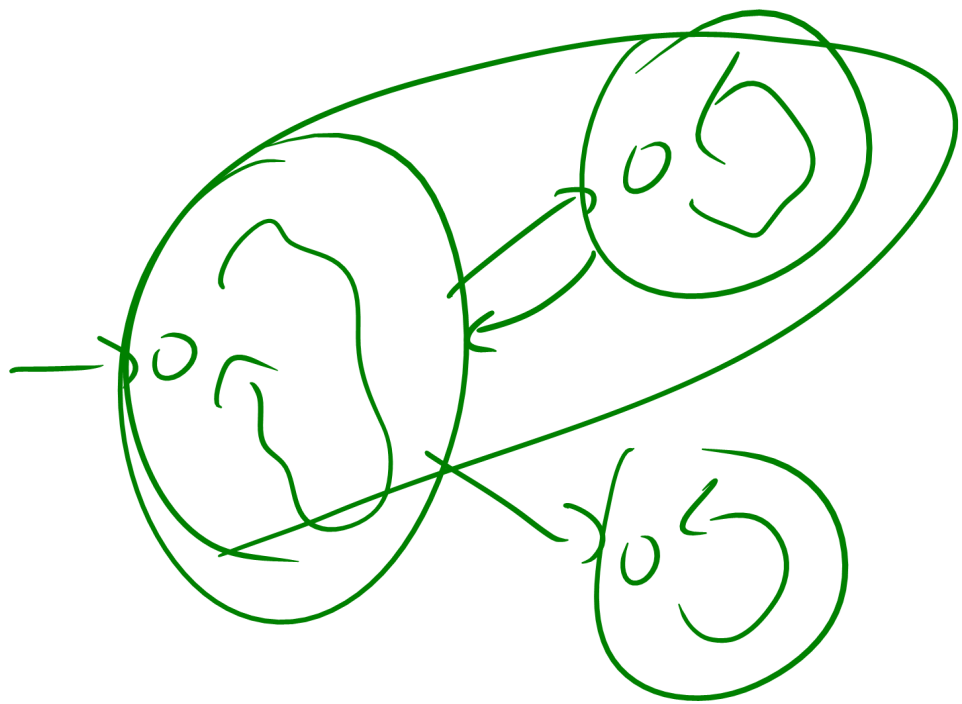
11) $AF\, \neg s \equiv A\, true\, U\, \neg s$

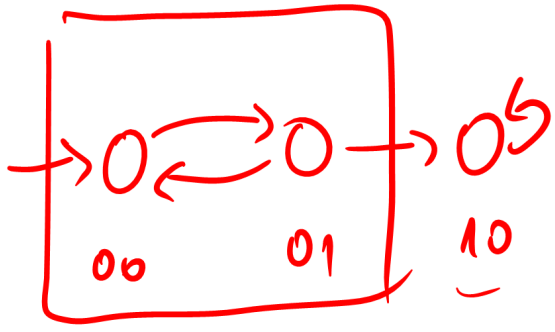
12) $AG\, \underline{\neg(w \wedge s)}_{\neg 12a}$

