Model Checking Linear Temporal Properties on Polyhedral Systems

Fabio Mogavero

Università degli Studi di Napoli Federico II

(joint work with Massimo Benerecetti & Marco Faella)

Time '24

October 28, 2024

The Problem

- Model Checking Cyber-Physical Systems
  + Continuous-Time
  + Infinite-State Space
  + Often modelled as Linear Hybrid Automata (LHA)

- Undecidability rules supreme, e.g., Reachability in LHA

- Temporal Reasoning inside a single location of an LHA has not been addressed

Our Contribution

We study the Model-Checking Problem of

+ Real-Time Linear Temporal Properties Ψ of

+ Trajectories Generated by Polyhedral Differential Inclusions $\mathcal{P}$

+ Solution: Exponential in $|\Psi|$ and Doubly-Exponential in $|\mathcal{P}|$ (Bounded-Time Trajectories)

Polyhedral Systems & Real-Time Linear Temporal Logic

Polyhedral Systems

- $\mathcal{P} = \langle Flow, Inv, [\cdot] \rangle$

Polyhedral Systems

- $\mathcal{P} = \langle Flow, Inv, [\cdot] \rangle$

$Flow \in ConvPoly(\mathbb{R}^n)$ **flow constraint**, i.e., constraints on the derivatives

Polyhedral Systems

- $\mathcal{P} = \langle Flow, Inv, [\cdot] \rangle$

$Inv \in Poly(\mathbb{R}^n)$ invariant condition

$Flow \in ConvPoly(\mathbb{R}^n)$ flow constraint, i.e., constraints on the derivatives

Polyhedral Systems

- $\mathcal{P} = \langle Flow, Inv, [\cdot] \rangle$

  $[\cdot] : AP \to Poly(\mathbb{R}^n)$ atomic proposition interpretation

  $Inv \in Poly(\mathbb{R}^n)$ invariant condition

  $Flow \in ConvPoly(\mathbb{R}^n)$ flow constraint, i.e., constraints on the derivatives

Polyhedral Systems

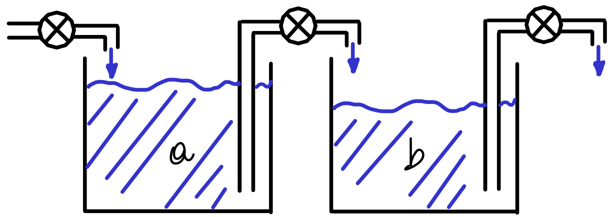
- $\mathcal{P} = \langle Flow, Inv, [\cdot] \rangle$

$[\cdot] : AP \to Poly(\mathbb{R}^n)$ atomic proposition interpretation

$Inv \in Poly(\mathbb{R}^n)$ invariant condition

$Flow \in ConvPoly(\mathbb{R}^n)$ flow constraint, i.e., constraints on the derivatives

- A Two-Tank Example



Polyhedral Systems

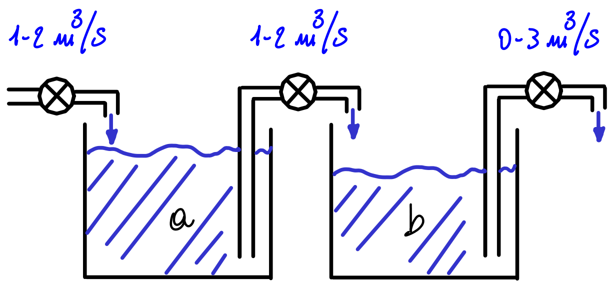
- $\mathcal{P} = \langle \mathit{Flow}, \mathit{Inv}, [\![\cdot]\!] \rangle$

$[\![\cdot]\!] : AP \to Poly(\mathbb{R}^n)$ atomic proposition interpretation

$\mathit{Inv} \in Poly(\mathbb{R}^n)$ invariant condition

$\mathit{Flow} \in ConvPoly(\mathbb{R}^n)$ flow constraint, i.e., constraints on the derivatives

- A Two-Tank Example



Polyhedral Systems

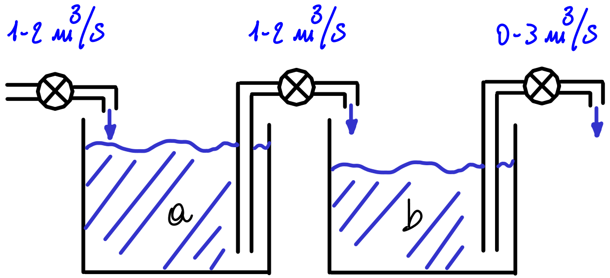
- $\mathcal{P} = \langle Flow, Inv, [\cdot] \rangle$

$[\cdot] : AP \to Poly(\mathbb{R}^n)$ atomic proposition interpretation

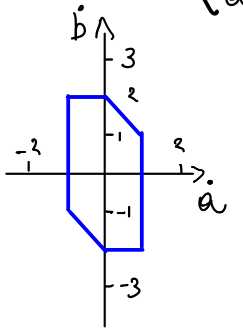
$Inv \in Poly(\mathbb{R}^n)$ invariant condition

$Flow \in ConvPoly(\mathbb{R}^n)$ flow constraint, i.e., constraints on the derivatives

- A Two-Tank Example



$$Flow = \begin{cases} \dot{a} \in [-1, 1] \\ \dot{b} \in [-2, 2] \\ \dot{a} + \dot{b} \in [-2, 2] \end{cases}$$



Polyhedral Systems

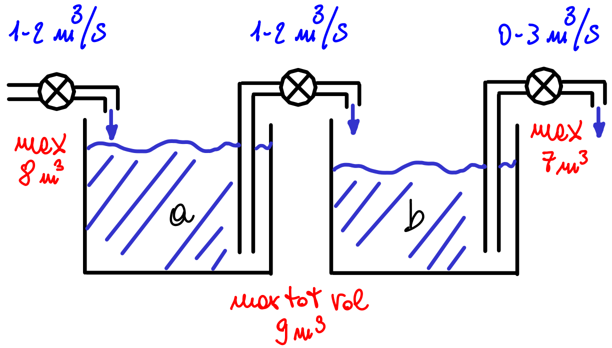
- $\mathcal{P} = \langle Flow, Inv, [\cdot] \rangle$

$[\cdot] : AP \to Poly(\mathbb{R}^n)$ atomic proposition interpretation

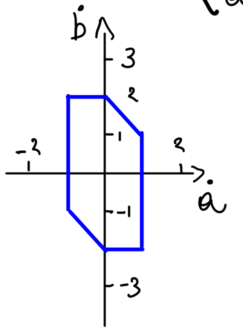
$Inv \in Poly(\mathbb{R}^n)$ invariant condition

$Flow \in ConvPoly(\mathbb{R}^n)$ flow constraint, i.e., constraints on the derivatives

- A Two-Tank Example



$$Flow = \begin{cases} \dot{a} \in [-1,1] \\ \dot{b} \in [-2,2] \\ \dot{a}+\dot{b} \in [-2,2] \end{cases}$$



Polyhedral Systems

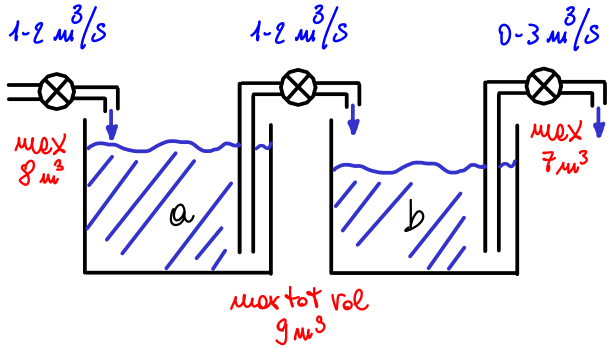
- $\mathcal{P} = \langle Flow, Inv, [\cdot] \rangle$

$[\cdot] : AP \to Poly(\mathbb{R}^n)$ atomic proposition interpretation

$Inv \in Poly(\mathbb{R}^n)$ invariant condition

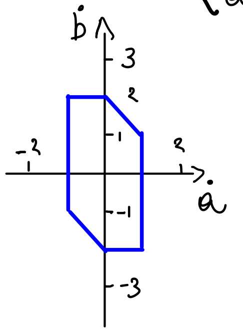
$Flow \in ConvPoly(\mathbb{R}^n)$ flow constraint, i.e., constraints on the derivatives

