Safety Controller Synthesis for Switched Systems using Multiscale Symbolic Models

Antoine Girard

Laboratoire des Signaux et Systèmes
Gif sur Yvette, France

Workshop on switching dynamics & verification
Paris, January 28-29, 2016

Introduction

- Controller synthesis for a class of continuous-time switched systems
  - Incrementally stable systems: the influence of initial condition asymptotically vanishes.
  - Safety specification: controlled invariance.
- Approach based on the use of symbolic models
  - Discrete (time and space) approximation of the switched system.
  - Approach based on uniform discretization of time and space. [Girard, Pola and Tabuada, 2010]
  - Distance between trajectories of incrementally stable switched system and of symbolic model is uniformly bounded, and can be made arbitrarily small.
  - Safety controller synthesis using symbolic models via algorithmic discrete controller synthesis.

Motivation

- Limitations of the symbolic control approach
  - Spatial and time resolution must be chosen carefully to achieve a given precision: fast switching requires fine spatial resolution;
  - Uniform spatial discretization: excessive computation time and memory consumption.

- Overcome this problem with multiscale symbolic models
  - Use of multiscale discretizations of time and space
  - Incremental exploration of symbolic models during controller synthesis: The finer scales explored only if safety cannot be ensured at coarser level.

Outline

1. Incrementally stable switched systems
2. Multiscale symbolic models
3. Safety controller synthesis using multiscale symbolic models
4. Computational experiments

Switched systems

Definition

A switched system is a tuple $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$, where

- $\mathbb{R}^n$ is the state space;
- $P = \{1, \ldots, m\}$ is the finite set of modes;
- $\mathcal{P}$ is a subset of $\mathcal{S}(\mathbb{R}_0^+, P)$, the set of functions from $\mathbb{R}_0^+$ to P with a finite number of discontinuities on every bounded interval of $\mathbb{R}_0^+$;
- $F = \{f_1, \ldots, f_m\}$ is a collection of smooth vector fields indexed by P.

- For a switching signal $\mathbf{p} \in \mathcal{P}$, initial state $x \in \mathbb{R}^n$, $\mathbf{x}(., x, \mathbf{p})$ is the trajectory of Σ, solution of:

$$\dot{\mathbf{x}}(t) = f_{\mathbf{p}(t)}(\mathbf{x}(t)),\ \mathbf{x}(0) = x.$$

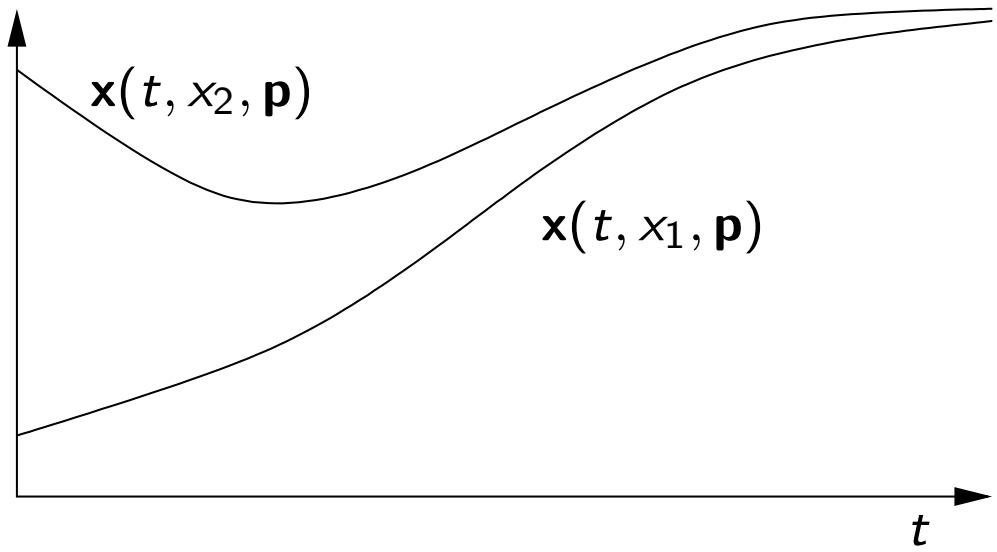
- $\mathcal{S}_{\tau_d}(\mathbb{R}_0^+, P)$ is the set of switching signals $\mathbf{p}$ with minimum dwell-time $\tau_d \in \mathbb{R}^+$: discontinuities of $\mathbf{p}$ are separated by at least τ_d.

