Optimal and Robust controller Synthesis

Using Energy Timed Automata with Uncertainty

Giovanni Bacci, Patricia Bouyer, Uli Fahrenberg,
Kim G. Larsen, Nicolas Markey, Pierre-Alain Reynier

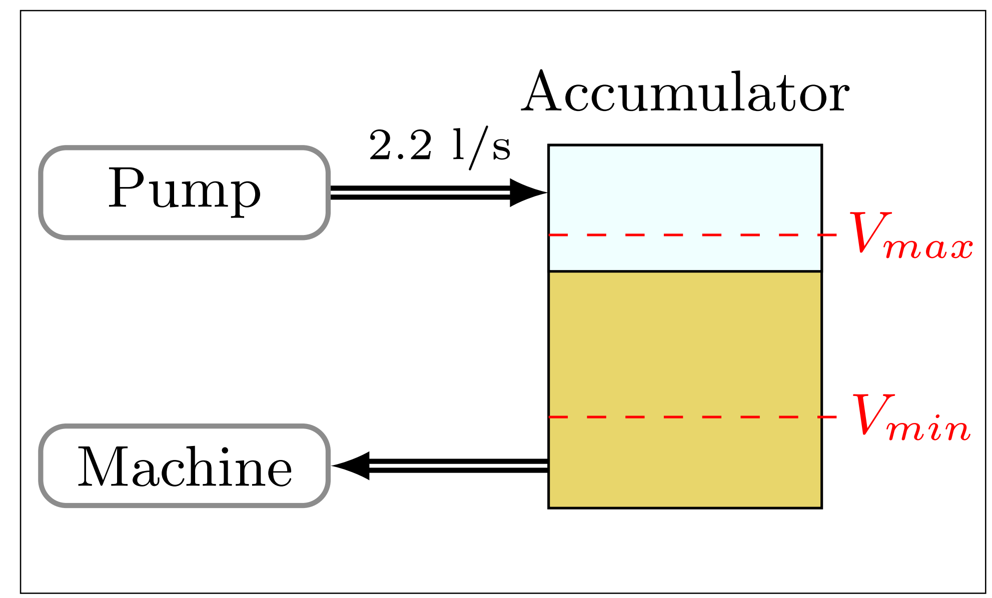
Presentation based on a paper accepted for publication at Formal Methods (FM'18)

Work supported by ERC projects LASSO and EQualIS

Industrial Example:
the HYDAC system

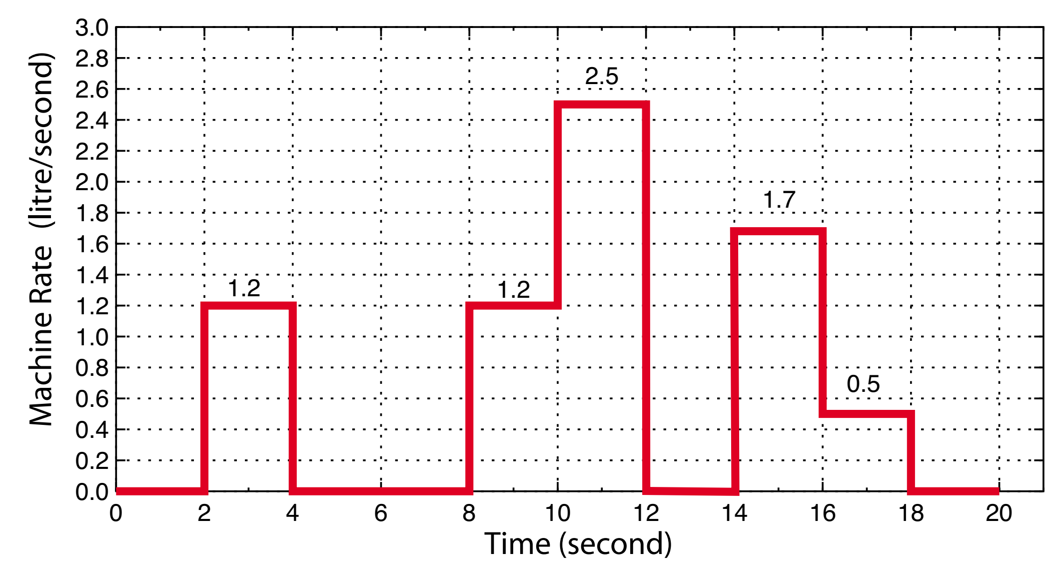
System components

- A **machine** that consumes oil according to a fixed cyclic pattern of 20 s
- Hydraulic **accumulator** containing oil and a fixed amount of gas that puts the oil under pressure
- **Controllable pump** (on/off) which pumps oil into the accumulator with rate 2.2 l/s



The control objective

- The level of oil shall be maintained within a **safe interval** [V_{max}; V_{min}] = [4.9; 25.1] l
- The system shall **never stop**
- The controller shall **minimise the average level of oil** so that the oil pressure is kept as low as possible



Cassez, Jensen, Larsen, Raskin, Reyner - Automatic Synthesis of Robust and Optimal Controllers (HSCC'09)

Motivation

- Automatic synthesis of controllers for embedded systems is a difficult task
- They need to satisfy safety properties involving non-functional aspects such as time constraints and limited resources
- While ensuring optimality w.r.t. given performance objectives

Energy constraints

GOMSPACE

picture taken from gomspace.com

Our contribution

- Novel framework for **automatic synthesis of safe & optimal controllers** for **resource-aware** systems modelled as **energy timed automata**
- Controller synthesis are obtained by solving **time- and energy-constrained infinite run problems**
- We address an open problem from [Bouyer, Fahrenberg, Larsen, Markey, Srba — FORMATS'08]

Context

Untimed

	games	existential problem	universal problem
L	$\in$ UP $\cap$ coUP P-h	$\in$ P	$\in$ P
L+W	$\in$ NP $\cap$ coNP P-h	$\in$ P	$\in$ P
L+U	EXPTIME-c	$\in$ PSPACE NP-h	$\in$ P

1 Clock

	games	existential problem	universal problem
L	?	$\in$ P	$\in$ P
L+W	?	$\in$ P	$\in$ P
L+U	undecidable	?	?

Bouyer, Fahrenberg, Larsen, Markey, Srba — Infinite Runs in Weighted Timed Automata with Energy Constraints (FORMATS'08)

Energy Timed Automata

Finite set of clocks

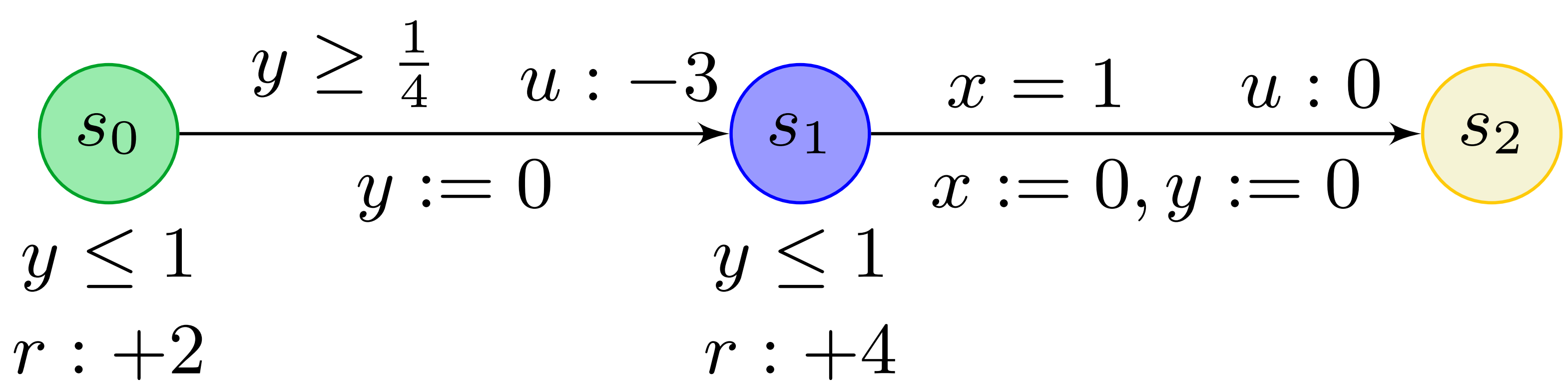
Clock invariants $I : S \to C(X)$

$$A = (S, S_0, X, I, r, T)$$

Finite set of states

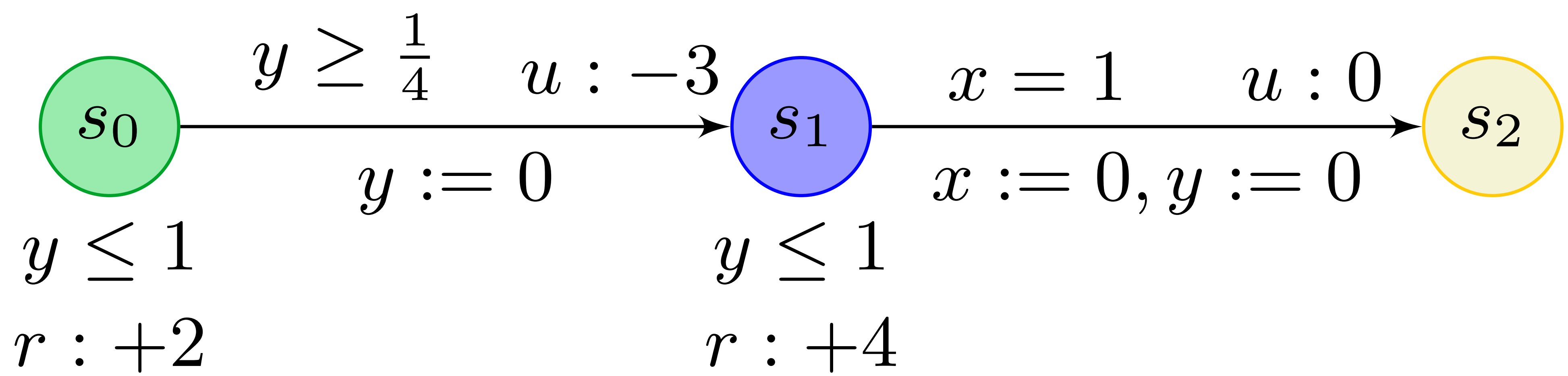
Rate assignment $r : S \to \mathbb{Q}$

Transition relation $T \subseteq S \times C(X) \times \mathbb{Q} \times 2^X \times S$