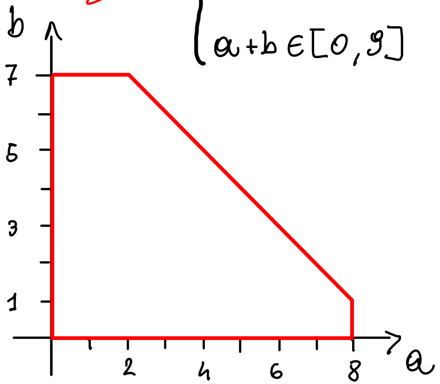
- A Two-Tank Example



$$Flow = \begin{cases} \dot{a} \in [-1, 1] \\ \dot{b} \in [-2, 2] \\ \dot{a} + \dot{b} \in [-2, 2] \end{cases}$$

$$Inv = \begin{cases} a \in [0, 8] \\ b \in [0, 7] \\ a + b \in [0, 9] \end{cases}$$





Polyhedral Systems

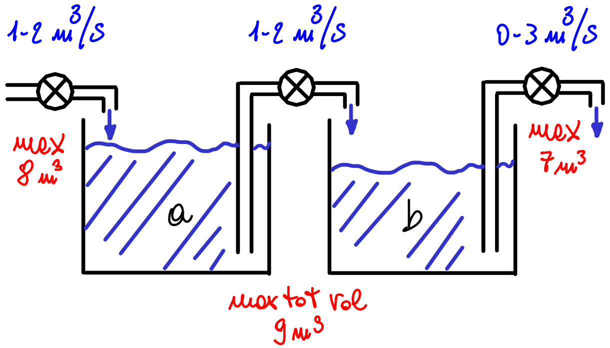
- $\mathcal{P} = \langle Flow, Inv, [\cdot] \rangle$

$[\cdot] : AP \to Poly(\mathbb{R}^n)$ atomic proposition interpretation

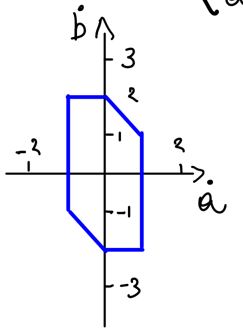
$Inv \in Poly(\mathbb{R}^n)$ invariant condition

$Flow \in ConvPoly(\mathbb{R}^n)$ flow constraint, i.e., constraints on the derivatives

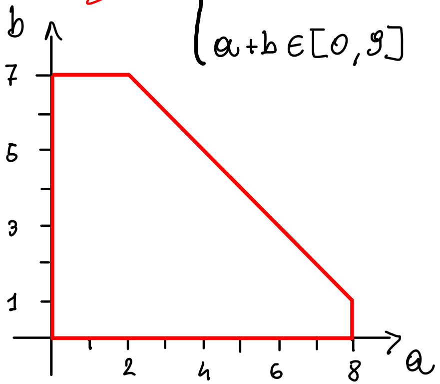
- A Two-Tank Example



$$Flow = \begin{cases} \dot{a} \in [-1,1] \\ \dot{b} \in [-2,2] \\ \dot{a}+\dot{b} \in [-2,2] \end{cases}$$



$$Inv = \begin{cases} a \in [0,8] \\ b \in [0,7] \\ a+b \in [0,9] \end{cases}$$



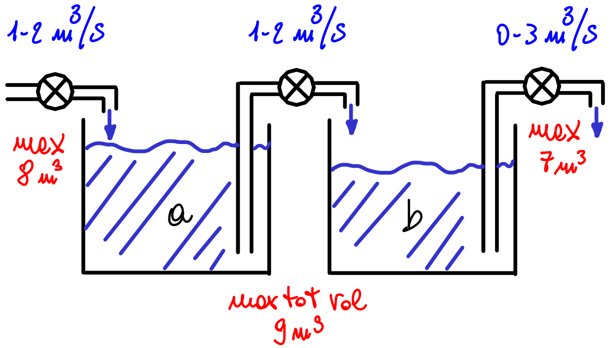
Idle state: $0 \le a \le 1 ;\ 0 \le b \le 2$

Optimal state: $3 < a \le 7 ;\ 3 < b \le 5$

Polyhedral Systems

- $\mathcal{P} = \langle Flow, Inv, [\cdot] \rangle$
  - $[\cdot] : AP \to Poly(\mathbb{R}^n)$ atomic proposition interpretation
  - $Inv \in Poly(\mathbb{R}^n)$ invariant condition
  - $Flow \in ConvPoly(\mathbb{R}^n)$ flow constraint, i.e., constraints on the derivatives

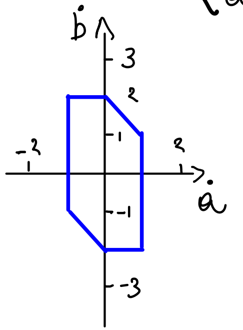
- A Two-Tank Example



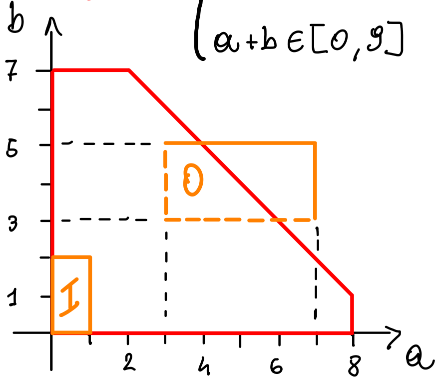
Idle state : $0 \le a \le 1$; $0 \le b \le 2$

Optimal state : $3 < a \le 7$; $3 < b \le 5$

$$Flow = \begin{cases} \dot{a} \in [-1, 1] \\ \dot{b} \in [-2, 2] \\ \dot{a} + \dot{b} \in [-2, 2] \end{cases}$$



$$Inv = \begin{cases} a \in [0, 8] \\ b \in [0, 7] \\ a + b \in [0, 9] \end{cases}$$



Atomic Propositions

$$[I] = \begin{cases} a \in [0, 1] \\ b \in [0, 2] \end{cases}$$

$$[O] = \begin{cases} a \in (3, 7] \\ b \in (3, 5] \end{cases}$$

Trajectories & Signals

- **Trajectory**: A continuous function $f : I \subseteq \mathbb{R}_+ \longrightarrow \mathbb{R}^n$

Time interval

Time domain

State space

TRAJECTORIES & SIGNALS

- **Trajectory**: A continuous function $f : \underset{\text{TIME INTERVAL}}{\underline{I}} \subseteq \underset{\text{TIME DOMAIN}}{\mathbb{R}_+} \longrightarrow \underset{\text{STATE SPACE}}{\mathbb{R}^n}$

+ f is a trajectory in the Polyhedral System P if $\begin{cases} f(t) \in Inv \\ \dot{f}(t) \in Flow \end{cases} \quad \forall t \in \underline{I}$

finite number of discontinuities in any bounded subinterval $I' \subseteq \underline{I}$

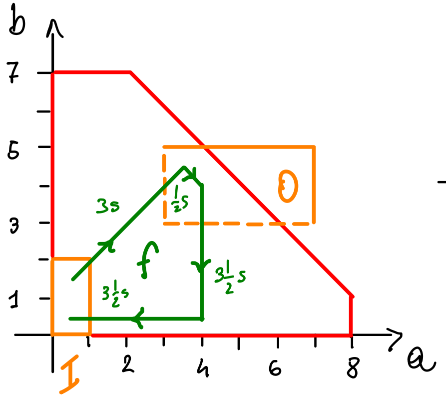
Trajectories & Signals

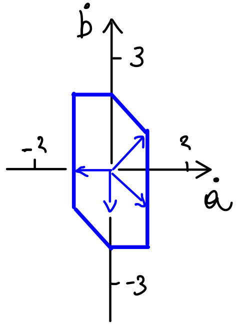
- **Trajectory**: A continuous function $f : I \subseteq \mathbb{R}_+ \longrightarrow \mathbb{R}^n$

Time Interval (I), Time Domain ($\mathbb{R}_+$), State Space ($\mathbb{R}^n$)