Incremental stability

Definition

Σ is incrementally globally uniformly asymptotically stable (δ-GUAS) if there exists a $\mathcal{KL}$ function β such that for all $x_1, x_2 \in \mathbb{R}^n$, $\mathbf{p} \in \mathcal{P}$, $t \in \mathbb{R}_0^+$:

$$\|\mathbf{x}(t, x_1, \mathbf{p}) - \mathbf{x}(t, x_2, \mathbf{p})\| \leq \beta(\|x_1 - x_2\|, t).$$



Lyapunov characterization

Definition

$V_p : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_0^+$, $p \in P$ are multiple δ-GUAS Lyapunov functions for Σ if there exist $\kappa, \mu \in \mathbb{R}^+$ with $\mu \geq 1$, $\mathcal{K}_\infty$ functions $\underline{\alpha}$, $\overline{\alpha}$, such that for all $x_1, x_2 \in \mathbb{R}^n$, $p, p' \in P$:

$$\underline{\alpha}(\|x_1 - x_2\|) \leq V_p(x_1, x_2) \leq \overline{\alpha}(\|x_1 - x_2\|);$$
$$\frac{\partial V_p}{\partial x_1}(x_1, x_2) f_p(x_1) + \frac{\partial V_p}{\partial x_2}(x_1, x_2) f_p(x_2) \leq -\kappa V_p(x_1, x_2);$$
$$V_p(x_1, x_2) \leq \mu V_{p'}(x_1, x_2).$$

Theorem

Let $\tau_d \in \mathbb{R}^+$, $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$ with $\mathcal{P} \subseteq \mathcal{S}_{\tau_d}(\mathbb{R}_0^+, P)$ admitting multiple δ-GUAS Lyapunov functions. If $\tau_d > \frac{\log \mu}{\kappa}$, then Σ is δ-GUAS.

Additional assumption

In the following, we will assume that there exists a $\mathcal{K}_\infty$ function γ such that for all $x_1, x_2, x_3 \in \mathbb{R}^n$

$$|V_p(x_1, x_2) - V_p(x_1, x_3)| \leq \gamma(\|x_2 - x_3\|), \quad \forall p \in P;$$

This is not restrictive if V_p are smooth and we work on a bounded subset of $\mathbb{R}^n$.

Outline

1. Incrementally stable switched systems
2. Multiscale symbolic models
3. Safety controller synthesis using multiscale symbolic models
4. Computational experiments

Transition systems

Definition

A transition system is a tuple $T = (X, U, Y, \Delta, X^0)$ where

- X, U, Y, X^0 are the sets of states, inputs, outputs and initial states;
- $\Delta \subseteq X \times U \times X \times Y$ is a transition relation.

T is metric if Y is equipped with a metric d, symbolic if X and U are finite or countable sets.

- $(x, u, x', y) \in \Delta$ is denoted $(x', y) \in \Delta(x, u)$;
- $u \in U$ is enabled at $x \in X$, denoted $u \in \mathrm{enab}(x)$, if $\Delta(x, u) \neq \emptyset$;
- If $\mathrm{enab}(x) = \emptyset$, then x is blocking, otherwise it is non-blocking;
- T is deterministic if for all $x \in X$ and $u \in \mathrm{enab}(x)$, $|\Delta(x, u)| = 1$.

Trajectories

- A trajectory of T is a finite or infinite sequence of transitions

$$\sigma = (x^0, u^0, y^0)(x^1, u^1, y^1)(x^2, u^2, y^2)\dots$$

  where $(x^{i+1}, y^i) \in \Delta(x^i, u^i)$, for all $i \geq 0$. It is:
  - initialized if $x^0 \in X^0$;
  - maximal if it is infinite or it is finite and ends in a blocking state.
- $x \in X$ is reachable if there exists an initialized trajectory reaching x.
- T is non-blocking if all initialized maximal trajectories are infinite or equivalently if all reachable states are non-blocking.