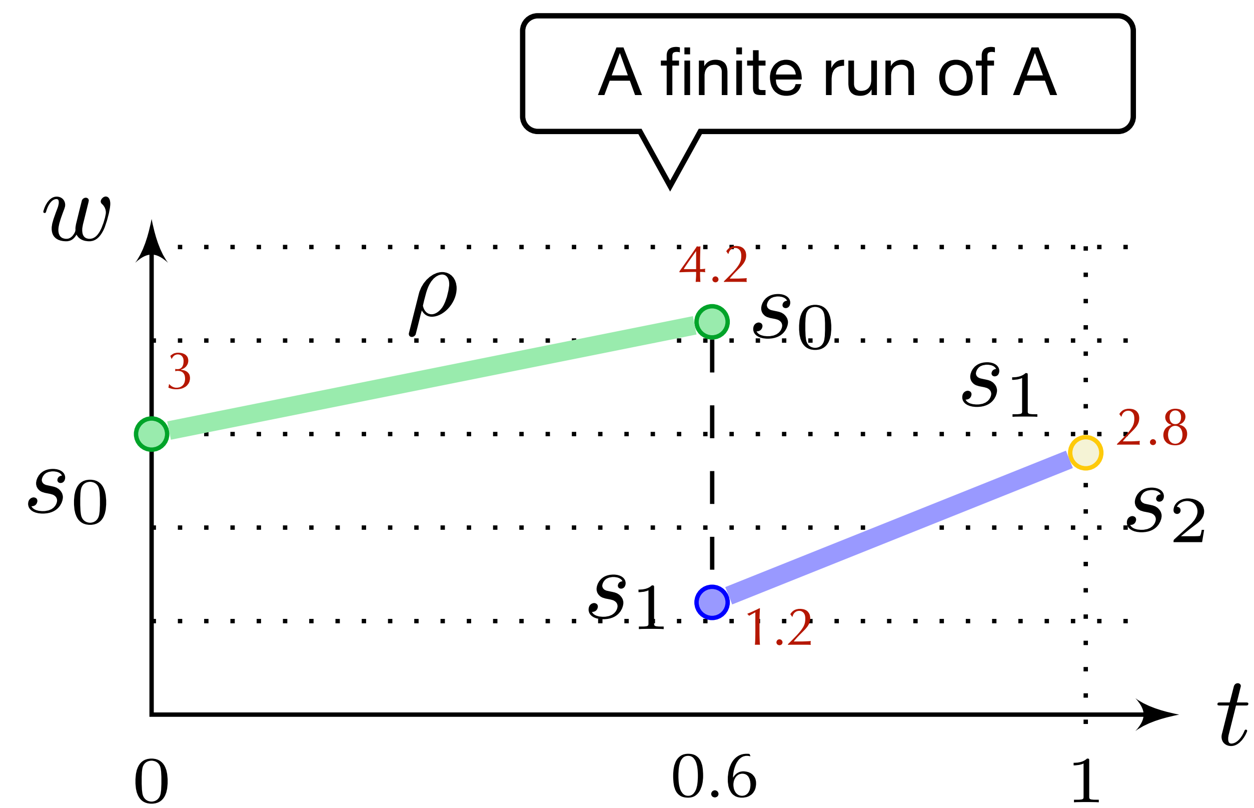


An ETA is an **Energy Timed Path (ETP)** when "it looks like a chain" and all *clocks are reset on the last transition*

Energy Timed Automata



An ETA generates runs (i.e., sequences of configurations) describing how the clocks and the energy level evolves over time



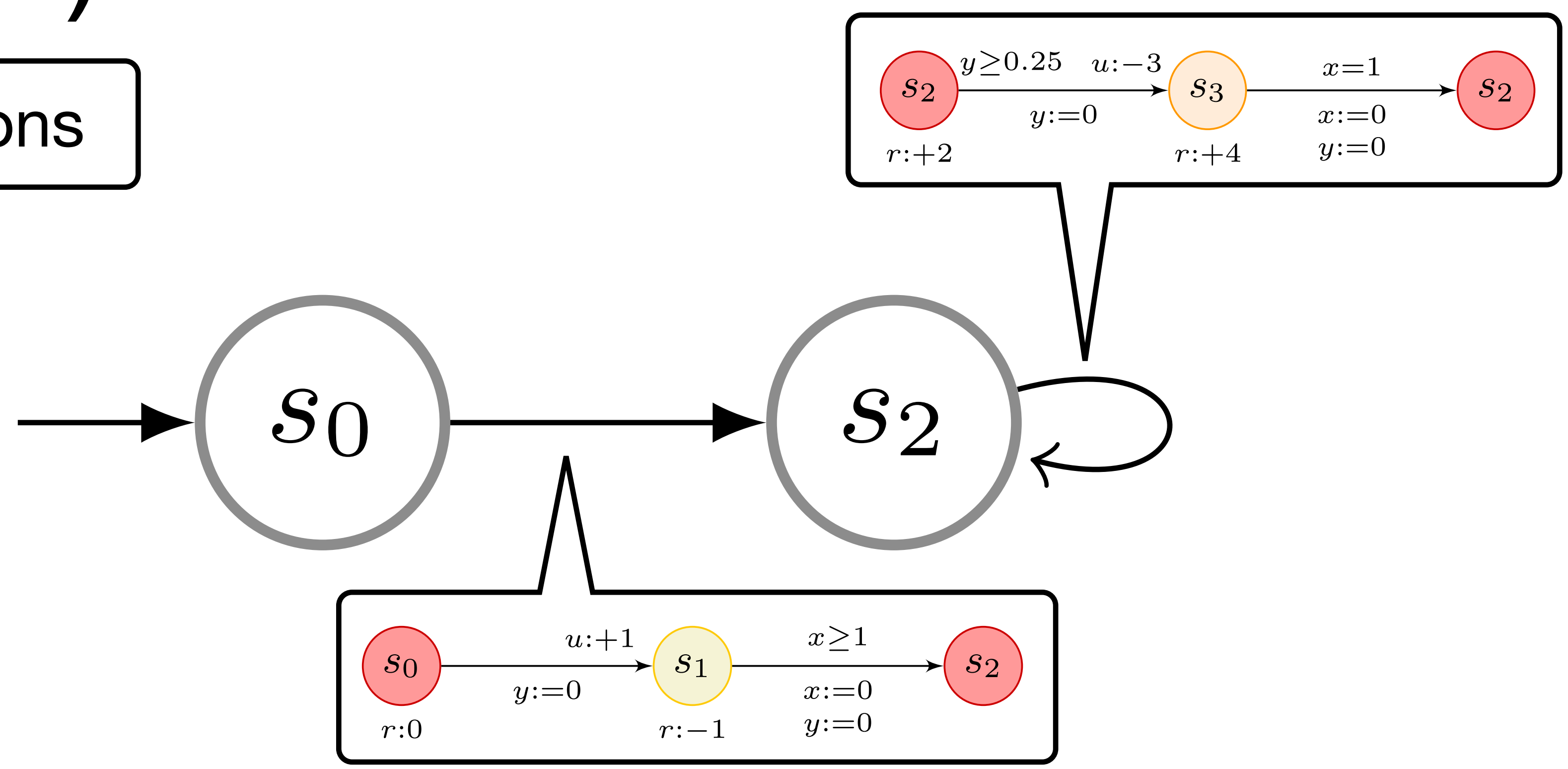
Segmented ETA

macro-states

Transition labels
$P : T \rightarrow ETP$

$A = (S,T,P)$

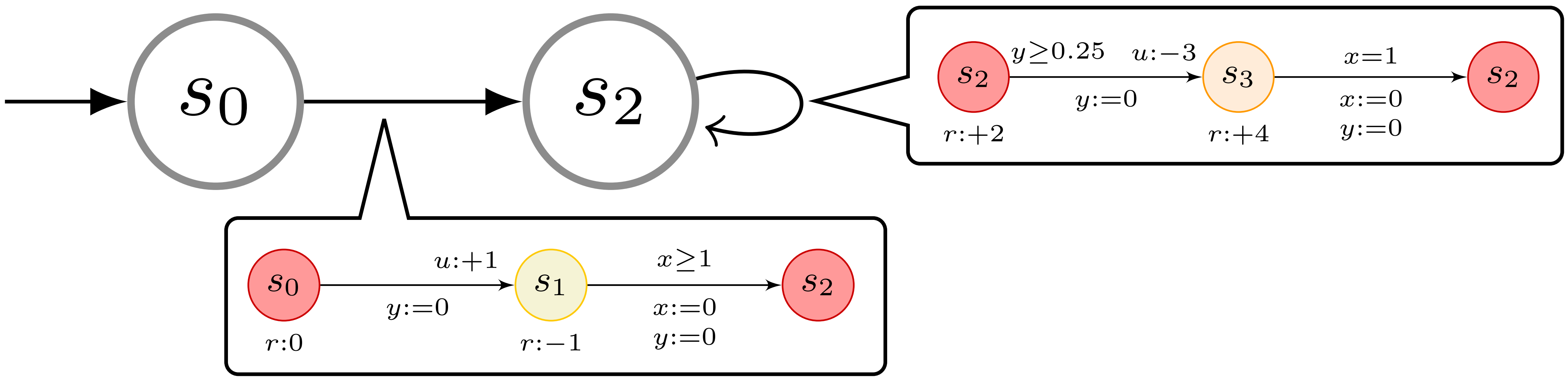
Transitions



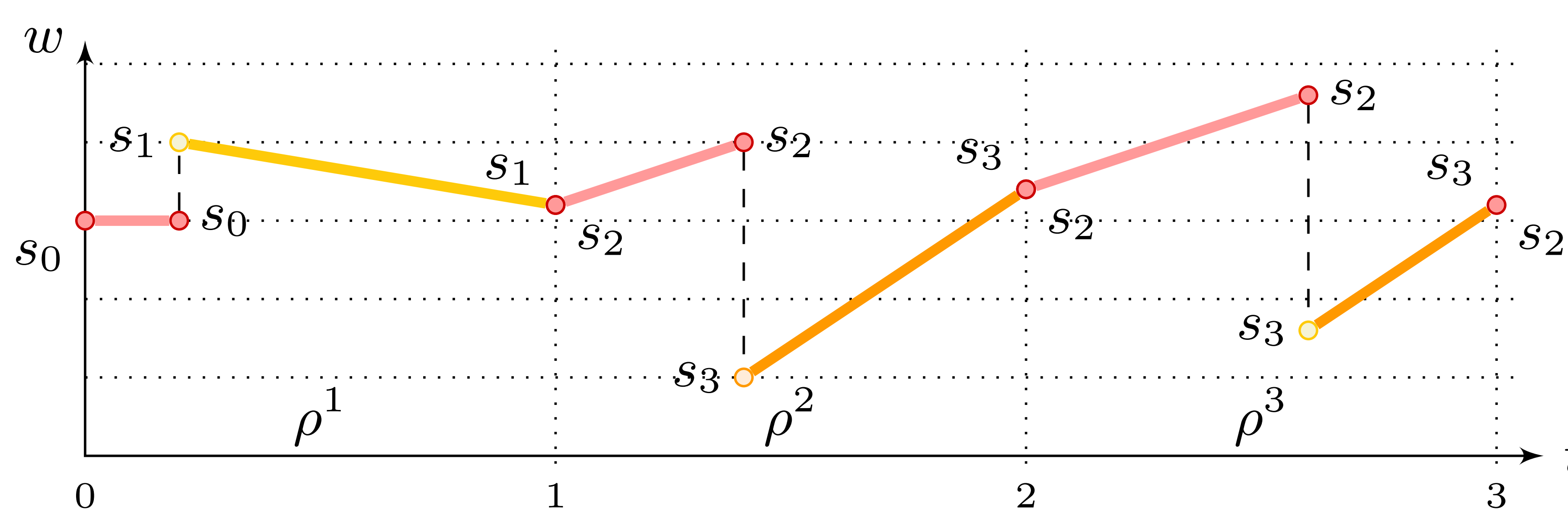
A SETA is called

- **flat** when for each $s \in S$ there is at most one path from s to itself.
- **depth-1** whenever the graph is tree-like with only loops at leaves

Segmented ETA



A finite (resp., infinite) execution of a SETA is a finite (resp., infinite) sequence of finite runs generated by its ETPs



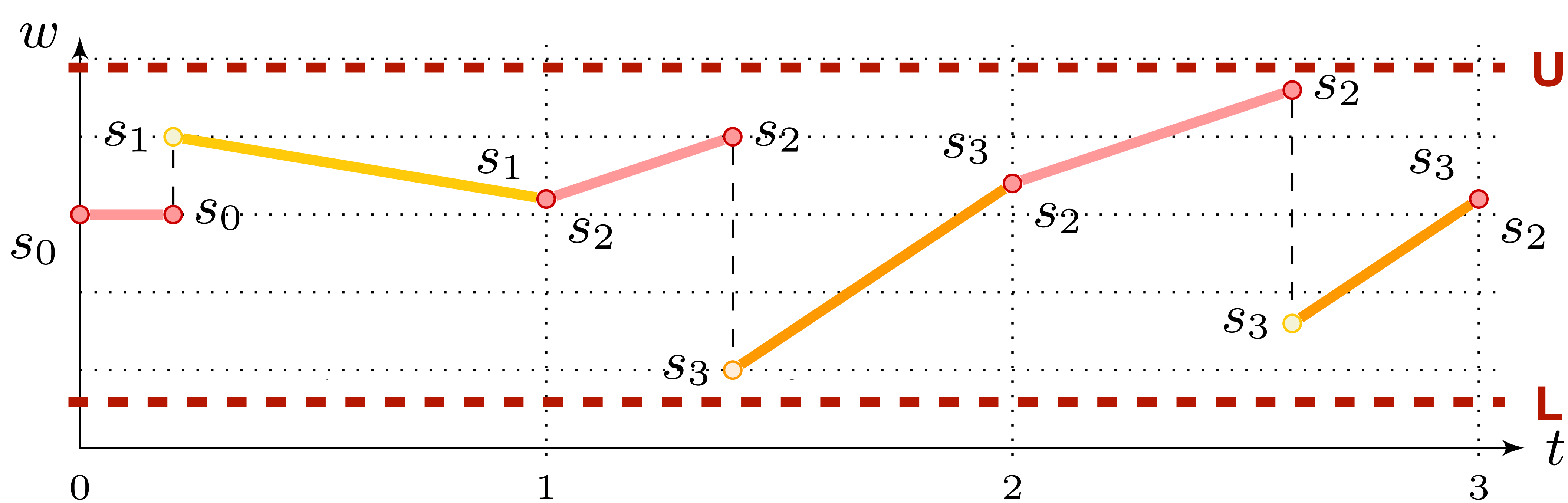
The energy-constrained infinite-run problem