+ f is a trajectory in the Polyhedral System $\mathcal{P}$ if $\begin{cases} f(t) \in Inv \\ \dot{f}(t) \in Flow \end{cases} \quad \forall t \in I$

finite number of discontinuities in any bounded subinterval $I' \subseteq I$



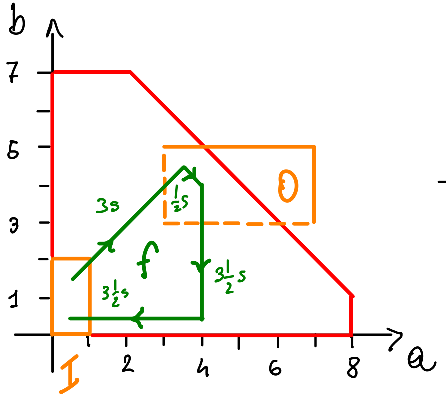


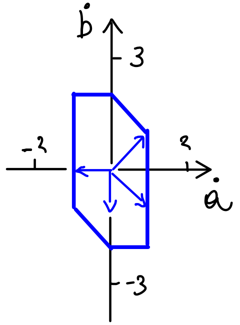
$$f(t) = \begin{cases} \left(\frac{1}{2}+t,\ 1\frac{1}{2}+t\right), & \text{if } t \in [0,3] \quad (3s) \\ \left(3\frac{1}{2}+t,\ 4\frac{1}{2}-t\right), & \text{if } t \in [3, 3\frac{1}{2}] \quad (\frac{1}{2}s) \\ \left(4,\ 4-t\right), & \text{if } t \in [3\frac{1}{2}, 7] \quad (3\frac{1}{2}s) \\ \left(4-t,\ \frac{1}{2}\right), & \text{if } t \in [7, 10\frac{1}{2}] \quad (3\frac{1}{2}s) \end{cases}$$

Trajectories & Signals

- **Trajectory**: A continuous function $f : I \subseteq \mathbb{R}_+ \longrightarrow \mathbb{R}^n$

  Time interval (I) · Time domain ($\mathbb{R}_+$) · State space ($\mathbb{R}^n$)





+ f is a trajectory in the Polyhedral System P if $\begin{cases} f(t) \in Inv \\ \dot{f}(t) \in Flow \end{cases} \quad \forall t \in I$

  finite number of discontinuities in any bounded subinterval $I' \subseteq I$

$$f(t) = \begin{cases} \left(\frac{1}{2}+t,\ 1\frac{1}{2}+t\right), & \text{if } t \in [0,3] \quad (3s) \\ \left(3\frac{1}{2}+t,\ 4\frac{1}{2}-t\right), & \text{if } t \in [3, 3\frac{1}{2}] \quad (\frac{1}{2}s) \\ \left(4,\ 4-t\right), & \text{if } t \in [3\frac{1}{2}, 7] \quad (3\frac{1}{2}s) \\ \left(4-t,\ \frac{1}{2}\right), & \text{if } t \in [7, 10\frac{1}{2}] \quad (3\frac{1}{2}s) \end{cases}$$

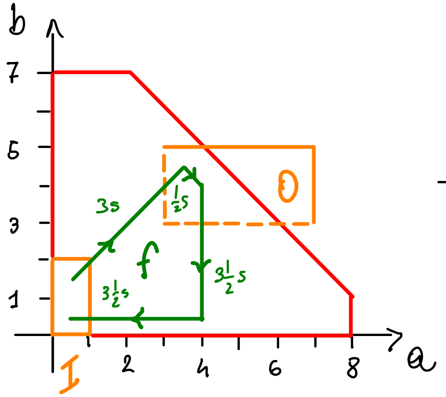
- **Signal** $\sigma : I \subseteq \mathbb{R}_+ \longrightarrow 2^{AP}$

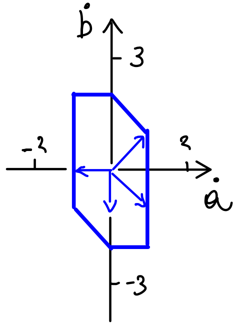
  Time interval (I) · Time domain ($\mathbb{R}_+$) · Atomic Proposition Space (2^{AP}) (Observables)

Trajectories & Signals

• **Trajectory**: A continuous function $f : I \subseteq \mathbb{R}_+ \longrightarrow \mathbb{R}^n$

Time interval (I), Time domain ($\mathbb{R}_+$), State space ($\mathbb{R}^n$)





+ f is a trajectory in the Polyhedral System P if $\begin{cases} f(t) \in Inv \\ \dot{f}(t) \in Flow \end{cases} \quad \forall t \in I$

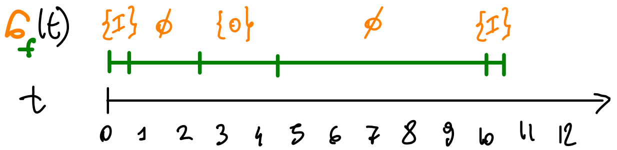
finite number of discontinuities in any bounded subinterval $I' \subseteq I$

$$f(t) = \begin{cases} \left(\tfrac{1}{2}+t,\ 1\tfrac{1}{2}+t\right), & \text{if } t \in [0,3] \quad (3s) \\ \left(3\tfrac{1}{2}+t,\ 4\tfrac{1}{2}-t\right), & \text{if } t \in [3, 3\tfrac{1}{2}] \quad (\tfrac{1}{2}s) \\ \left(4,\ 4-t\right), & \text{if } t \in [3\tfrac{1}{2}, 7] \quad (3\tfrac{1}{2}s) \\ \left(4-t,\ \tfrac{1}{2}\right), & \text{if } t \in [7, 10\tfrac{1}{2}] \quad (3\tfrac{1}{2}s) \end{cases}$$

• **Signal** $\sigma : I \subseteq \mathbb{R}_+ \longrightarrow 2^{AP}$

Time interval (I), Time domain ($\mathbb{R}_+$), Atomic Proposition Space (2^{AP}) (Observables)

• Every trajectory f has a corresponding signal σ_f!



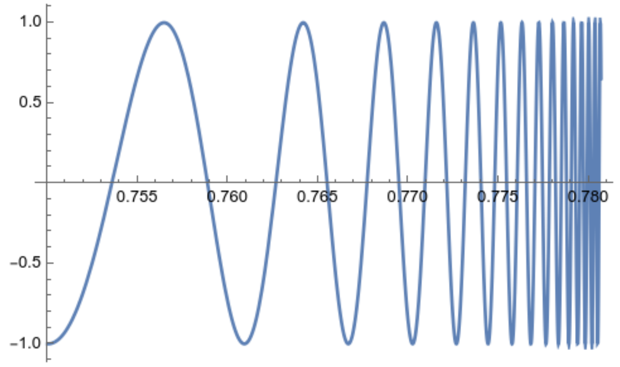
$$\sigma_f(t) = \begin{cases} \{I\}, & \text{if } t \in [0, \tfrac{1}{2}] \quad (\tfrac{1}{2}s) \\ \emptyset, & \text{if } t \in (\tfrac{1}{2}, 2\tfrac{1}{2}] \quad (2s) \\ \{O\}, & \text{if } t \in (2\tfrac{1}{2}, 4\tfrac{1}{2}) \quad (2s) \\ \emptyset, & \text{if } t \in [4\tfrac{1}{2}, 10) \quad (5\tfrac{1}{2}s) \\ \{I\}, & \text{if } t \in [10, 10\tfrac{1}{2}] \quad (\tfrac{1}{2}s) \end{cases}$$

Properties

- A trajectory $f : I \subseteq \mathbb{R}_+ \to \mathbb{R}^n$ is well-behaved if it crosses any hyperplane finitely many times in any bounded interval of time

- A signal $\sigma : I \subseteq \mathbb{R}_+ \to 2^{AP}$ has finite variability if it changes value finitely many times in any bounded interval of time

- Property : f is well-behaved $\Rightarrow$ σ_f has finite variability



$f(t) = \sin\left(\frac{1}{t}\right)$ ill-behaved

Real-Time Temporal Logic

RTL $\psi := \underbrace{\bot \mid \top}_{\text{Boolean values}} \mid \underbrace{p}_{\text{Atomic proposition}} \mid \underbrace{\neg\psi \mid \psi \wedge \psi \mid \psi \vee \psi}_{\text{Boolean connectives}} \mid$

vs LTL $\psi := \bot \mid \top \mid p \mid \neg\psi \mid \psi \wedge \psi \mid \psi \vee \psi \mid X\psi \mid \psi \,U\, \psi \mid \psi \,R\, \psi$