Approximate bisimulation

Definition

Let $T_i = (X_i, U, Y, \Delta_i, X_i^0)$, with $i = 1, 2$ be metric transition systems with the same sets of inputs U and outputs Y equipped with the metric d. Let $\varepsilon \in \mathbb{R}_0^+$, $R \subseteq X_1 \times X_2$ is an ε-approximate bisimulation relation between T_1 and T_2 if for all $(x_1, x_2) \in R$, $u \in U$:

$$\forall (x_1', y_1) \in \Delta_1(x_1, u), \exists (x_2', y_2) \in \Delta_2(x_2, u),$$
$$d(y_1, y_2) \leq \varepsilon \text{ and } (x_1', x_2') \in R;$$
$$\forall (x_2', y_2) \in \Delta_2(x_2, u), \exists (x_1', y_1) \in \Delta_1(x_1, u),$$
$$d(y_1, y_2) \leq \varepsilon \text{ and } (x_1', x_2') \in R.$$

T_1 and T_2 are ε-approximately bisimilar, denoted $T_1 \sim_\varepsilon T_2$, if $X_1^0 \subseteq R^{-1}(X_2^0)$ and $X_2^0 \subseteq R(X_1^0)$.

Switched systems as transition systems

- Let $\Sigma_{\tau_d} = (\mathbb{R}^n, P, \mathcal{P}, F)$ be a switched system with $\mathcal{P} = \mathcal{S}_{\tau_d}(\mathbb{R}_0^+, P)$.
- We consider controllers that can select:
  1. a mode $p \in P$;
  2. a duration $\theta \in \Theta_\tau^N$ during which the mode remains active where

$$\Theta_\tau^N = \{\theta_s = 2^{-s}\tau \mid s = 0, \ldots, N\}.$$

  where $\tau \in \mathbb{R}^+$, $N \in \mathbb{N}$ are time sampling and scale parameters.

- We assume $\tau_d = \theta_{N_d}$ for some $N_d \in \{0, \ldots, N\}$, then

$$\Theta_\tau^{N_d} = \{\theta_s \in \Theta_\tau^N \mid \theta_s \geq \tau_d\}.$$

- Let $\mathcal{C}(I, \mathbb{R}^n)$ denote the set of continuous functions from I to $\mathbb{R}^n$.

Switched systems as transition systems

Let $T_\tau^N(\Sigma_{\tau_d}) = (X, U, Y, \Delta, X^0)$ where:

- $X = \mathbb{R}^n \times P$,
  $z = (x, p) \in X$ consists of a continuous state x and an active mode p.
- $U = P \times \Theta_\tau^N$,
  $u = (p, \theta_s) \in U$ consists of a mode p and a duration θ_s.
- $Y = \bigcup_{s=0}^{s=N} \mathcal{C}([0, \theta_s], \mathbb{R}^n)$ is a set of continuous functions,
  equipped with the metric:

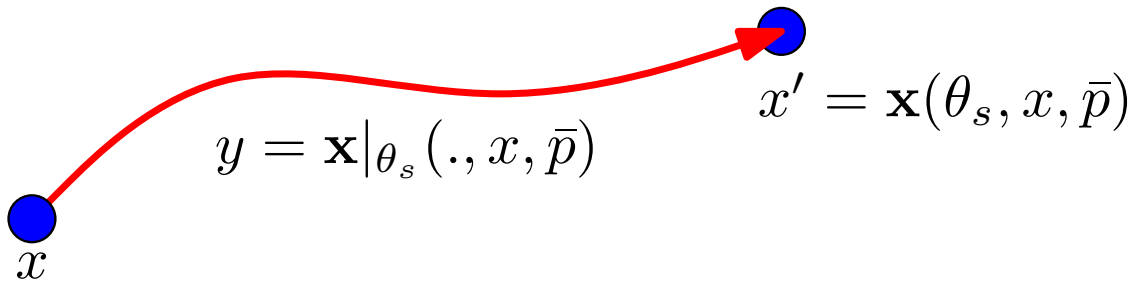
$$d(y, y') = \begin{cases} \|y - y'\|_\infty & \text{if } \theta_s = \theta_{s'} \\ +\infty & \text{if } \theta_s \neq \theta_{s'} \end{cases}$$

- $X^0 = \mathbb{R}^n \times P$.

Switched systems as transition systems

- For $z = (x, p) \in X$, $z' = (x', p') \in X$, $u = (\bar{p}, \theta_s) \in U$, $y \in Y$,

$$(z, u, z', y) \in \Delta \iff \begin{cases} (\bar{p}, \theta_s) \in \{p\} \times \Theta_\tau^N \cup (P \setminus \{p\}) \times \Theta_\tau^{N_d} \\ x' = \mathbf{x}(\theta_s, x, \bar{p}) \text{ and } p' = \bar{p}. \\ y = \mathbf{x}|_{\theta_s}(., x, \bar{p}) \end{cases}$$



- $T_\tau^N(\Sigma_{\tau_d})$ is deterministic and metric.