INPUT

- An Energy timed automaton A
- Initial state s_0
- Initial energy level w_0
- Energy interval E = [L,U]

GOAL

Decide whether exists an **infinite execution** of A starting from (s_0, 0, w_0) **that satisfies E**



The energy-constrained infinite-run problem

INPUT

- An Energy timed automaton A
- Initial state s_0
- Initial energy level w_0
- Energy interval E = [L,U]

GOAL

Decide whether exists an **infinite execution** of A starting from (s_0, 0, w_0) **that satisfies E**

… what was known so far

Theorem ***[Markey'11]***

The energy constrained infinite-run problem is **undecidable for ETAs with at least 2 clocks**

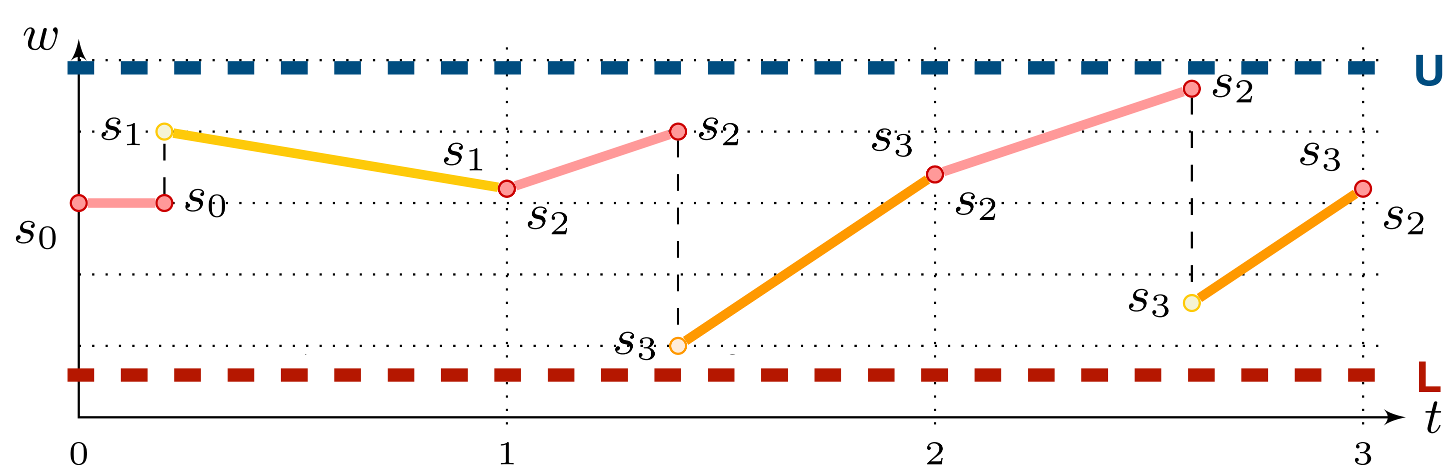
Our contribution to the problem

Theorem *[Bacci et al. FM'18]*

The energy-constrained infinite-run problem is **decidable for flat SETAs**

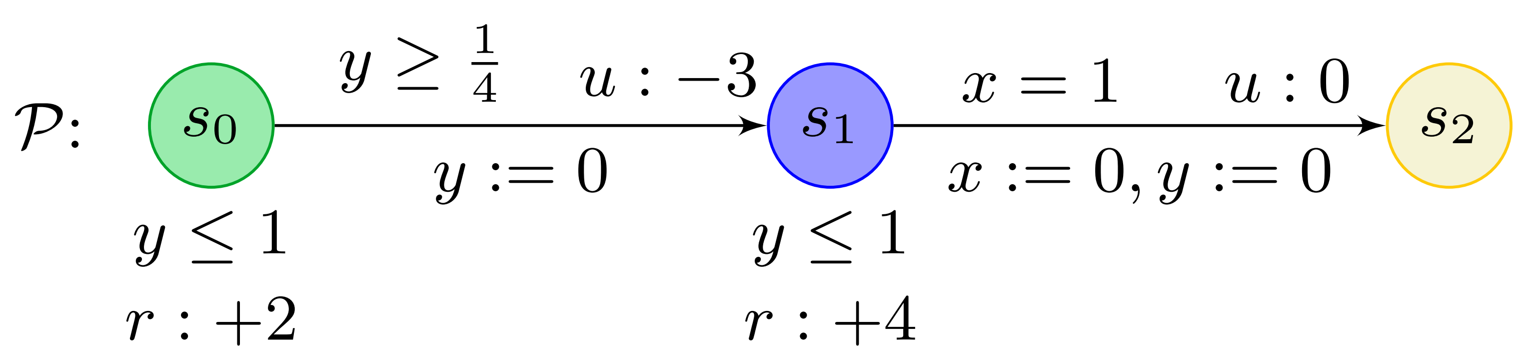
Theorem *[Bacci et al. FM'18]*

For a fixed lower bound L, **the existence of an energy upper bound U** that solves the energy-constrained infinite run problem is decidable for flat SETA.
For **depth-1 flat SETA we can compute the least U.**



The idea behind

Consider an Energy Timed Path



***E* = [0;5]**

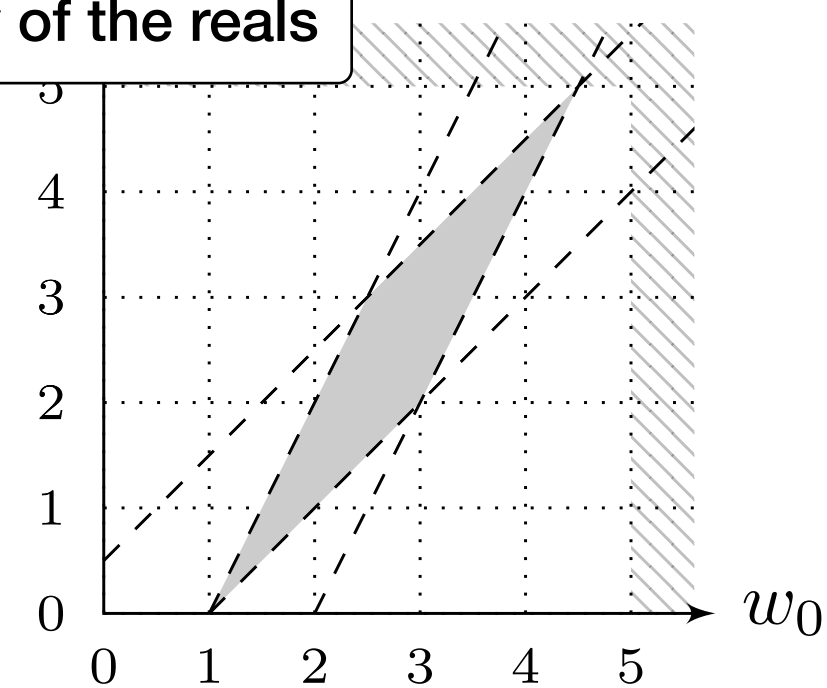
$$\mathcal{R}_{\mathcal{P}}^{E}(w_0, w_1)$$

Def.

$$\exists d_0, d_1.\ d_0 \in [0.25; 1] \wedge d_1 \in [0; 1] \wedge d_0 + d_1 = 1 \wedge \\ w_0 \in [0; 5] \wedge w_0 + 2d_0 \in [0; 5] \wedge w_0 + 2d_0 - 3 \in [0; 5] \wedge \\ w_1 = w_0 + 2d_0 + 4d_1 - 3 \wedge w_1 \in [0; 5].$$

$$(w_1 + 2 \leq 2w_0 \leq w_1 + 4) \wedge (w_1 - 0.5 \leq w_0 \leq w_1 + 1)$$

Translation into a first-order formula in the linear theory of the reals



Quantifier elimination

The Energy Relation

Energy Relation

$$\mathcal{R}^{E}_{\mathcal{P}}(w_0, w_1) \iff \exists (d_i)_{0 \le i < n}.\ \Phi_{\text{timing}} \wedge \Phi_{\text{energy}} \wedge w_1 = w_0 + \sum_{k=0}^{n-1} (d_k \cdot r(s_k) + u_k)$$

Energy Functions

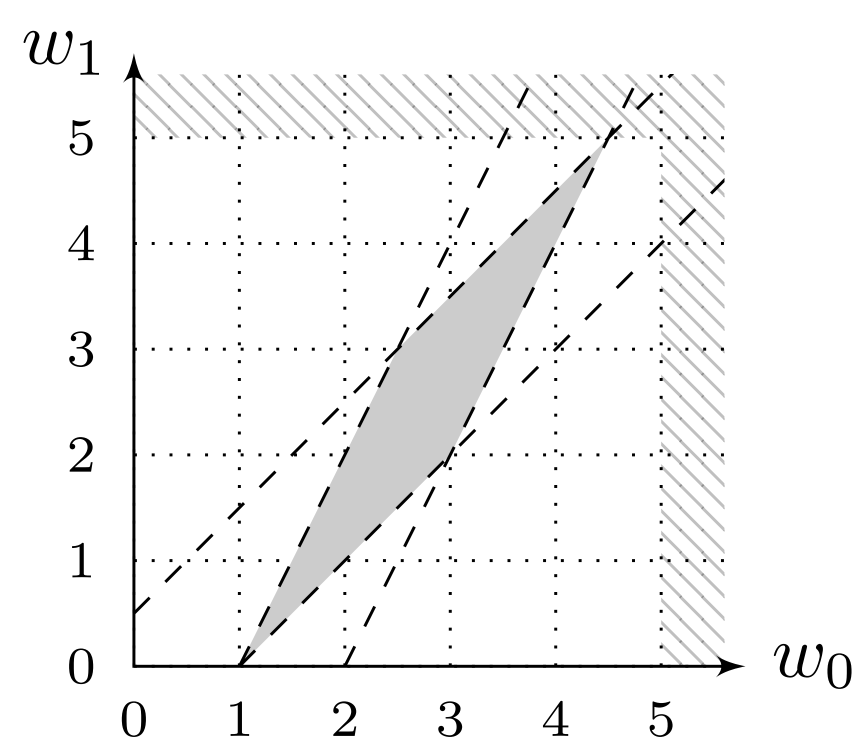
(*) Indices are removed to shorten notation

Forward propagation

$$\mathcal{R}(I) = \{w_1 \in E \mid \exists w_0 \in I.\ \mathcal{R}(w_0, w_1)\}$$

Backward propagation

$$\mathcal{R}^{-1}(I) = \{w_0 \in E \mid \exists w_1 \in I.\ \mathcal{R}(w_0, w_1)\}$$



The Energy Relation

Energy Relation

$$\mathcal{R}^{E}_{\mathcal{P}}(w_0, w_1) \iff \exists (d_i)_{0 \le i < n}.\ \Phi_{\text{timing}} \wedge \Phi_{\text{energy}} \wedge w_1 = w_0 + \sum_{k=0}^{n-1} (d_k \cdot r(s_k) + u_k)$$