Real-Time Temporal Logic

$$\text{RTL} \quad \psi ::= \overbrace{\bot \mid \top}^{\text{Boolean values}} \mid \underbrace{p}_{\text{Atomic proposition}} \mid \overbrace{\neg\psi \mid \psi \land \psi \mid \psi \lor \psi}^{\text{Boolean connectives}} \mid \underbrace{\psi \,\dot{U}\, \psi \mid \psi \,\dot{R}\, \psi}_{\text{Temporal operators}}$$

vs

$$\text{LTL} \quad \psi ::= \bot \mid \top \mid p \mid \neg\psi \mid \psi \land \psi \mid \psi \lor \psi \mid X\psi \mid \psi \,U\, \psi \mid \psi \,R\, \psi$$

Real-Time Temporal Logic

$$\text{RTL}\quad \psi ::= \overbrace{\bot \mid \top}^{\text{Boolean values}} \mid \underbrace{p}_{\text{Atomic proposition}} \mid \overbrace{\neg\psi \mid \psi \wedge \psi \mid \psi \vee \psi}^{\text{Boolean connectives}} \mid \underbrace{\psi \,\dot{U}\, \psi \mid \psi \,\dot{R}\, \psi}_{\text{Temporal operators}} \quad \text{vs} \quad \text{LTL}\quad \psi ::= \bot \mid \top \mid p \mid \neg\psi \mid \psi \wedge \psi \mid \psi \vee \psi \mid X\psi \mid \psi U \psi \mid \psi R \psi$$

$$\sigma \models \psi_1 \,\dot{U}\, \psi_2 \quad \text{if} \quad \exists t_2 > 0 .\ \sigma_{\geq t_2} \models \psi_2 \ \text{and} \ \forall t_1 > 0,\ t_1 < t_2 .\ \sigma_{\geq t_1} \models \psi_1$$

Real-Time Temporal Logic

$$\text{RTL}\quad \psi ::= \overbrace{\bot \mid \top}^{\text{Boolean values}} \mid \underbrace{p}_{\text{Atomic Proposition}} \mid \overbrace{\neg\psi \mid \psi\wedge\psi \mid \psi\vee\psi}^{\text{Boolean connectives}} \mid \underbrace{\psi\, \dot{U}\, \psi \mid \psi\, \dot{R}\, \psi}_{\text{Temporal operators}} \qquad \text{vs} \qquad \text{LTL}\quad \psi ::= \bot \mid \top \mid p \mid \neg\psi \mid \psi\wedge\psi \mid \psi\vee\psi \mid X\psi \mid \psi\, U\, \psi \mid \psi\, R\, \psi$$

$$\sigma \models \psi_1\, \dot{U}\, \psi_2 \quad \text{if} \quad \exists\, t_2 > 0 \,.\; \sigma_{\geq t_2} \models \psi_2 \quad \text{and} \quad \forall\, t_1 > 0,\; t_1 < t_2 \,.\; \sigma_{\geq t_1} \models \psi_1$$

differences w.r.t. classic until U

$$\psi_1\, U\, \psi_2 \triangleq \psi_2 \vee \psi_1 \wedge (\psi_1\, \dot{U}\, \psi_2)$$

Real-Time Temporal Logic

$$\text{RTL} \quad \psi ::= \overbrace{\bot \mid \top}^{\text{Boolean values}} \mid \underbrace{p}_{\text{Atomic proposition}} \mid \overbrace{\neg\psi \mid \psi \wedge \psi \mid \psi \vee \psi}^{\text{Boolean connectives}} \mid \underbrace{\psi \,\dot{U}\, \psi \mid \psi \,\dot{R}\, \psi}_{\text{Temporal operators}}$$

vs

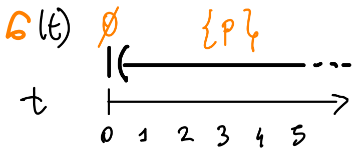
$$\text{LTL} \quad \psi ::= \bot \mid \top \mid p \mid \neg\psi \mid \psi \wedge \psi \mid \psi \vee \psi \mid X\psi \mid \psi \,U\, \psi \mid \psi \,R\, \psi$$

$$\sigma \models \psi_1 \,\dot{U}\, \psi_2 \quad \text{if} \quad \exists\, t_2 > 0 .\ \sigma_{\geq t_2} \models \psi_2 \ \text{ and } \ \forall\, t_1 > 0,\ t_1 < t_2 .\ \sigma_{\geq t_1} \models \psi_1$$

differences w.r.t. classic until U

$$\psi_1 \,U\, \psi_2 \triangleq \psi_2 \vee \psi_1 \wedge (\psi_1 \,\dot{U}\, \psi_2)$$

$$\sigma_f \models \neg p \wedge (p \,\dot{U}\, p)$$



$$\sigma(t) = \begin{cases} \emptyset, & \text{if } t = 0 \\ \{p\}, & \text{if } t > 0 \end{cases}$$

Real-Time Temporal Logic

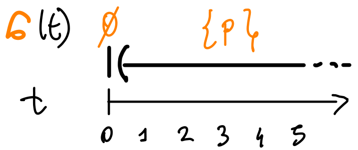
RTL $\psi ::= \overbrace{\bot \mid \top}^{\text{Boolean values}} \mid \underbrace{p}_{\text{Atomic proposition}} \mid \overbrace{\neg\psi \mid \psi \wedge \psi \mid \psi \vee \psi}^{\text{Boolean connectives}} \mid \underbrace{\psi \dot{U} \psi \mid \psi \dot{R} \psi}_{\text{Temporal operators}}$ vs LTL $\psi ::= \bot \mid \top \mid p \mid \neg\psi \mid \psi \wedge \psi \mid \psi \vee \psi \mid X\psi \mid \psi U \psi \mid \psi R \psi$

$\sigma \models \psi_1 \dot{U} \psi_2$ if $\exists t_2 > 0 .\ \sigma_{\geq t_2} \models \psi_2$ and $\forall t_1 > 0,\ t_1 < t_2 .\ \sigma_{\geq t_1} \models \psi_1$

differences w.r.t. classic until U

$$\psi_1 U \psi_2 \triangleq \psi_2 \vee \psi_1 \wedge (\psi_1 \dot{U} \psi_2)$$

$\sigma_f \models \neg p \wedge (p \dot{U} p)$



$$\sigma(t) = \begin{cases} \emptyset, & \text{if } t = 0 \\ \{p\}, & \text{if } t > 0 \end{cases}$$

- Note that RTL cannot enforce any requirement on the duration of the intervals, i.e., it is not metric!

The Model-Checking Problems

Polyhedral Systems as Trajectory Generators

- Given $\mathrm{Traj}(\mathcal{P})$ the set of all well-behaved trajectories in the Polyhedral System $\mathcal{P}$:

Polyhedral Systems as Trajectory Generators

- Given $\mathrm{Traj}(\mathcal{P})$ the set of all well-behaved trajectories in the Polyhedral System $\mathcal{P}$:

  + $\mathrm{Traj}^f(\mathcal{P}) \subseteq \mathrm{Traj}(\mathcal{P})$ subset of finite-time trajectories,
    i.e., with bounded domain interval

Polyhedral Systems as Trajectory Generators

- Given $\mathrm{Traj}(\mathcal{P})$ the set of all well-behaved trajectories in the Polyhedral System $\mathcal{P}$:

  + $\mathrm{Traj}^{f}(\mathcal{P}) \subseteq \mathrm{Traj}(\mathcal{P})$ subset of finite-time trajectories, i.e., with bounded domain interval

  + $\mathrm{Traj}^{m}_{max}(\mathcal{P}) \subseteq \mathrm{Traj}(\mathcal{P})$ subset of may-maximal trajectories, i.e., trajectories that can immediately exit the invariant Inv

Polyhedral Systems as Trajectory Generators

- Given $Traj(\mathcal{P})$ the set of all well-behaved trajectories in the Polyhedral System $\mathcal{P}$:

  + $Traj^{f}(\mathcal{P}) \subseteq Traj(\mathcal{P})$ subset of finite-time trajectories,
    i.e., with bounded domain interval

  + $Traj^{m}_{max}(\mathcal{P}) \subseteq Traj(\mathcal{P})$ subset of may-maximal trajectories,
    i.e., trajectories that can immediately exit the invariant Inv

  + $Traj^{M}_{max}(\mathcal{P}) \subseteq Traj(\mathcal{P})$ subset of must-maximal trajectories,
    i.e., trajectories that cannot be extended without exiting the invariant Inv

Polyhedral Systems as Trajectory Generators

- Given $Traj(\mathcal{P})$ the set of all well-behaved trajectories in the Polyhedral System $\mathcal{P}$:

  + $Traj^{f}(\mathcal{P}) \subseteq Traj(\mathcal{P})$ subset of finite-time trajectories,
    i.e., with bounded domain interval

  + $Traj^{m}_{max}(\mathcal{P}) \subseteq Traj(\mathcal{P})$ subset of may-maximal trajectories, ⟵ can model guard activation in a hybrid automaton
    i.e., trajectories that can immediately exit the invariant Inv

  + $Traj^{M}_{max}(\mathcal{P}) \subseteq Traj(\mathcal{P})$ subset of must-maximal trajectories, ⟵ can model best-effort control strategies
    i.e., trajectories that cannot be extended without exiting the invariant Inv

Model-Checking Problems

- Given $\Bigg\{$

Model-Checking Problems

- Given $\left\{ \text{a Polyhedral System } P, \right.$

Model-Checking Problems

- Given $\begin{cases} \text{a Polyhedral System } \mathcal{P}, \\ \text{an RTL formula } \varphi, \text{ and} \\ \end{cases}$

Model-Checking Problems

- Given $\begin{cases} \text{a Polyhedral System } \mathcal{P}, \\ \text{an RTL formula } \Psi, \text{ and} \\ \text{a trajectory-semantic flag } \alpha \in \{ f, \overset{m}{\max}, \overset{M}{\max} \}, \end{cases}$

Model-Checking Problems

- Given $\begin{cases} \text{a Polyhedral System } \mathcal{P}, \\ \text{an RTL formula } \varphi, \text{ and} \\ \text{a trajectory-semantic flag } \alpha \in \{f, \overset{m}{max}, \overset{M}{max}\}, \end{cases}$

compute the set $[\![\varphi]\!]_{\mathcal{P}} \subseteq \mathbb{R}^n$ of points $x \in \mathbb{R}^n$ in the state space s.t.

Model-Checking Problems

- Given $\begin{cases} \text{a Polyhedral System } \mathcal{P}, \\ \text{an RTL formula } \Psi, \text{ and} \\ \text{a trajectory-semantic flag } \alpha \in \{ f, \overset{m}{\max}, \overset{M}{\max} \}, \end{cases}$

Compute the set $[\![\Psi]\!]_{\mathcal{P}} \subseteq \mathbb{R}^n$ of points $x \in \mathbb{R}^n$ in the state space s.t.

+ (Existential Problem) $\exists\, f \in Traj^{\alpha}(\mathcal{P}),\ \underbrace{f \text{ starts in } x}_{f(0)=x} \,.\ \sigma_f \models \Psi$

+ (Universal Problem) $\forall\, f \in Traj^{\alpha}(\mathcal{P}),\ \overbrace{f \text{ starts in } x}^{f(0)=x} \,.\ \sigma_f \models \Psi$

Interreducible

Model Checking PolyF against RTLF

Signal Discretisation I

- A time-slicing $\tau = \{t_i \in I\}_i$ for a signal $\sigma : I \subseteq \mathbb{R}_+ \longrightarrow 2^{AP}$ is a sequence of time instants in I s.t.
  a) $\inf(I) = t_0 < t_1 < \cdots < t_k = \sup(I)$
  b) the observable $\sigma(t)$ is constant in any interval (t_i, t_{i+1})
  c) no accumulation point in τ

Signal Discretisation I

- A time-slicing $\tau = \{t_i \in I\}_i$ for a signal $\sigma : I \subseteq \mathbb{R}_+ \longrightarrow 2^{AP}$ is a sequence of time instants in I s.t.
  a) $\inf(I) = t_0 < t_1 < \cdots < t_K = \sup(I)$
  b) the observable $\sigma(t)$ is constant in any interval (t_i, t_{i+1})
  c) no accumulation point in τ

- Property: σ has finite variability $\iff$ σ has at least one time-slicing τ

Signal Discretisation I

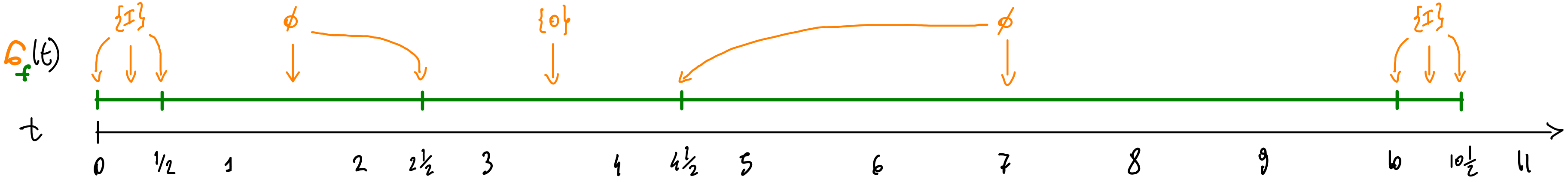
- A a time-slicing $\tau = \{t_i \in I\}_i$ for a signal $\sigma : I \subseteq \mathbb{R}_+ \longrightarrow 2^{AP}$ is a sequence of time instants in I s.t.
  a) $\inf(I) = t_0 < t_1 < \cdots < t_k = \sup(I)$
  b) the observable $\sigma(t)$ is constant in any interval (t_i, t_{i+1})
  c) no accumulation point in τ

- Property: σ has finite variability $\Longleftrightarrow$ σ has at least one time-slicing τ

- $\text{trace}(\sigma, \tau) \in 2^{AP \cup \{\text{SING}\}}$ $\begin{cases} \text{to every time instant } t_i, \text{ we associate the labelling } \sigma(t_i) \cup \{\text{SING}\} \\ \text{to every interval } (t_i, t_{i+1}), \text{ we associate the labelling } \sigma(t) \text{ with } t \in (t_i, t_{i+1}) \end{cases}$

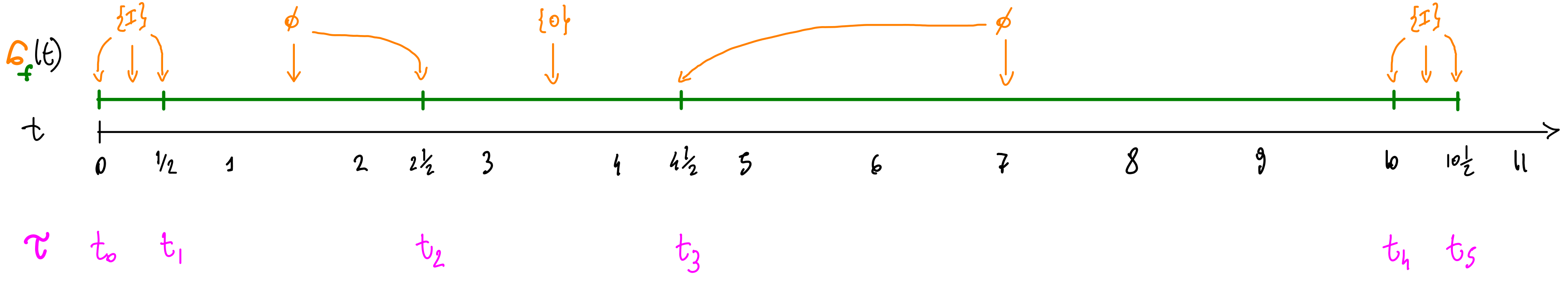
Signal Discretisation II

$$\sigma_f(t) = \begin{cases} \{I\}, & \text{if } t \in [0, \tfrac{1}{2}] & (\tfrac{1}{2}s) \\ \emptyset, & \text{if } t \in (\tfrac{1}{2}, 2\tfrac{1}{2}] & (2s) \\ \{0\}, & \text{if } t \in (2\tfrac{1}{2}, 4\tfrac{1}{2}) & (2s) \\ \emptyset, & \text{if } t \in [4\tfrac{1}{2}, 10) & (5\tfrac{1}{2}s) \\ \{I\}, & \text{if } t \in [10, 10\tfrac{1}{2}] & (\tfrac{1}{2}s) \end{cases}$$