Computation of the symbolic model

- We approximate $\mathbb{R}^n$ by a sequence of embedded multiscale lattices

$$[\mathbb{R}^n]_{2^{-s}\eta} = \left\{ q \in \mathbb{R}^n \;\middle|\; q[i] = k_i \frac{2^{-s+1}\eta}{\sqrt{n}},\ k_i \in \mathbb{Z},\ i = 1, ..., n \right\}$$

  where $\eta \in \mathbb{R}^+$ is a state space sampling parameter.

- We associate a multiscale quantizer $Q^s_\eta : \mathbb{R}^n \to [\mathbb{R}^n]_{2^{-s}\eta}$ such that

$$Q^s_\eta(x) = q \iff q[i] - \frac{2^{-s}\eta}{\sqrt{n}} \leq x[i] < q[i] + \frac{2^{-s}\eta}{\sqrt{n}},\ i = 1, \ldots, n.$$

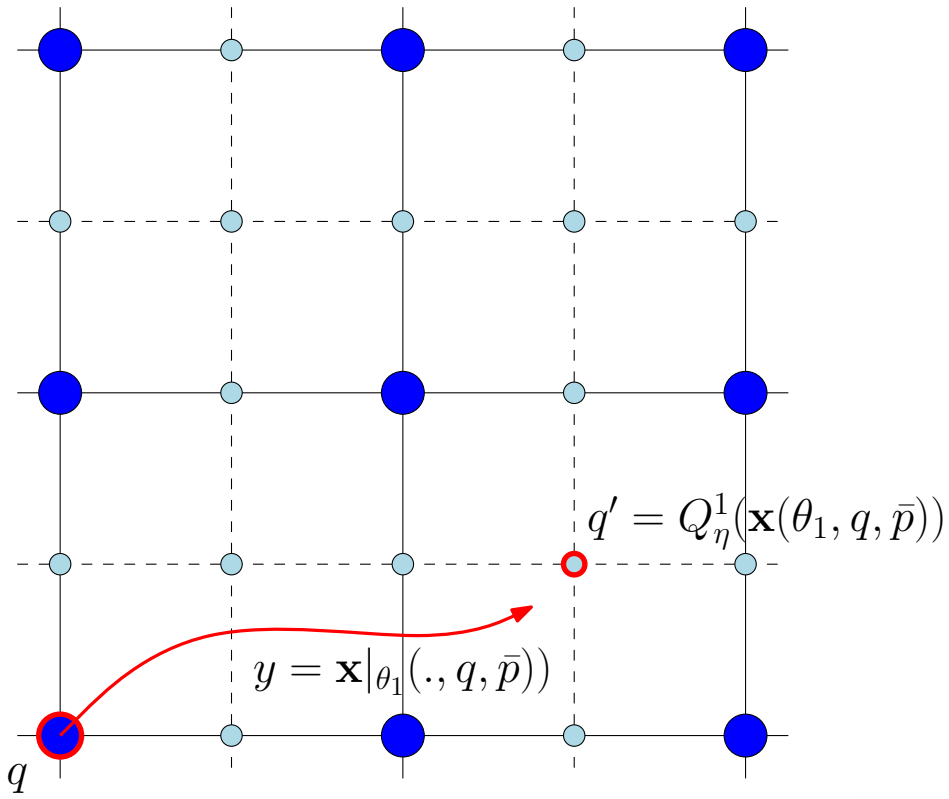
- Let $X^s_\eta = [\mathbb{R}^n]_{2^{-s}\eta} \times P$, then $X^0_\eta \subseteq X^1_\eta \subseteq \cdots \subseteq X^N_\eta$.

- We define the symbolic model as $T^N_{\tau,\eta}(\Sigma_{\tau_d}) = (X^N_\eta, U, Y, \Delta_\eta, X^0_\eta)$.