Energy Functions

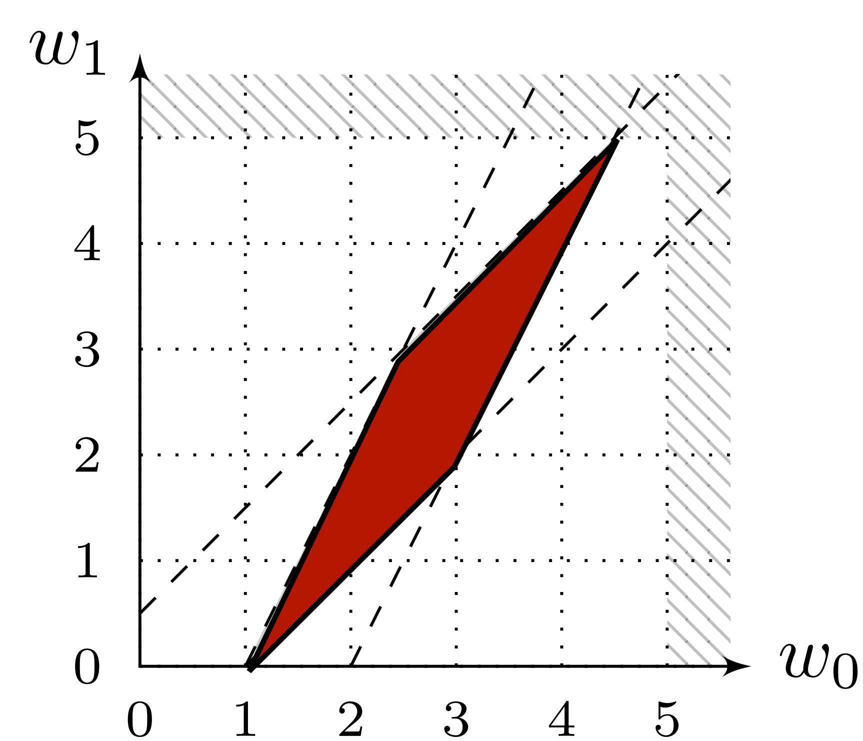
(*) Indices are removed shorten notation

Forward propagation

$$\mathcal{R}(I) = \{ w_1 \in E \mid \exists w_0 \in I.\ \mathcal{R}(w_0, w_1) \}$$

Backward propagation

$$\mathcal{R}^{-1}(I) = \{ w_0 \in E \mid \exists w_1 \in I.\ \mathcal{R}(w_0, w_1) \}$$



The Energy Relation

Energy Relation

$$\mathcal{R}^{E}_{\mathcal{P}}(w_0, w_1) \iff \exists (d_i)_{0 \le i < n}.\ \varPhi_{\text{timing}} \wedge \varPhi_{\text{energy}} \wedge w_1 = w_0 + \sum_{k=0}^{n-1} (d_k \cdot r(s_k) + u_k)$$

Energy Functions

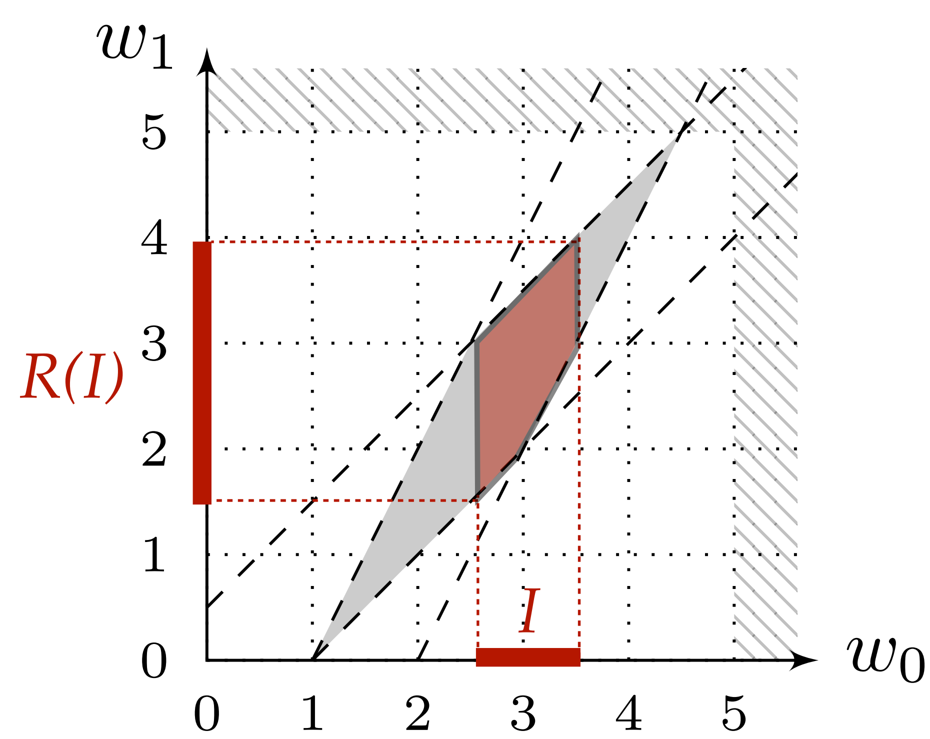
(*) Indices are removed shorten notation

Forward propagation

$$\mathcal{R}(I) = \{w_1 \in E \mid \exists w_0 \in I.\ \mathcal{R}(w_0, w_1)\}$$

Backward propagation

$$\mathcal{R}^{-1}(I) = \{w_0 \in E \mid \exists w_1 \in I.\ \mathcal{R}(w_0, w_1)\}$$



The Energy Relation

Energy Relation

$$\mathcal{R}^{E}_{\mathcal{P}}(w_0, w_1) \iff \exists (d_i)_{0\le i<n}.\ \Phi_{\text{timing}} \wedge \Phi_{\text{energy}} \wedge w_1 = w_0 + \sum_{k=0}^{n-1} (d_k \cdot r(s_k) + u_k)$$

Energy Functions

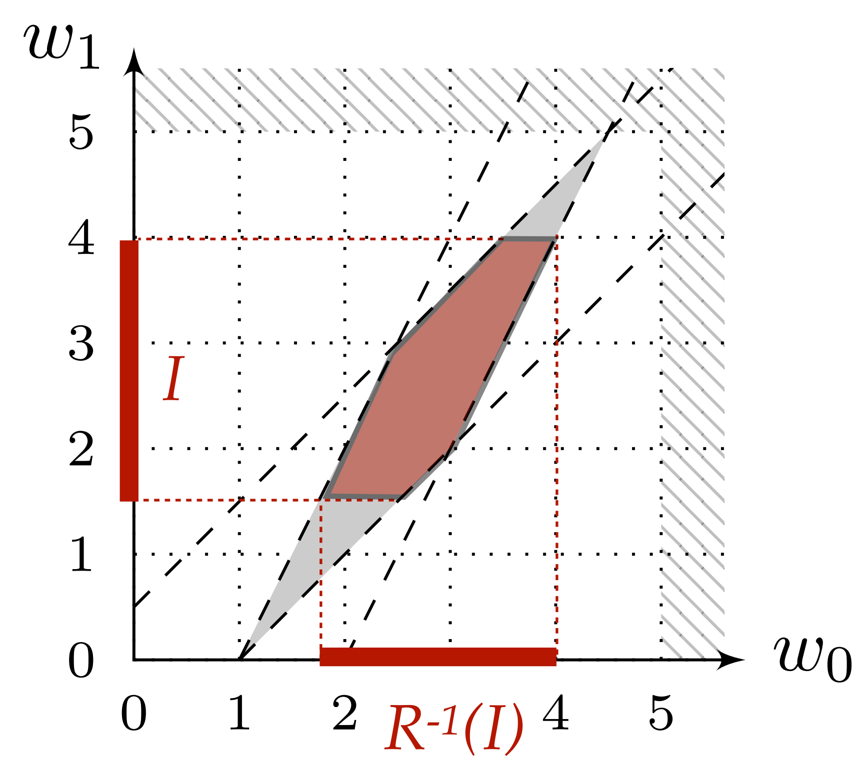
(*) Indices are removed shorten notation

Forward propagation

$$\mathcal{R}(I) = \{w_1 \in E \mid \exists w_0 \in I.\ \mathcal{R}(w_0, w_1)\}$$

Backward propagation

$$\mathcal{R}^{-1}(I) = \{w_0 \in E \mid \exists w_1 \in I.\ \mathcal{R}(w_0, w_1)\}$$



The Energy Relation

Energy Relation

$$\mathcal{R}^E_{\mathcal{P}}(w_0, w_1) \iff \exists (d_i)_{0 \le i < n}.\ \Phi_{\text{timing}} \wedge \Phi_{\text{energy}} \wedge w_1 = w_0 + \sum_{k=0}^{n-1} (d_k \cdot r(s_k) + u_k)$$

Energy Functions

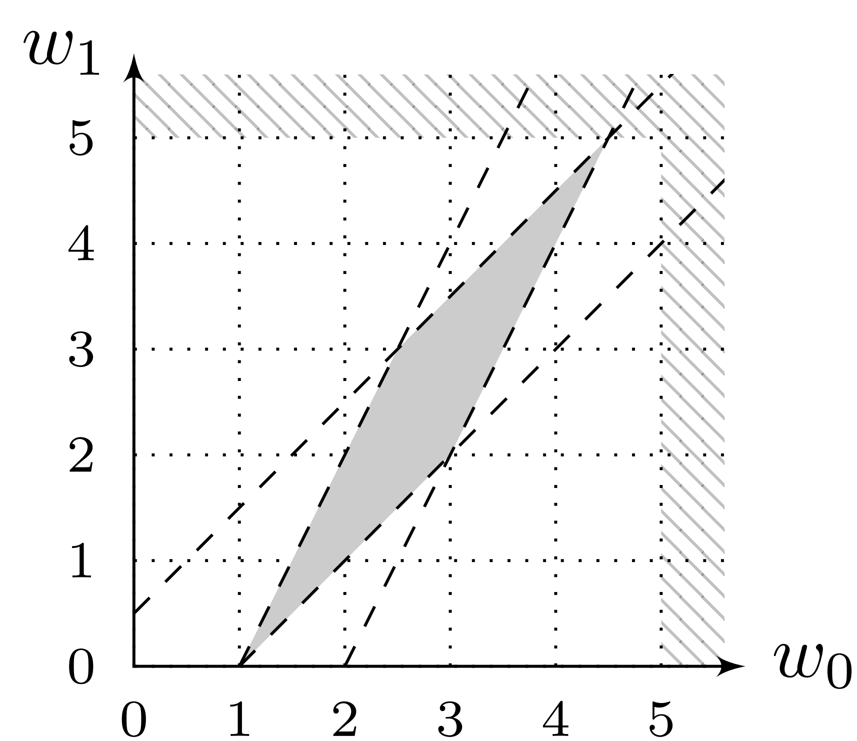
(*) Indices are removed shorten notation

Forward propagation

$$\mathcal{R}(I) = \{w_1 \in E \mid \exists w_0 \in I.\ \mathcal{R}(w_0, w_1)\}$$

Backward propagation

$$\mathcal{R}^{-1}(I) = \{w_0 \in E \mid \exists w_1 \in I.\ \mathcal{R}(w_0, w_1)\}$$



Consider a finite sequence of ETAs $(\mathcal{P}_i)_{1 \le i \le k}$

$$\mathcal{R}^E_{\mathcal{P}} = \mathcal{R}^E_{\mathcal{P}_k} \circ \cdots \circ \mathcal{R}^E_{\mathcal{P}_1}$$

Described as a finite conjunction of linear constraints over w_0 and w_1

From R to infinite runs

Consider a finite sequence of ETAs $(\mathcal{P}_i)_{1\leq i\leq k}$ **forming a cycle**

$$\mathcal{R}^E_{\mathcal{P}} = \mathcal{R}^E_{\mathcal{P}_k} \circ \cdots \circ \mathcal{R}^E_{\mathcal{P}_1}$$

A post-fixed point for $\mathcal{R}^{-1}$ is a set of initial energy values that can be forward propagated infinitely many times.