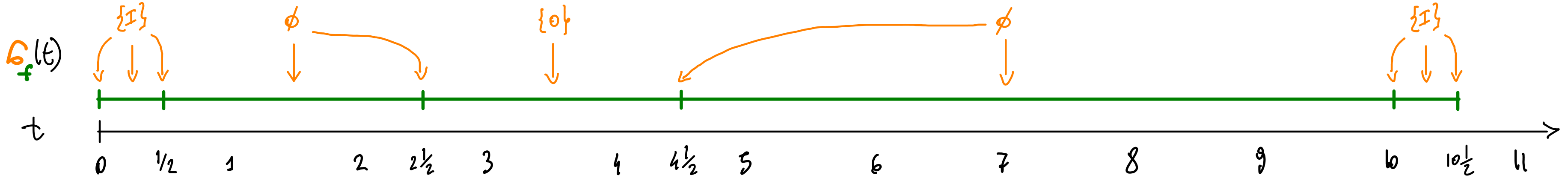
Signal Discretisation II

$$\sigma_f(t) = \begin{cases} \{I\}, & \text{if } t \in [0, \tfrac{1}{2}] \quad (\tfrac{1}{2}s) \\ \emptyset, & \text{if } t \in (\tfrac{1}{2}, 2\tfrac{1}{2}] \quad (2s) \\ \{O\}, & \text{if } t \in (2\tfrac{1}{2}, 4\tfrac{1}{2}) \quad (2s) \\ \emptyset, & \text{if } t \in [4\tfrac{1}{2}, 10) \quad (5\tfrac{1}{2}s) \\ \{I\}, & \text{if } t \in [10, 10\tfrac{1}{2}] \quad (\tfrac{1}{2}s) \end{cases}$$



Signal Discretisation II

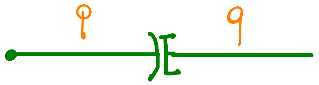
$$\sigma_f(t) = \begin{cases} \{I\}, & \text{if } t \in [0, \tfrac{1}{2}] \quad (\tfrac{1}{2}s) \\ \emptyset, & \text{if } t \in (\tfrac{1}{2}, 2\tfrac{1}{2}] \quad (2s) \\ \{O\}, & \text{if } t \in (2\tfrac{1}{2}, 4\tfrac{1}{2}) \quad (2s) \\ \emptyset, & \text{if } t \in [4\tfrac{1}{2}, 10) \quad (5\tfrac{1}{2}s) \\ \{I\}, & \text{if } t \in [10, 10\tfrac{1}{2}] \quad (\tfrac{1}{2}s) \end{cases}$$



τ	t_0		t_1		t_2		t_3		t_4		t_5
$tree(\sigma_f, \tau)$	W_0	W_1	W_2	W_3	W_4	W_5	W_6	W_7	W_8	W_9	W_{10}
	$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$
$APo\{SING\} \supseteq$	$\begin{Bmatrix}SING\\ I\end{Bmatrix}$	$\{I\}$	$\begin{Bmatrix}SING\\ I\end{Bmatrix}$	$\emptyset$	$\{SING\}$	$\{O\}$	$\{SING\}$	$\emptyset$	$\begin{Bmatrix}SING\\ I\end{Bmatrix}$	$\{I\}$	$\begin{Bmatrix}SING\\ I\end{Bmatrix}$

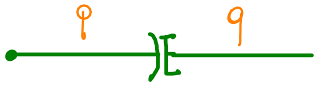
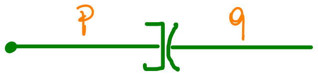
Formula Discretisation

$\sigma \models \psi \in \mathrm{RTL}$ $\qquad$ $\mathit{tree}(\sigma, \tau) \models \mathit{disc}(\psi) \in \mathrm{LTL}$

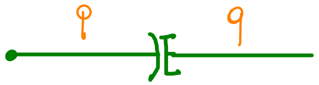
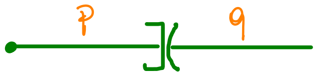
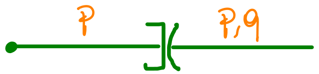


$\models p \, \mathsf{U} \, q$ $\qquad$ $\{p\}\{q, \mathit{sing}\}\{q\} \models p \, \mathsf{U} \, (q \wedge \mathit{sing})$

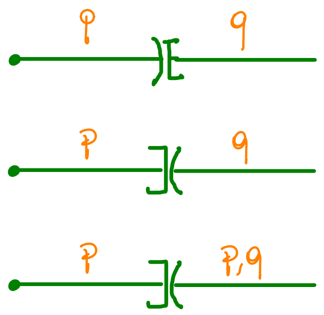
Formula Discretisation

σ	$\models \psi \in \mathrm{RTL}$	$\mathrm{trace}(\sigma, \tau)$	$\models \mathrm{disc}(\psi) \in \mathrm{LTL}$
	$\models p \,\mathcal{U}\, q$	$\{p\}\{q, \mathrm{SING}\}\{q\}$	$\models p \,\mathcal{U}\, (q \land \mathrm{SING})$
	$\not\models p \,\mathcal{U}\, q$	$\{p\}\{p, \mathrm{SING}\}\{q\}$	$\not\models p \,\mathcal{U}\, (q \land \mathrm{SING})$

Formula Discretisation

σ	$\models \psi \in \mathrm{RTL}$	$\mathrm{tree}(\sigma, \tau)$	$\models \mathrm{disc}(\psi) \in \mathrm{LTL}$
	$\models p \, \mathcal{U} \, q$	$\{p\}\{q, \mathrm{SING}\}\{q\}$	$\models p \, \mathcal{U} \, (q \wedge \mathrm{SING})$
	$\not\models p \, \mathcal{U} \, q$	$\{p\}\{p, \mathrm{SING}\}\{q\}$	$\not\models p \, \mathcal{U} \, (q \wedge \mathrm{SING})$
	$\models p \, \mathcal{U} \, q$	$\{p\}\{p, \mathrm{SING}\}\{p, q\}$	$\models p \, \mathcal{U} \, (q \wedge p)$

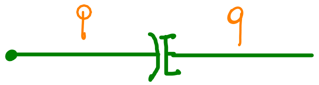
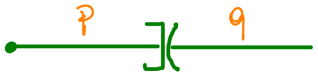
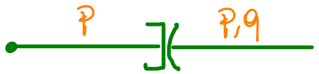
FORMULA DISCRETISATION



σ	$\models \psi \in RTL$	$tree(\sigma, \tau)$	$\models disc(\psi) \in LTL$
1	$\models p\,\mathcal{U}\,q$	$\{p\}\{q, SING\}\{q\}$	$\models p\,\mathcal{U}(q \wedge SING)$
2	$\not\models p\,\mathcal{U}\,q$	$\{p\}\{p, SING\}\{q\}$	$\not\models p\,\mathcal{U}(q \wedge SING)$
3	$\models p\,\mathcal{U}\,q$	$\{p\}\{p, SING\}\{p, q\}$	$\models p\,\mathcal{U}(q \wedge p)$

$$p\,\mathcal{U}\,(q \wedge (p \vee SING))$$

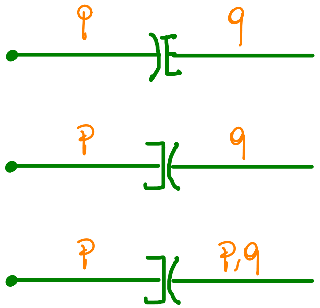
Formula Discretisation

σ	$\models \psi \in RTL$	$trace(\sigma, \tau)$	$\models disc(\psi) \in LTL$
	$\models p \, U \, q$	$\{p\}\{q, SING\}\{q\}$	$\models p \, U (q \wedge SING)$
	$\not\models p \, U \, q$	$\{p\}\{p, SING\}\{q\}$	$\not\models p \, U (q \wedge SING)$
	$\models p \, U \, q$	$\{p\}\{p, SING\}\{p, q\}$	$\models p \, U (q \wedge p)$

$$\Big\} \; p \, U \big(q \wedge (p \vee SING)\big)$$

One $\longleftarrow$- - - $p \, \dot{U} \, q$ behaves as $p \, U \, q$ on the same signal

Formula Discretisation

σ	$\models \psi \in RTL$	$trace(\sigma, \tau)$	$\models disc(\psi) \in LTL$
	$\models p \, U \, q$	$\{p\}\{q, sing\}\{q\}$	$\models p \, U (q \wedge sing)$
	$\not\models p \, U \, q$	$\{p\}\{p, sing\}\{q\}$	$\not\models p \, U (q \wedge sing)$
	$\models p \, U \, q$	$\{p\}\{p, sing\}\{p, q\}$	$\models p \, U (q \wedge p)$