Computation of the symbolic model

- For $r = (q, p) \in X$, $r' = (q', p') \in X$, $u = (\bar{p}, \theta_s) \in U$, $y \in Y$,

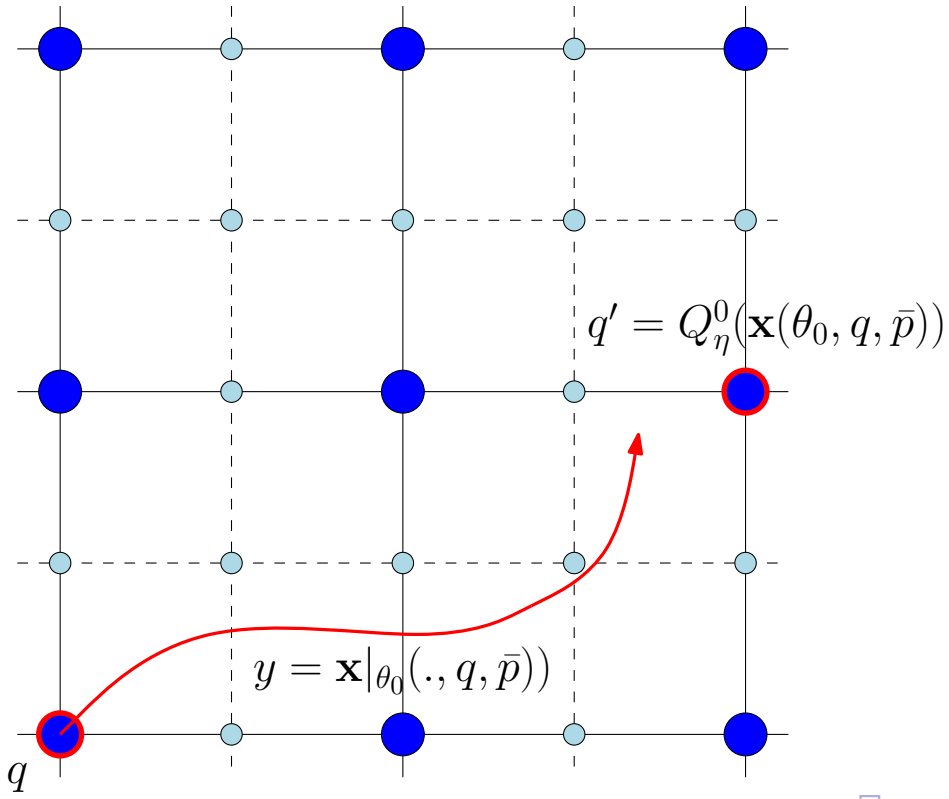
$$(r, u, r', y) \in \Delta \iff \begin{cases} (\bar{p}, \theta_s) \in \{p\} \times \Theta_\tau^N \cup (P \setminus \{p\}) \times \Theta_\tau^{N_d} \\ q' = Q_\eta^s(\mathbf{x}(\theta_s, q, \bar{p})) \text{ and } p' = \bar{p}. \\ y = \mathbf{x}|_{\theta_s}(., q, \bar{p}) \end{cases}$$



Computation of the symbolic model

- For $r = (q, p) \in X$, $r' = (q', p') \in X$, $u = (\bar{p}, \theta_s) \in U$, $y \in Y$,

$$(r, u, r', y) \in \Delta \iff \begin{cases} (\bar{p}, \theta_s) \in \{p\} \times \Theta_\tau^N \cup (P \setminus \{p\}) \times \Theta_\tau^{N_d} \\ q' = Q_\eta^s(\mathbf{x}(\theta_s, q, \bar{p})) \text{ and } p' = \bar{p}. \\ y = \mathbf{x}|_{\theta_s}(., q, \bar{p}) \end{cases}$$



Approximation result

$T_\tau^N(\Sigma_{\tau_d})$ is symbolic, deterministic and metric.

Theorem

Let Σ_{τ_d} admit multiple δ-GUAS Lyapunov functions V_p, $p \in P$. Consider parameters $\tau, \eta \in \mathbb{R}^+$, $N \in \mathbb{N}$, and a precision $\varepsilon \in \mathbb{R}^+$. If $\tau_d > \frac{\log \mu}{\kappa}$ and

$$\eta \leq \min \left\{ \begin{array}{l} \min\limits_{s=0}^{s=N_d} \left[2^s \gamma^{-1} \left(\left(\frac{1}{\mu} - e^{-\kappa\theta_s} \right) \underline{\alpha}(\varepsilon) \right) \right], \\ \min\limits_{s=0}^{s=N} \left[2^s \gamma^{-1} \left(\frac{1 - e^{-\kappa\theta_s}}{\mu} \underline{\alpha}(\varepsilon) \right) \right], \overline{\alpha}^{-1} \left(\frac{1}{\mu} \underline{\alpha}(\varepsilon) \right) \end{array} \right\}$$

then $T_\tau^N(\Sigma_{\tau_d}) \sim_\varepsilon T_{\tau,\eta}^N(\Sigma_{\tau_d})$.