In particular, **the greatest fixed point contains all the initial energy values that admit an infinite run satisfying E**

$$\nu\mathcal{R}^{-1} = \bigcap_{i\in\mathbb{N}} (\mathcal{R}^{-1})^i(E)$$

Characterising $\nu\mathcal{R}^{-1}$

$$\nu\mathcal{R}^{-1} = \bigcap_{i\in\mathbb{N}} (\mathcal{R}^{-1})^i(E)$$

A generic post-fixed point [a; b] is logically characterised as follows

$$\phi(a,b) := a \leq b \wedge a \in E \wedge b \in E \wedge$$
$$\forall w_0 \in [a;b].\ \exists w_1 \in [a;b].\ \mathcal{R}^E_{\mathcal{P}}(w_0, w_1)$$

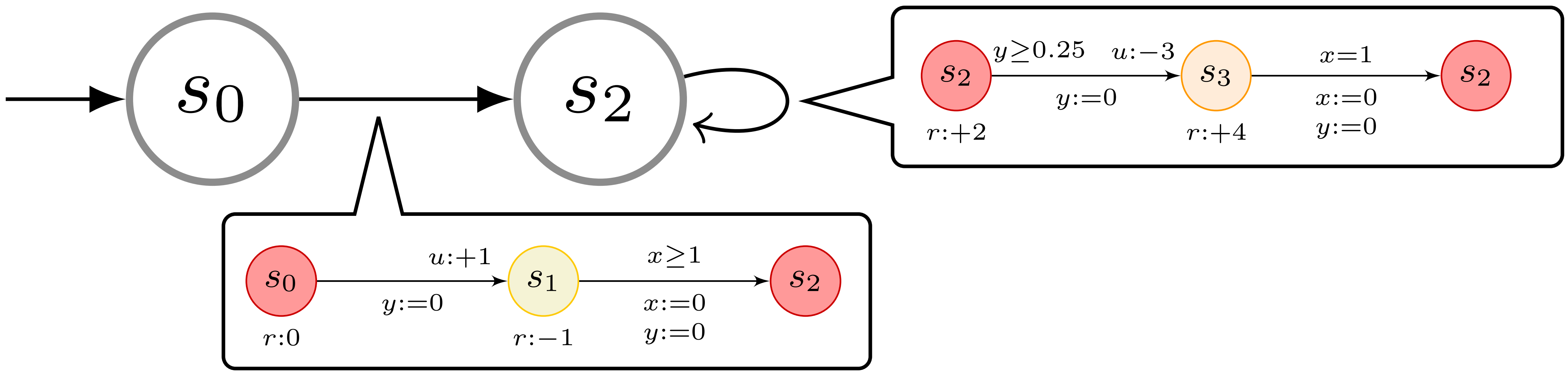
By applying **quantifier elimination** (to w_0 an w_1) the above formula may be transformed in a finite disjunction of linear constraints, thus

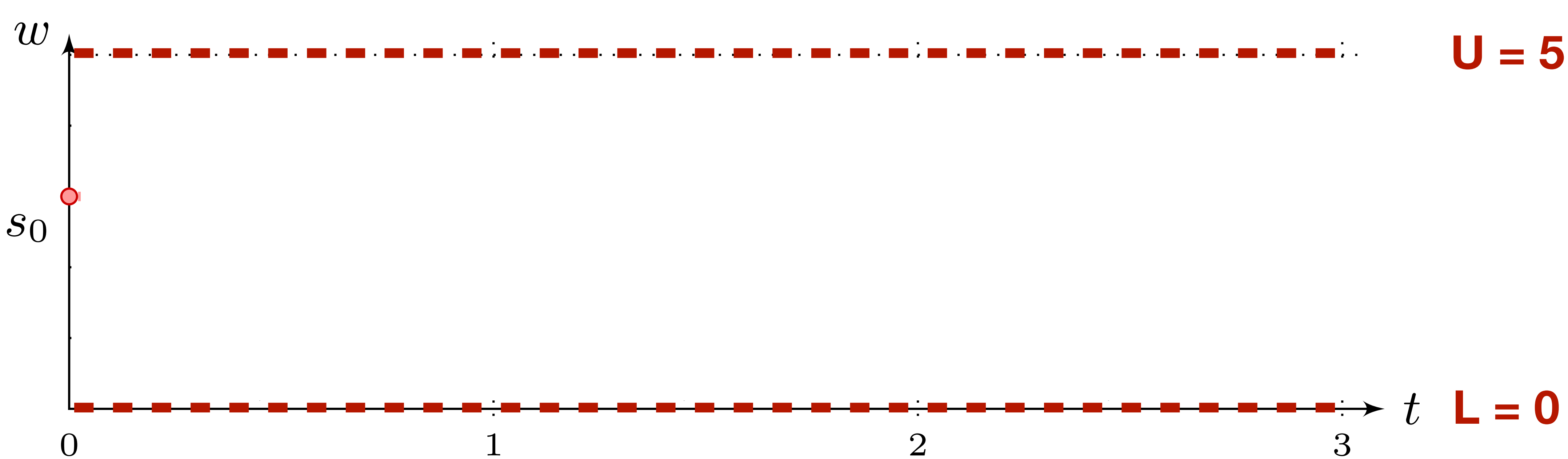
$$\max_{a,b}\{b - a \mid \phi(a,b) \text{ holds}\}$$

This gives a method for computing $\nu\mathcal{R}^{-1}$

Finding an infinite-run in a SETA

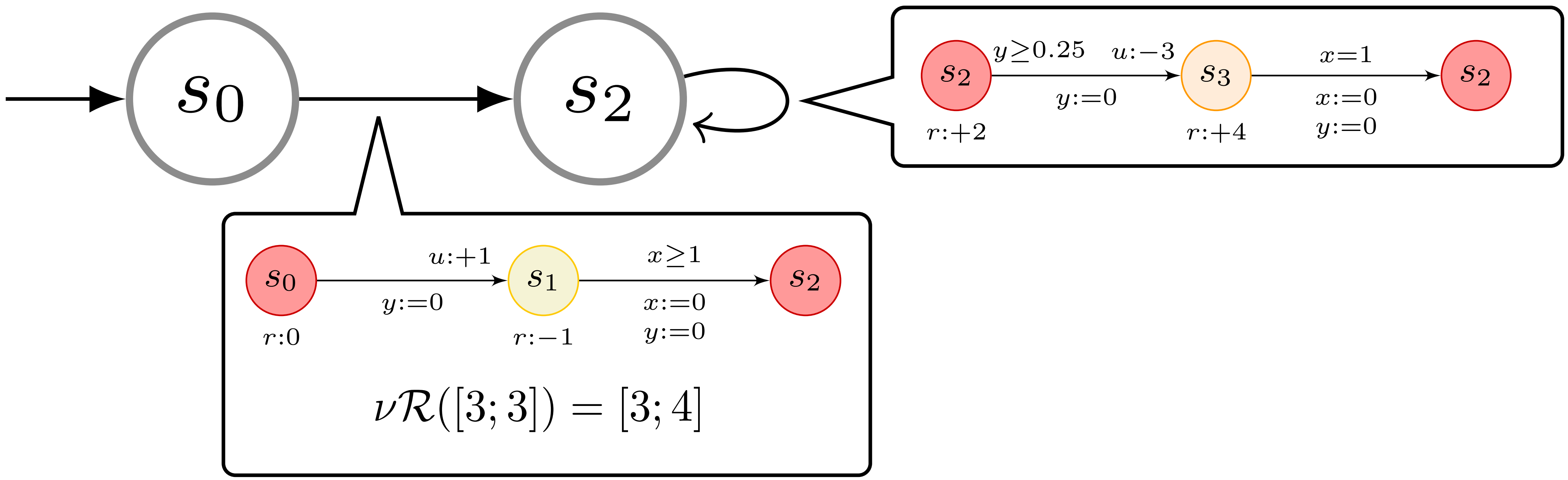
Consider the initial energy $w_0 = 3$ and the energy interval $E = [0; 5]$