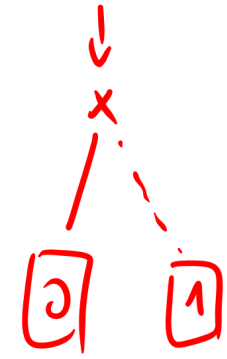




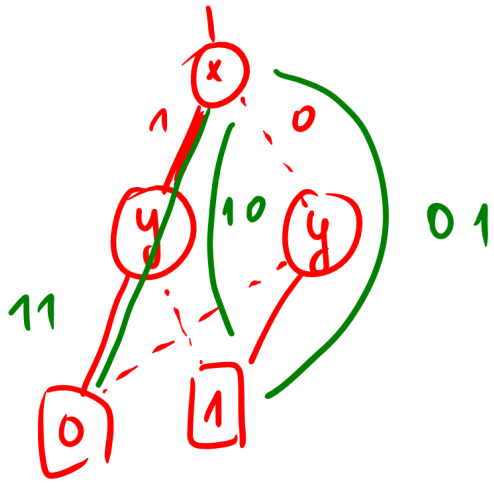
A g a

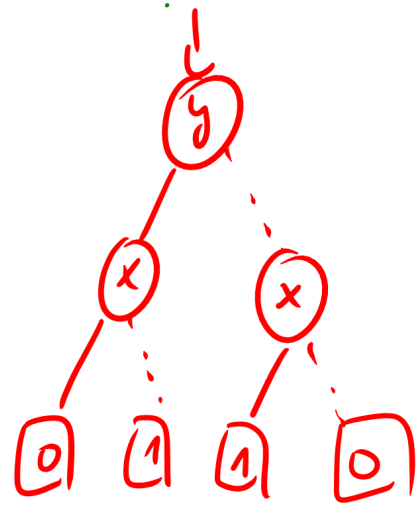


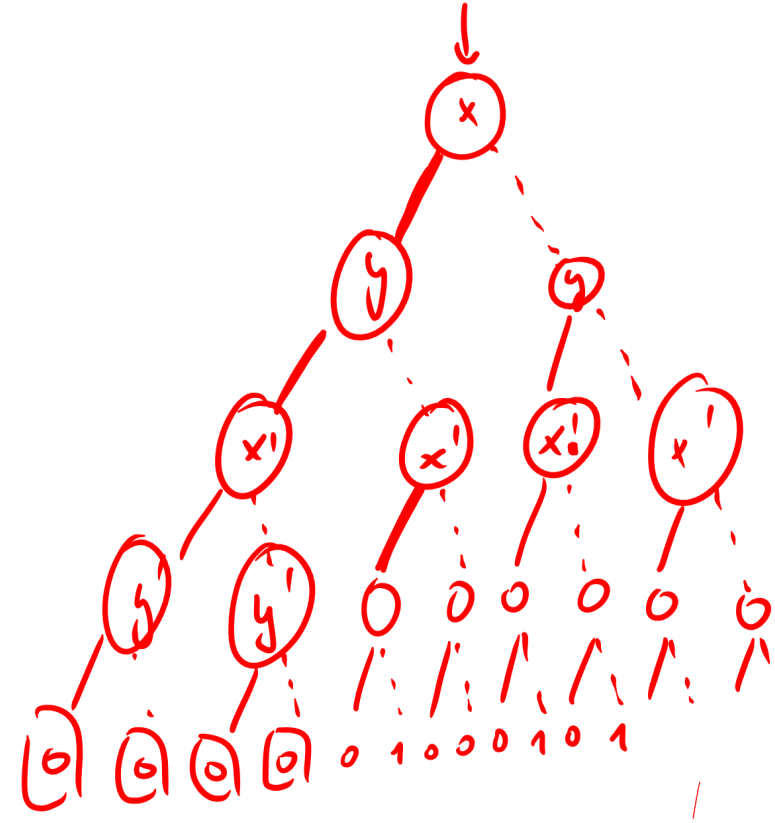




Binary Decision Diagram (BDD)







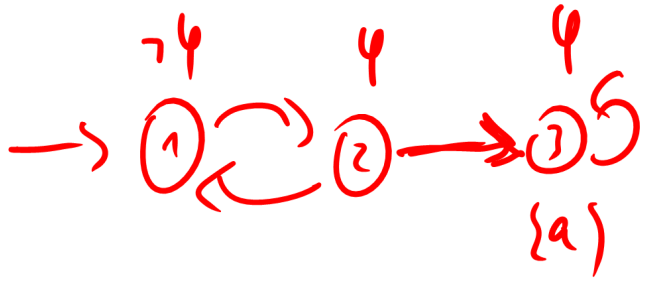
$\exists x'.\ S(x') \wedge T(x, x')$

$= \neg S \wedge$

$$I(x) \cdot T(x, x') \quad A(x) \quad (1)$$

$$\text{EF}\, a \qquad \exists x'.\ A(x') \wedge T(x, x') \quad (2)$$

$$2 - 1 = \phi$$



$\varphi := E\, F_{\leq 1}\, a$

$E(a \vee Xa)$

$F_{=5}\, a$

$=$

$XXXXXa$

CTL model checking

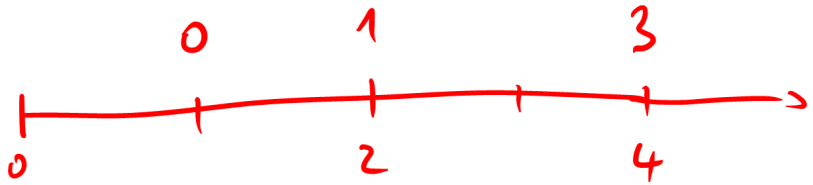
Given a state transition system and a CTL formula ψ^s, CTL model checking labels the states recursively with the sub-formulae of ψ^s inside-out.