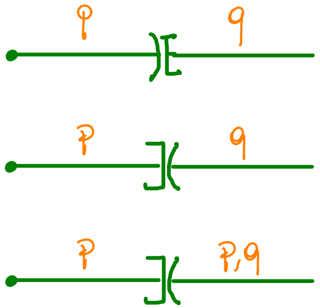
$\left.\begin{array}{l} p \, U (q \wedge sing) \\ p \, U (q \wedge sing) \\ p \, U (q \wedge p) \end{array}\right\} p \, U (q \wedge (p \vee sing))$

On (——--- $p \, \dot{U} \, q$ behaves as $p \, U \, q$ on the same signal

On [——--- $p \, \dot{U} \, q$ behaves as $p \, U \, q$ on (——---

Formula Discretisation

σ	$\models \varphi \in RTL$	$tree(\sigma, \tau)$	$\models disc(\varphi) \in LTL$



$\models p \, U \, q$	$\{p\}\{q, \text{SING}\}\{q\} \models$	$p \, U (q \wedge \text{SING})$
$\not\models p \, U \, q$	$\{p\}\{p, \text{SING}\}\{q\} \not\models$	$p \, U (q \wedge \text{SING})$
$\models p \, U \, q$	$\{p\}\{p, \text{SING}\}\{p, q\} \models$	$p \, U (q \wedge p)$

$$\Big\} \; p \, U (q \wedge (p \vee \text{SING}))$$

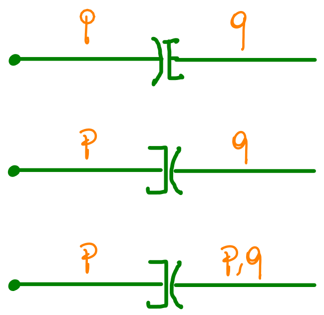
On $(\longleftarrow$--- $p \, \dot{U} \, q$ behaves as $p \, U \, q$ on the same signal

On $[\longleftarrow$--- $p \, \dot{U} \, q$ behaves as $p \, U \, q$ on $(\longleftarrow$---

$$\Big\} \; \begin{array}{l} \neg\text{SING} \wedge disc(p \, U \, q) \\ \vee \\ \text{SING} \wedge X \, disc(p \, U \, q) \end{array}$$

Formula Discretisation

σ	$\models \psi \in \mathrm{RTL}$	$tree(\sigma, \tau)$	$\models disc(\psi) \in \mathrm{LTL}$



$\models$	$p\,\mathcal{U}\,q$	$\{p\}\{q, \mathrm{SING}\}\{q\} \models$	$p\,\mathcal{U}(q \wedge \mathrm{SING})$
$\not\models$	$p\,\mathcal{U}\,q$	$\{p\}\{p, \mathrm{SING}\}\{q\} \not\models$	$p\,\mathcal{U}(q \wedge \mathrm{SING})$
$\models$	$p\,\mathcal{U}\,q$	$\{p\}\{p, \mathrm{SING}\}\{p, q\} \models$	$p\,\mathcal{U}(q \wedge p)$

$\Rightarrow p\,\mathcal{U}(q \wedge (p \vee \mathrm{SING}))$

On (———--- $p\,\dot{\mathcal{U}}\,q$ behaves as $p\,\mathcal{U}\,q$ on the same signal

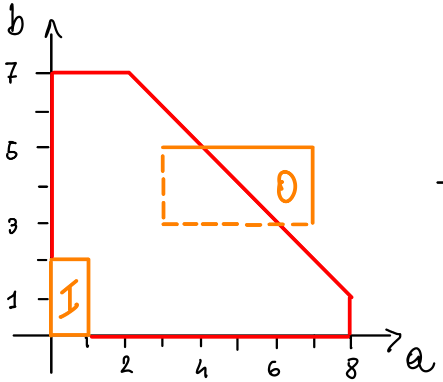
On [———--- $p\,\dot{\mathcal{U}}\,q$ behaves as $p\,\mathcal{U}\,q$ on (———---

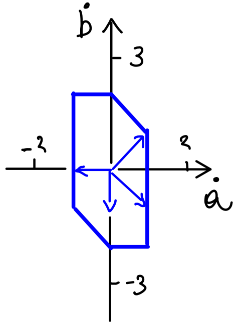
$$\neg\mathrm{SING} \wedge disc(p\,\mathcal{U}\,q) \;\vee\; \mathrm{SING} \wedge X\, disc(p\,\mathcal{U}\,q)$$

- Theorem: $\sigma \models \psi \in \mathrm{RTL}$ iff $tree(\sigma, \tau) \models disc(\psi) \in \mathrm{LTL}$ $\forall$ time-slicing τ of σ

Example

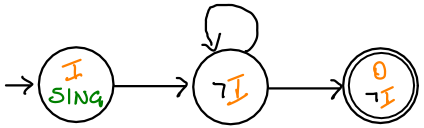
$$\psi = I \land (\neg I \,\dot{U}\, O) \;\mapsto\; disc(\psi) = I \land \textsc{sing} \land X(\neg I \,U\, (O \land \neg I))$$

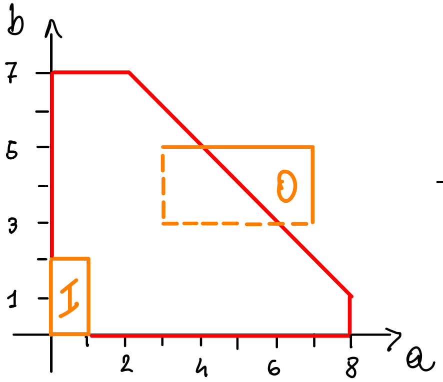


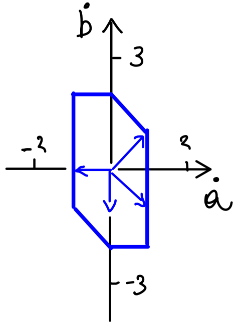


Example

$$\psi = I \wedge (\neg I \,\dot{U}\, O) \;\mapsto\; \mathit{dise}(\psi) = I \wedge \mathrm{SING} \wedge X(\neg I \,U\, (O \wedge \neg I))$$

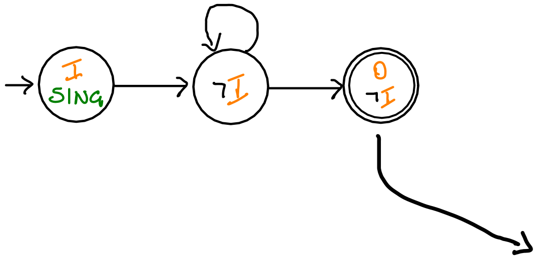


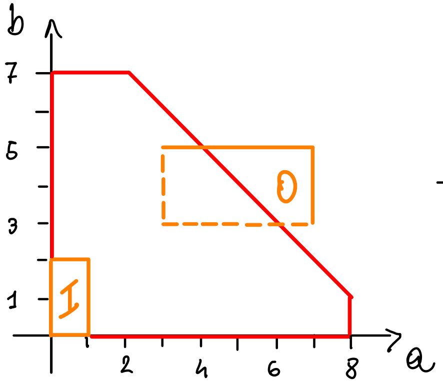


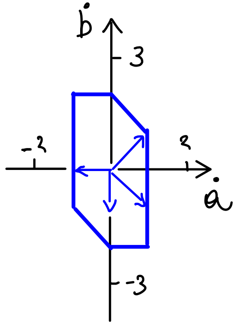


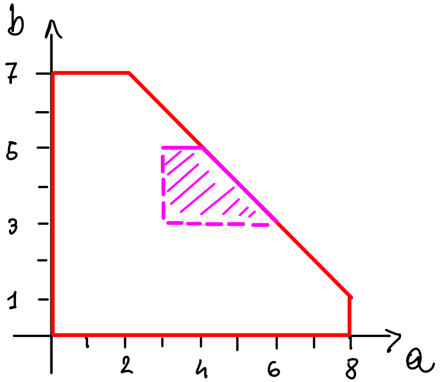
Example

$$\psi = I \wedge (\neg I \,\dot{\mathsf{U}}\, O) \mapsto \mathit{disc}(\psi) = I \wedge \mathrm{SING} \wedge \mathsf{X}(\neg I \,\mathsf{U}\, (O \wedge \neg I))$$