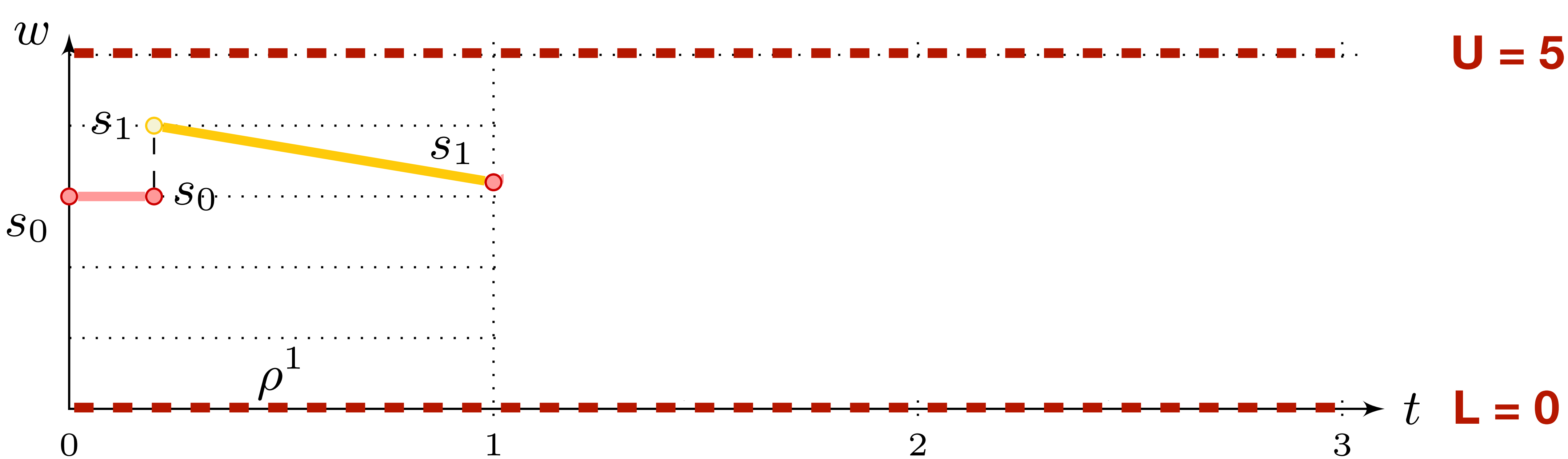




Finding an infinite-run in a SETA

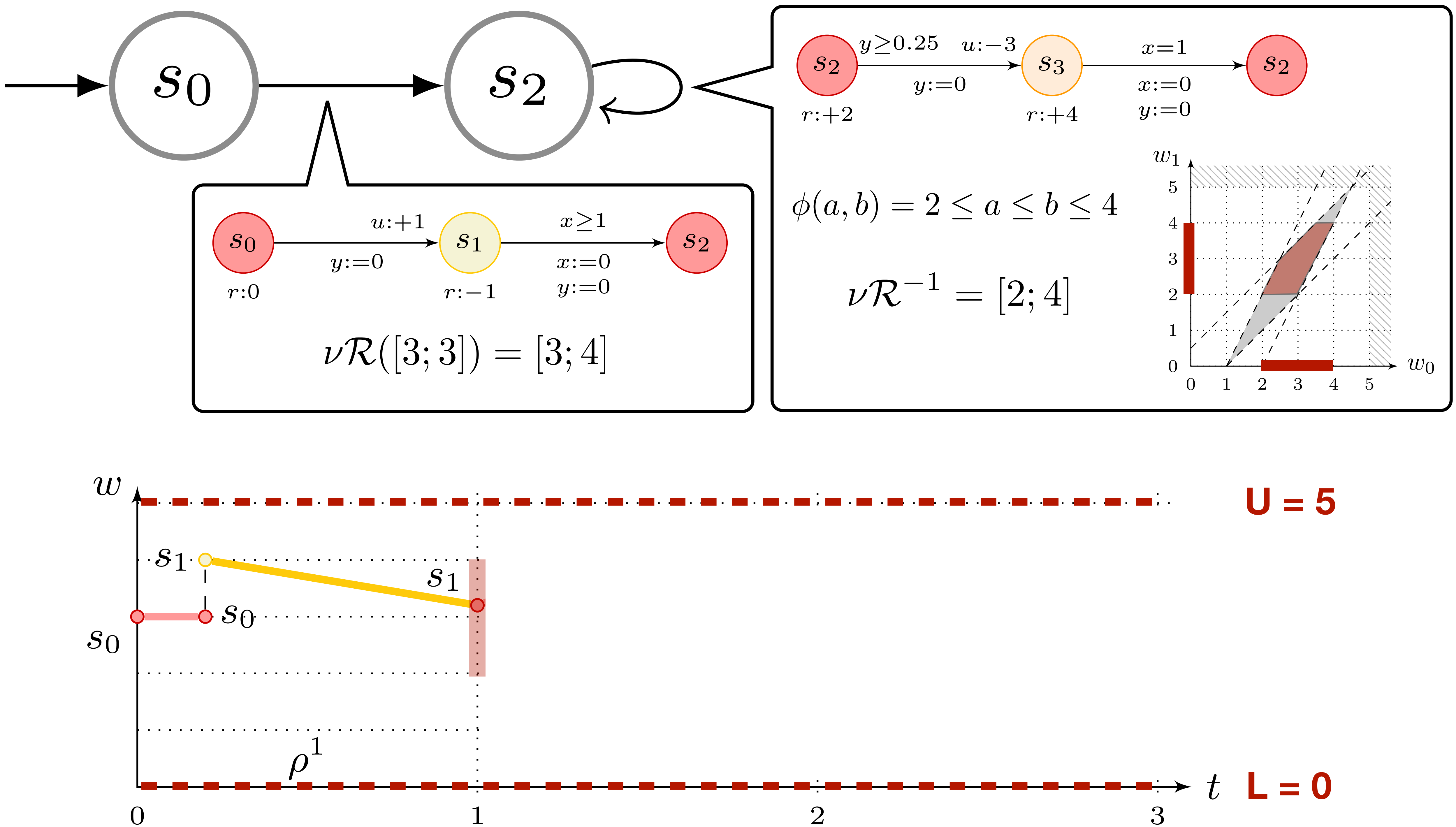
Consider the initial energy $w_0 = 3$ and the energy interval E = [0; 5]





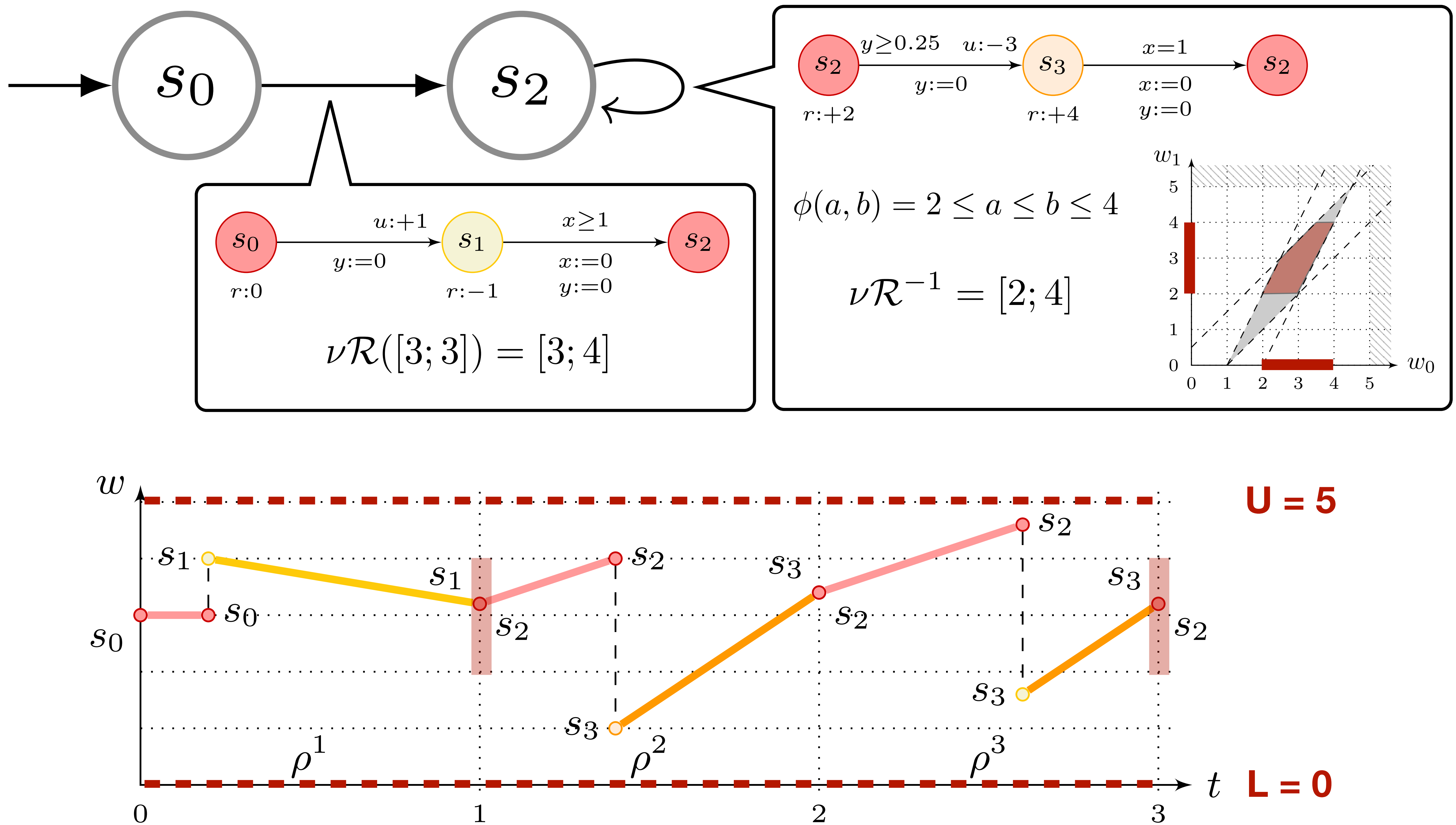
Finding an infinite-run in a SETA

Consider the initial energy w_0 = 3 and the energy interval E = [0; 5]

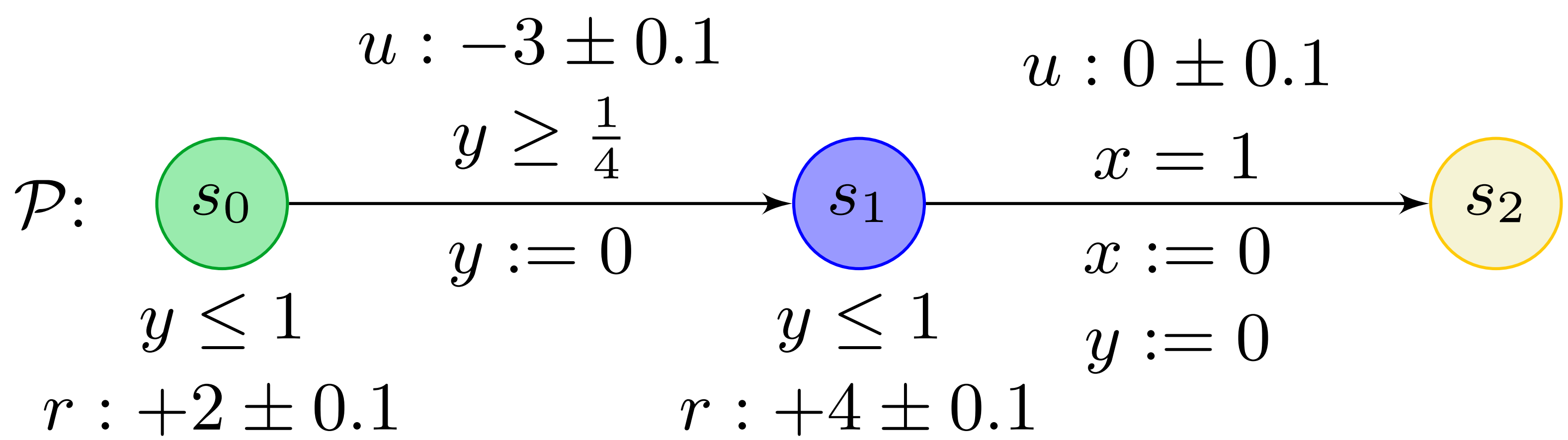


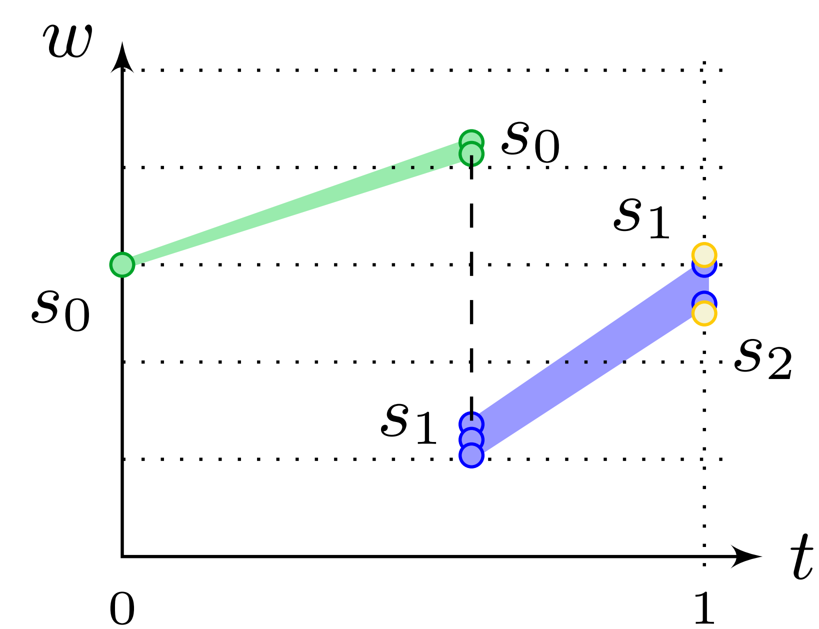
Finding an infinite-run in a SETA

Consider the initial energy w_0 = 3 and the energy interval E = [0; 5]



Adding uncertainty to ETA





$$
\begin{aligned}
\mathcal{U}^E_{\mathcal{P}}(w_0, a, b) \iff\ & \exists d_0, d_1.\ d_0 \in [0.25; 1] \wedge d_1 \in [0; 1] \wedge d_0 + d_1 = 1 \wedge w_0 \in [0; 5] \wedge \\
& w_0 + [1.9; 2.1] \cdot d_0 \subseteq [0; 5] \wedge \\
& w_0 + [1.9; 2.1] \cdot d_0 + [-3.1; -2.9] \subseteq [0; 5] \wedge \\
& w_0 + [1.9; 2.1] \cdot d_0 + [-3.1; -2.9] + [3.9; 4.1] \cdot d_1 \subseteq [0; 5] \wedge \\
& w_0 + [1.9; 2.1] \cdot d_0 + [-3.1; -2.9] + [3.9; 4.1] \cdot d_1 + [-0.1; 0.1] \subseteq [a; b] \subseteq [0; 5]]
\end{aligned}
$$

$\Updownarrow$ QE

$$
\begin{aligned}
& 0 \leq a \leq b \leq 5 \wedge b \geq a + 0.6 \wedge a - 0.2 \leq w_0 \leq b + 0.7 \wedge \\
& (4.87 + 1.9 \cdot a)/3.9 \leq w_0 \leq (7.27 + 2.1 \cdot b)/4.1
\end{aligned}
$$

The (ternary) energy relation takes into account all possible energy outcomes

Our contribution to the problem

Theorem *[Bacci et al. FM'18]*

The energy-constrained infinite-run problem is **decidable for SETAu satisfying (R)**

We do not require flatness!