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

CTL model checking

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

Discrete-time LTL



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

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

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

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

$\equiv \varphi_1 \wedge \mathcal{X}(\varphi_1 \wedge (\varphi_2 \vee (\varphi_1 \wedge \mathcal{X}(\varphi_2 \vee \varphi_1 \wedge \mathcal{X}\varphi$

$\varphi_1 \; \mathcal{U}^{[2,4]} \; \varphi_2 \equiv \varphi_1 \wedge \mathcal{X}(\varphi_1 \; \mathcal{U}^{[1,3]} \; \varphi_2)$

$\equiv \varphi_1 \wedge \mathcal{X}(\varphi_1 \wedge \varphi_1 \; \mathcal{U}^{[0,2]} \; \varphi_2]$

$\equiv \varphi_1 \wedge \mathcal{X}(\varphi_1 \wedge (\varphi_2 \vee \varphi_1 \wedge \mathcal{X}\varphi_1 \; \mathcal{U}^{[0,1]} \; \varphi_2))$

Discrete-time CTL

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

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

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

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

Syntactic sugar

We also write

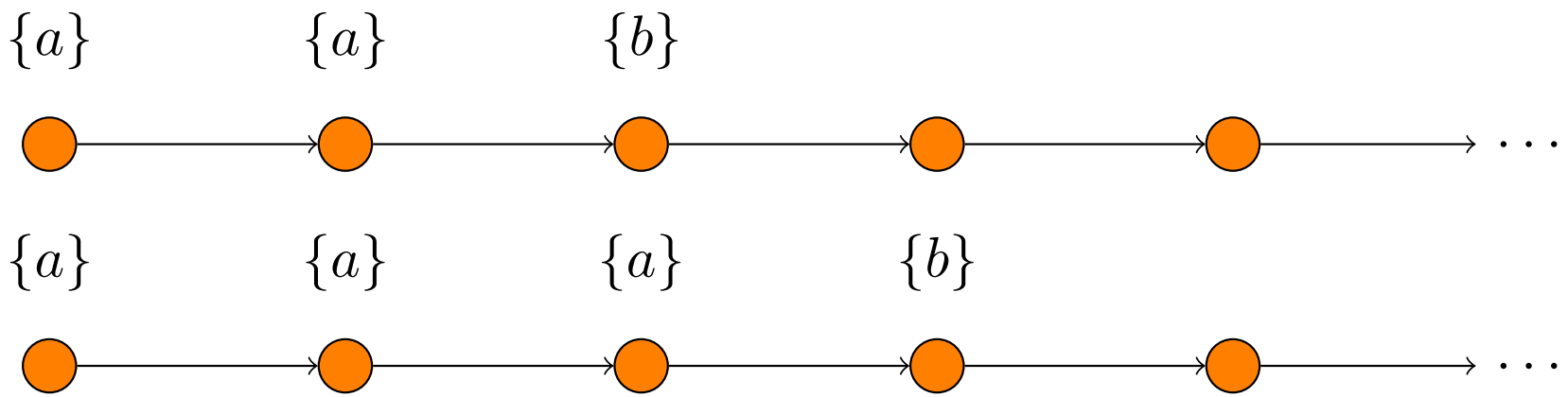
- $\mathcal{U}^{\leq k}$ instead of $\mathcal{U}^{[0,k]}$,
- $\mathcal{U}^{\geq k}$ for $\mathcal{U}^{[k,\infty]}$,
- $\mathcal{U}^{=k}$ for $\mathcal{U}^{[k,k]}$, and
- $\mathcal{U}$ for $\mathcal{U}^{[0,\infty]}$.

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.