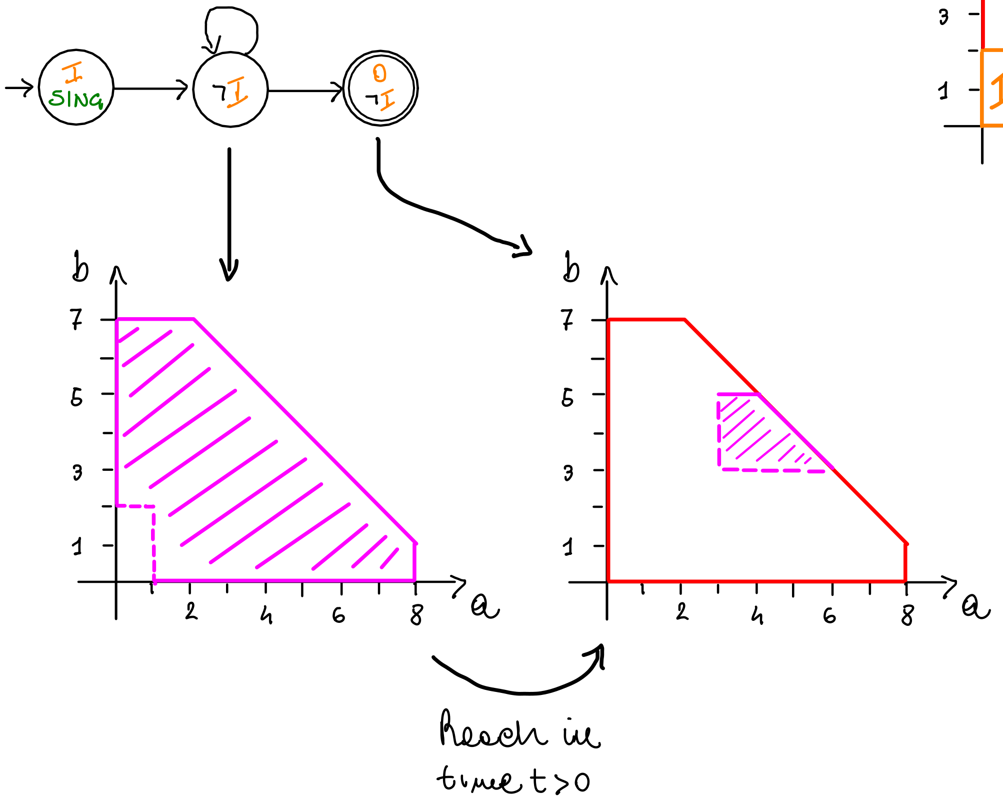


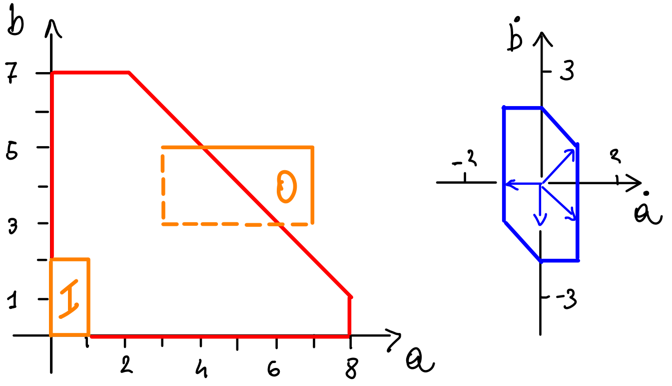




Example

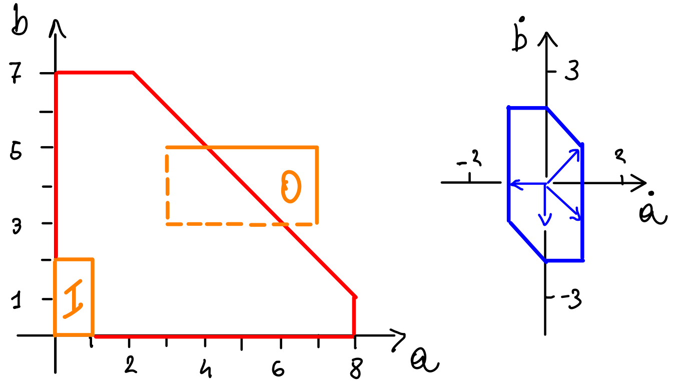
$\psi = I \wedge (\neg I \,\dot{U}\, O) \;\mapsto\; disc(\psi) = I \wedge SING \wedge X(\neg I \,U\, (O \wedge \neg I))$

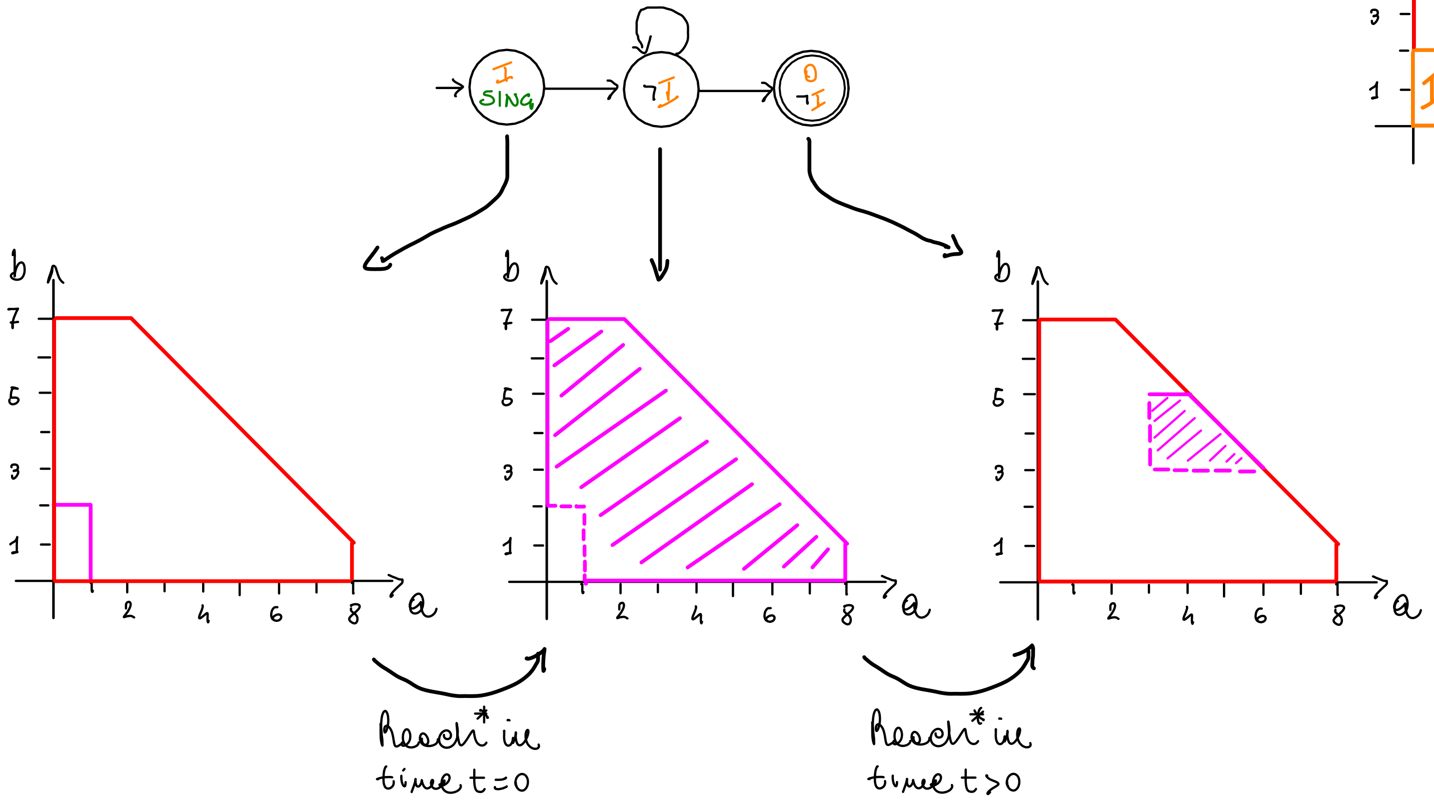




Example

$$\psi = I \wedge (\neg I \,\dot{U}\, O) \;\mapsto\; \mathrm{disc}(\psi) = I \wedge \mathrm{SING} \wedge X(\neg I \,U\, (O \wedge \neg I))$$





* defined in

Benerecetti, Faella, Minopoli TCS'13

Automatic Synthesis of Switching Controllers for LHS: Safety Control

Thank You Very Much