(R) in any ETPu of the SETAu some clock is compared with a positive lower bound. Thus, there is an (overall minimal) positive time-duration D to complete any ETAu.

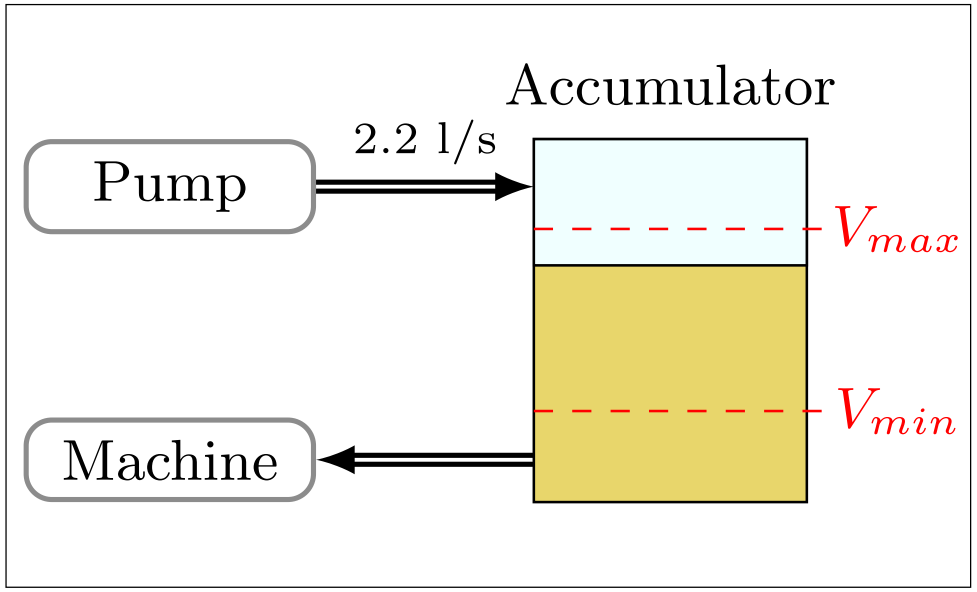
Theorem *[Bacci et al. FM'18]*

For a fixed lower bound L, **the existence of an energy upper bound U** that solves the energy-constrained infinite run problem is decidable for **depth-1 flat SETAu**. Furthermore, **we can compute the least U.**

Back to the Case Study:
the HYDAC system

System components

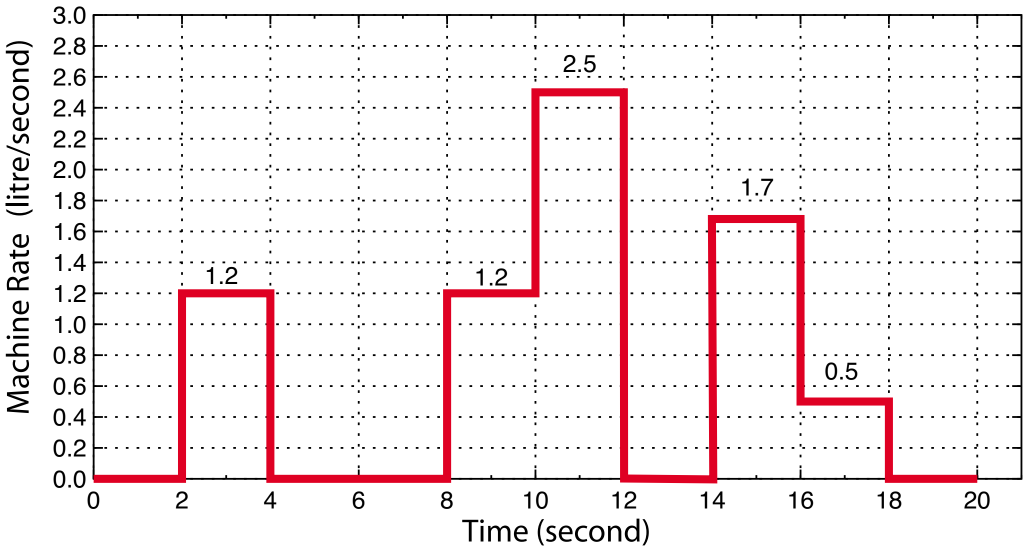
- A **machine** that consumes oil according to a fixed cyclic pattern of 20s
- Hydraulic **accumulator** containing oil and a fixed amount of gas that puts the oil under pressure
- **Controllable pump (on/off)** which pumps oil into the accumulator with rate 2.2 l/s



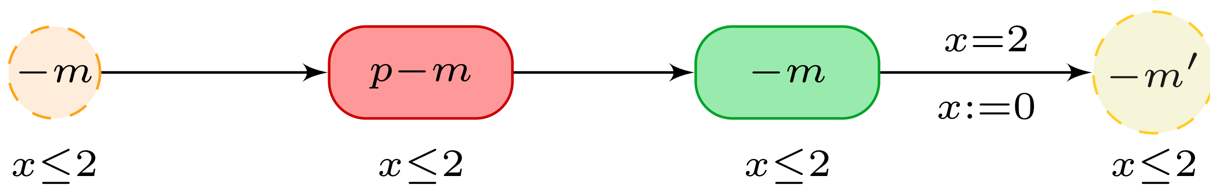
The control objective

- The level of oil shall be maintained within a **safe interval [V_{max}; V_{min}] = [4.9; 25.1] l**
- The **system shall never stop**
- **Minimise the average level of oil**

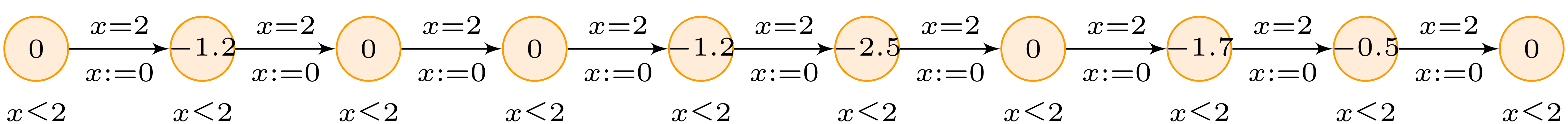
$$\int_{t=0}^{t=T} \frac{v(t)}{T}\,dt$$



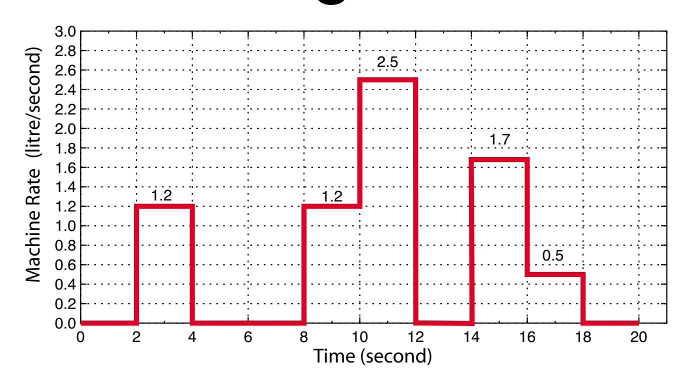
Modelling the HYDAC system



An ETP modelling a single switch of the pump (initially off)
- p = 2.2 pump rate,
- m and m' two consecutive machine consumption rate



ETP modelling a machine cycle



The parallel composition of the two ETPs Models the system precisely, however it is not a flat-SETA

We propose two variants of the system:
- **H_1 allows the pump to switch once every 2-sec slot**
- **H_2 allows the pump to switch once every second 2-sec slot**

We consider also extensions $H_1(\epsilon)$ and $H_2(\epsilon)$ with uncertainty ϵ = 0.1 l/s

Machine consumption rate [-m - ϵ, -m + ϵ]

Synthesising Controllers

- **Synthesis of optimal energy bounds**

  A. synthesise the **minimal upper bound U** admitting an infinite run satisfying the energy interval $[V_{min}, U]$

  B. Determine the **greatest safe energy interval** $[a,b] \subseteq [V_{min}, U]$

- **Synthesis of optimal safe strategies**

  1. The set of **permissive strategies** is modelled as a quantifier-free first-order formula

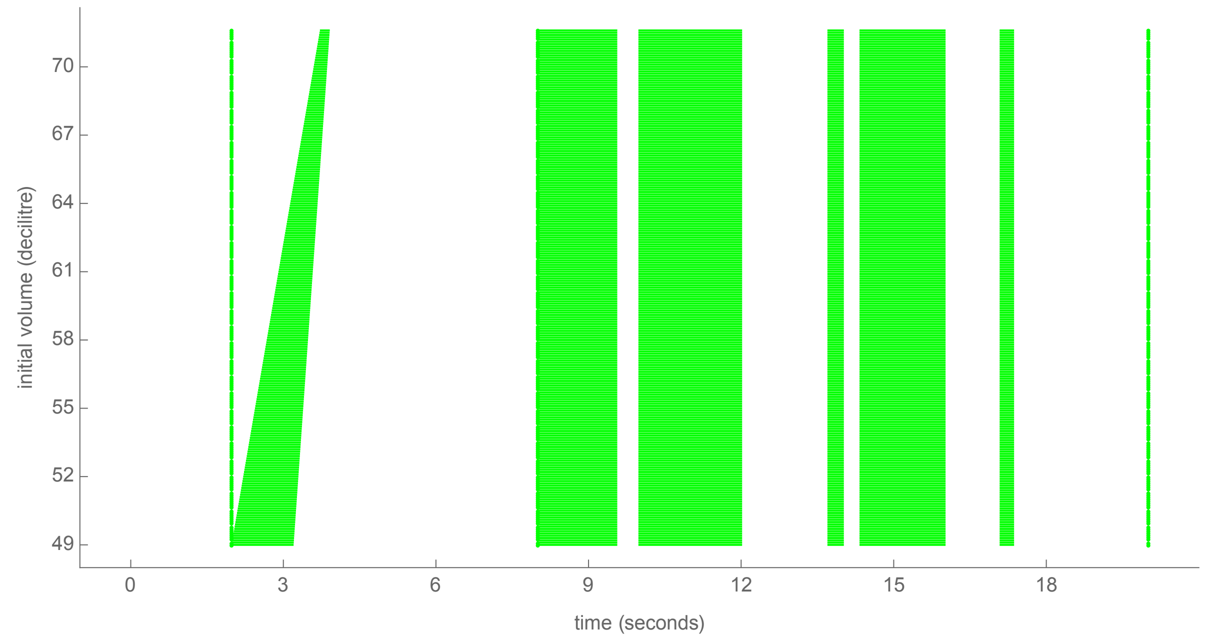
  2. Minimise the (non-linear) cost function $\int_{t=0}^{t=T} \frac{v(t)}{T} dt$ expressing the average oil volume

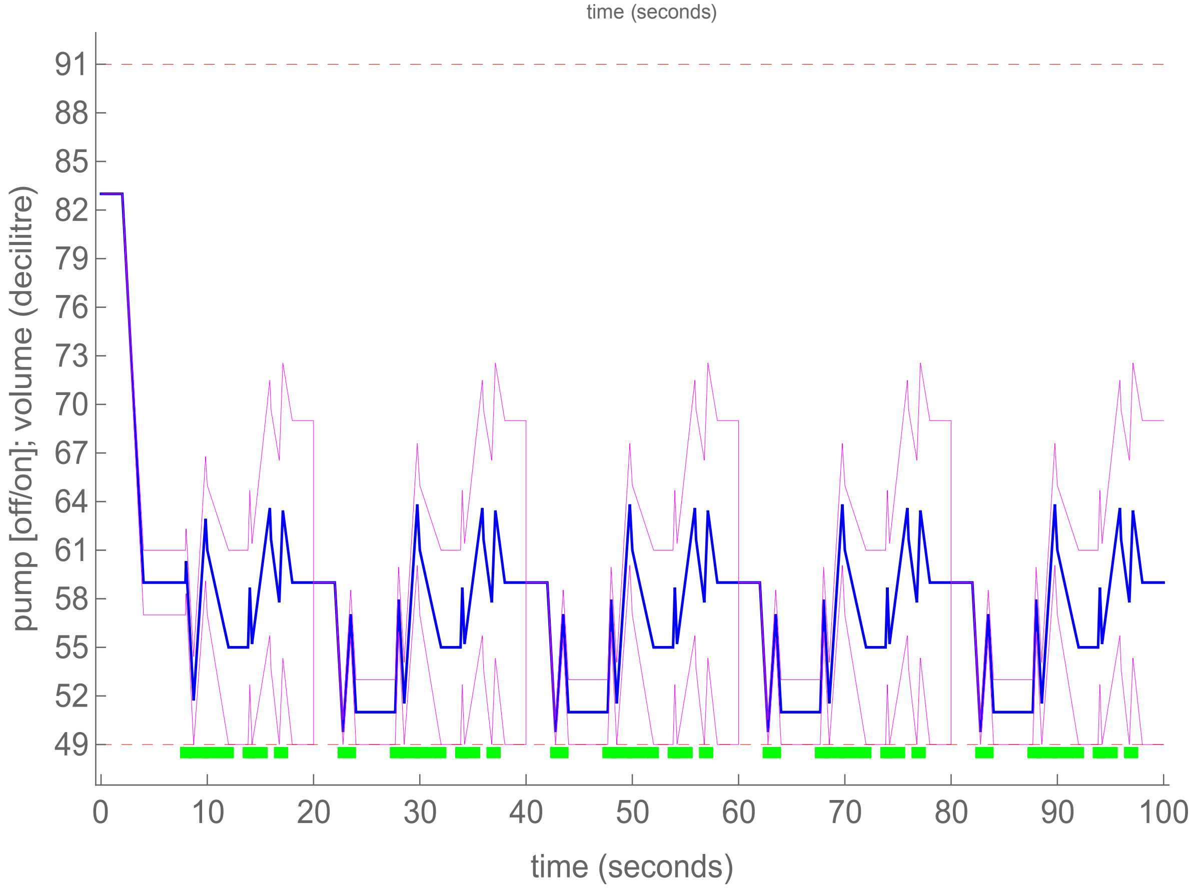
Synthesised Controllers

Local controller

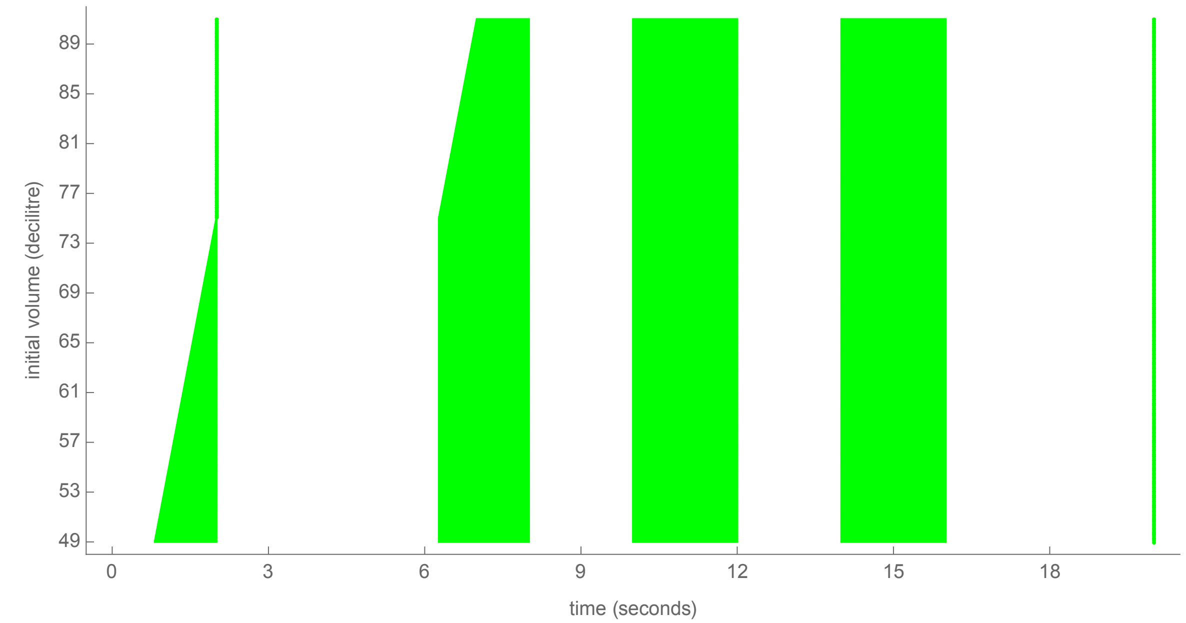
Simulation (10 cycles)

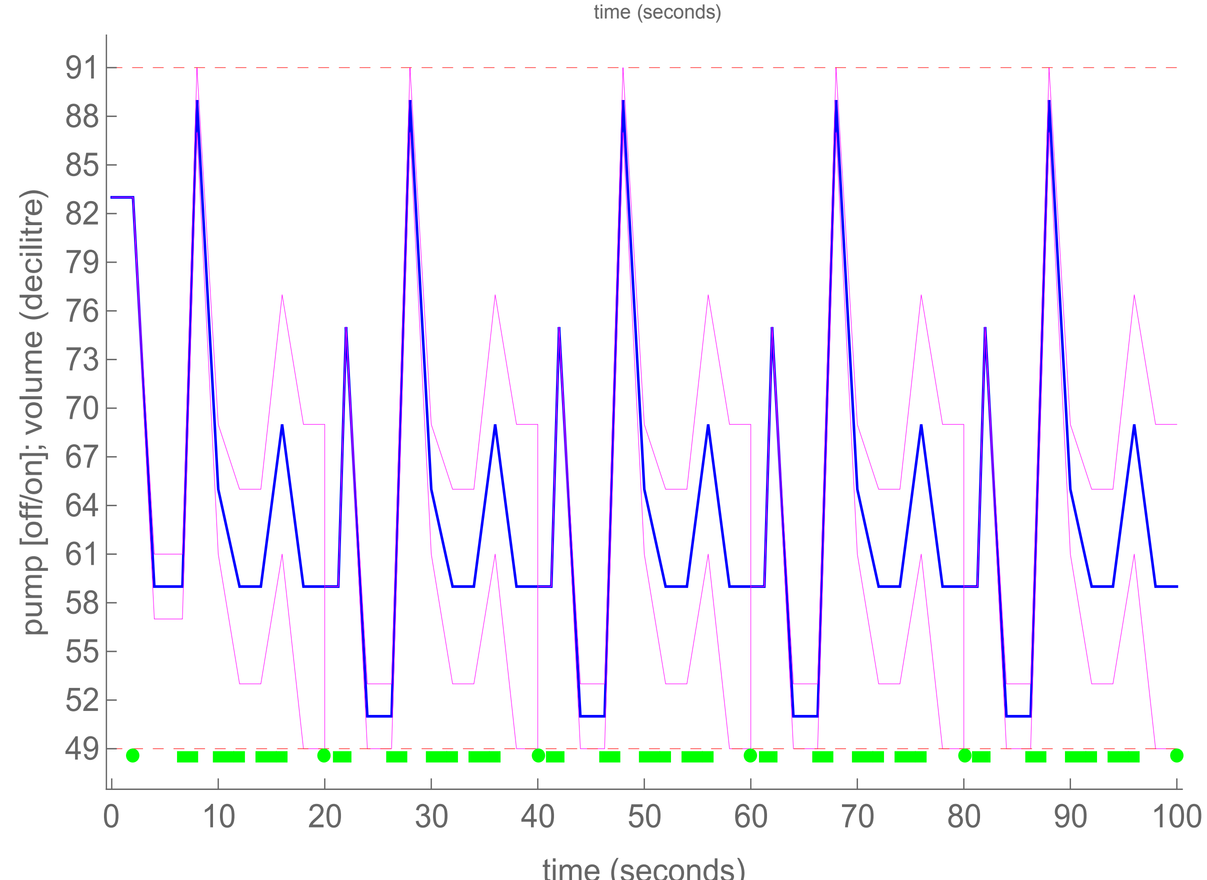
$H_1(\epsilon)$





$H_2(\epsilon)$





Performance

Controller	$[L;U]$	$[a;b]$	Mean vol. (l)
$\mathcal{H}_1$	$[4.9;5.84]$	$[4.9;5.84]$	5.43
$\mathcal{H}_1(\epsilon)$	$[4.9;7.16]$	$[5.1;7.16]$	6.15
$\mathcal{H}_2$	$[4.9;7.9]$	$[4.9;7.9]$	6.12
$\mathcal{H}_2(\epsilon)$	$[4.9;9.1]$	$[5.1;9.1]$	7.24
G1M1 [16]	$[4.9;25.1]^{(*)}$	$[5.1;9.4]$	8.2
G2M1 [16]	$[4.9;25.1]^{(*)}$	$[5.1;8.3]$	7.95
[29]	$[4.9;25.1]^{(*)}$	$[5.2;8.1]$	7.35

$^{(*)}$ Safety interval given by the HYDAC company.

Tool Chain:
- *Mathematica* (constr & simpl)
- *Mjollnir* (QE)

Compositional Methods:
20 min → 20 ms

Controller	Acc. vol. (l)	Mean vol. (l)
$\mathcal{H}_1$	1081.77	5.41
$\mathcal{H}_2$	1158.90	5.79
$\mathcal{H}_1(\epsilon)$	1200.21	6.00
$\mathcal{H}_2(\epsilon)$	1323.42	6.62

Controller	Acc. vol. (l)	Mean vol. (l)
Bang-Bang	2689	13.45
HYDAC	2232	11.60
G1M1	1518	7.59
G2M1	1489	7.44

[16] Cassez, Jensen, Larsen, Raskin, Reyner - Automatic Synthesis of Robust and Optimal Controllers (HSCC'09)
[29] Zhao, Zhan, Kapur, Larsen - A "hybrid" approach for synthesising optimal controllers of hybrid systems: A case study of the oil pump industrial example (FM'12)

Conclusion

- Novel framework for synthesis of safe and optimal controllers, based on energy timed automata.

- Approach based on
  1. translation into first-order formulas in the linear theory of the reals
  2. quantifier elimination
  3. Numerical optimisation

- Applicable on real industrial applications

- Prototype tool using Mathematica & Mjollnir (available at http://people.cs.aau.dk/~giovbacci/tools.html)

Future Work

- Extend the result to (non-flat) and non-segmented ETAs
- Add UPPAAL STRATEGO to our tool chain

Thank you

Synthesising Controllers

Synthesis of optimal energy bounds

We **synthesise a minimal upper bound U*** (within the interval E = [V_{min}, V_{max}]) admitting an infinite run satisfying the energy interval E' = [V_{min}, U*]

$$min\left\{U \,\middle|\, V_{min} \leq a \leq b \leq U \leq V_{max} \wedge \forall w_0 \in [a,b].\, \exists w_1 \in [a,b].\, \mathcal{R}_{\mathcal{P}}^{[V_{min},U]}(w_0, w_1)\right\}$$

We compute **the greatest energy-safe interval [a,b]** ⊆ **E'**

$$max\left\{b - a \,\middle|\, V_{min} \leq a \leq b \leq U^* \wedge \forall w_0 \in [a,b].\, \exists w_1 \in [a,b].\, \mathcal{R}_{\mathcal{P}}^{E'}(w_0, w_1)\right\}$$

Synthesis of optimal safe strategy

The set of **permissive strategies** is described as a quantifier-free first-order formula

$$\Phi_{\text{on}} \wedge \Phi_{\text{off}} \wedge \Phi_{\text{timing}} \wedge \Phi_{\text{energy}} \wedge w_1 = w_0 + \sum_{k=0}^{n-1} (d_k \cdot r(s_k) + u_k)$$

An optimal strategy is a permissive strategy that **minimise the non-linear cost function expressing the average oil volume**