Outline

1. Incrementally stable switched systems
2. Multiscale symbolic models
3. Safety controller synthesis using multiscale symbolic models
4. Computational experiments

Safety specification

- Let $T = (X, U, Y, \Delta, X^0)$ be a symbolic, deterministic transition system where

$$Y \subseteq \bigcup_{\theta_y \in \mathbb{R}^+} \mathcal{C}([0, \theta_y], \mathbb{R}^n).$$

- Let $S \subseteq \mathbb{R}^n$ be a subset of safe states.
- We define the transition system $T_S = (X, U, Y, \Delta_S, X^0)$ where for $x, x' \in X$, $u \in U$, $y \in Y$,

$$(x', y) \in \Delta_S(x, u) \iff \begin{cases} u \in \mathrm{enab}(x); \\ (x', y) = \Delta(x, u); \\ \forall t \in [0, \theta_y],\ y(t) \in S. \end{cases}$$

- T_S is symbolic and deterministic.
- Remark: safety is defined on continuous-time outputs.

Safety controller

Definition

A safety controller for $T_S = (X, U, Y, \Delta_S, X^0)$ is a relation $C \subseteq X \times U$ such that for all $x \in X$:

- $C(x) \subseteq \mathrm{enab}(x)$;
- if $C(x) \neq \emptyset$, then $\forall u \in C(x)$, $C(x') \neq \emptyset$ with $\Delta_S(x, u) = (x', y)$.

We denote the domain of C as $\mathrm{dom}(C) = \{x \in X |\ C(x) \neq \emptyset\}$.

- The controlled transition system is $T_{S/C} = (X, U, Y, \Delta_{S/C}, X_C^0)$ where $X_C^0 = X^0 \cap \mathrm{dom}(C)$ and for $x, x' \in X$, $u \in U$, $y \in Y$,

$$(x', y) \in \Delta_{S/C}(x, u) \iff \begin{cases} u \in C(x); \\ (x', y) = \Delta_S(x, u). \end{cases}$$

- $T_{S/C}$ is symbolic, deterministic and non-blocking.

Maximal safety controller

Lemma

There exists a unique maximal safety controller $C^* \subseteq X \times U$ *such that for all safety controllers* C, $C \subseteq C^*$.

Definition

A state $x \in X$ is safety controllable if and only if $x \in \mathrm{dom}(C^*)$. The set of safety controllable states is denoted $\mathrm{cont}(T_S)$.

Computation of C^* requires complete exploration of T_S.

Lazy safety synthesis

- Lazy safety synthesis: trade-off between maximality and efficiency.
  - Give priority to inputs with longer duration, which lead to states on coarser grids.
  - Compute the symbolic model on the fly.
  - Finer scales are explored (computed) only if safety cannot be ensured at the coarser scales.
- Let us define a priority relation on inputs: total preorder $\preceq \subseteq U \times U$
  - The associated equivalence and strict weak order relations are

$$\begin{aligned} u \simeq u' &\iff u \preceq u' \text{ and } u' \preceq u; \\ u \prec u' &\iff u \preceq u' \text{ and } u \not\simeq u'. \end{aligned}$$

  - For multiscale symbolic models where $U = P \times \Theta_\tau^N$:

$$\begin{aligned} (p, \theta_s) \preceq (p', \theta_s') &\iff \theta_s \leq \theta_s'; \\ (p, \theta_s) \simeq (p', \theta_s') &\iff \theta_s = \theta_s'; \\ (p, \theta_s) \prec (p', \theta_s') &\iff \theta_s < \theta_s'. \end{aligned}$$

Maximal lazy safety controller

Definition

A maximal lazy safety (MLS) controller for $T_S = (X, U, Y, \Delta_S, X^0)$ is a safety controller $C \subseteq X \times U$ such that:

- all safety controllable initial states are in $\mathrm{dom}(C)$:

$$X^0 \cap \mathrm{cont}(T_S) \subseteq \mathrm{dom}(C);$$

- all states $x \in \mathrm{dom}(C)$ are reachable in $T_{S/C}$;
- for all states $x \in \mathrm{dom}(C)$:
  1. if $u \in C(x)$, then $\forall u' \in \mathrm{enab}(x)$ with $u \simeq u'$, $(x', y) = \Delta_S(x, u')$,

$$u' \in C(z) \iff x' \in \mathrm{cont}(T_S);$$

  2. if $u \in C(x)$, then $\forall u' \in \mathrm{enab}(x)$ with $u \prec u'$, $(x', y) = \Delta_S(x, u')$,

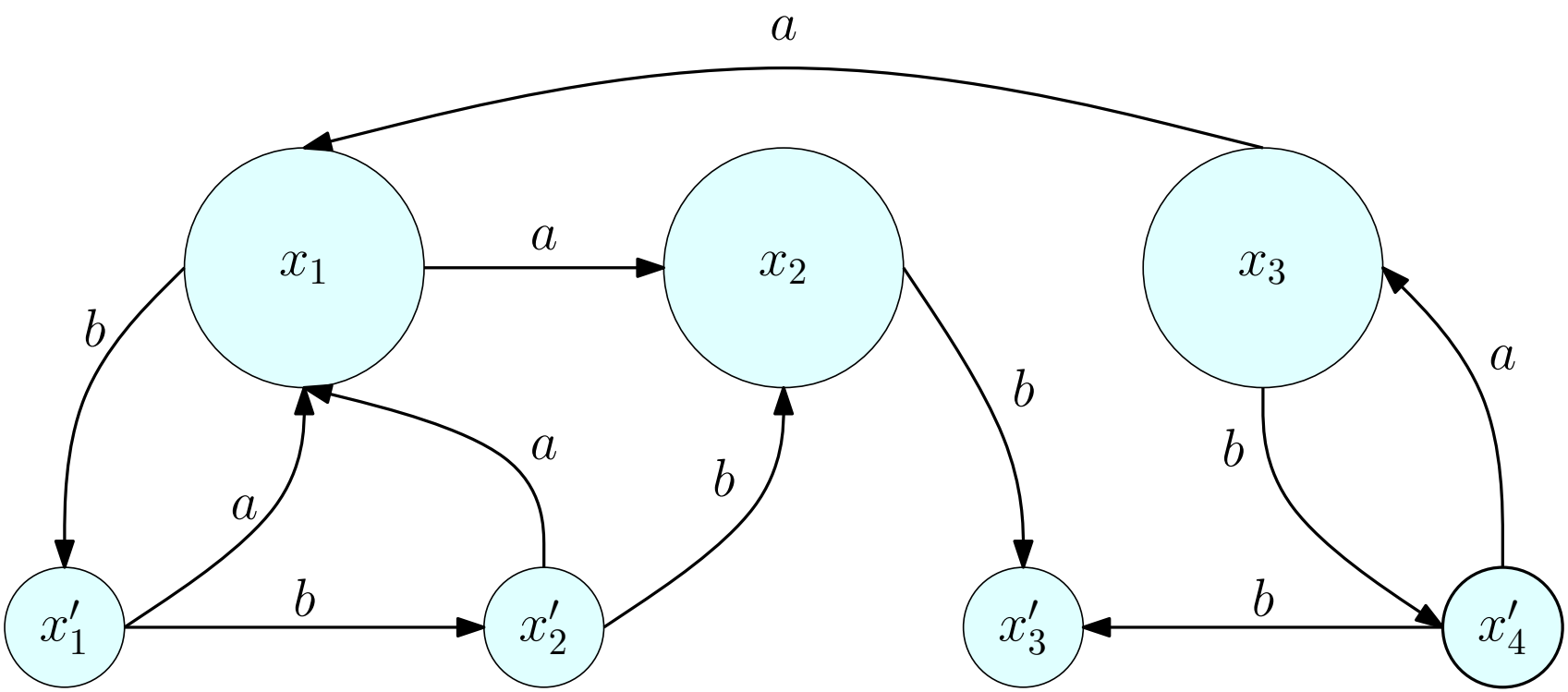
$$x' \notin \mathrm{cont}(T_S).$$

Maximal lazy safety controller

Theorem

There exists a unique MLS controller for T_S.

MLS controller synthesis: $X_0 = \{x_1, x_2, x_3\}$, $b \prec a$.

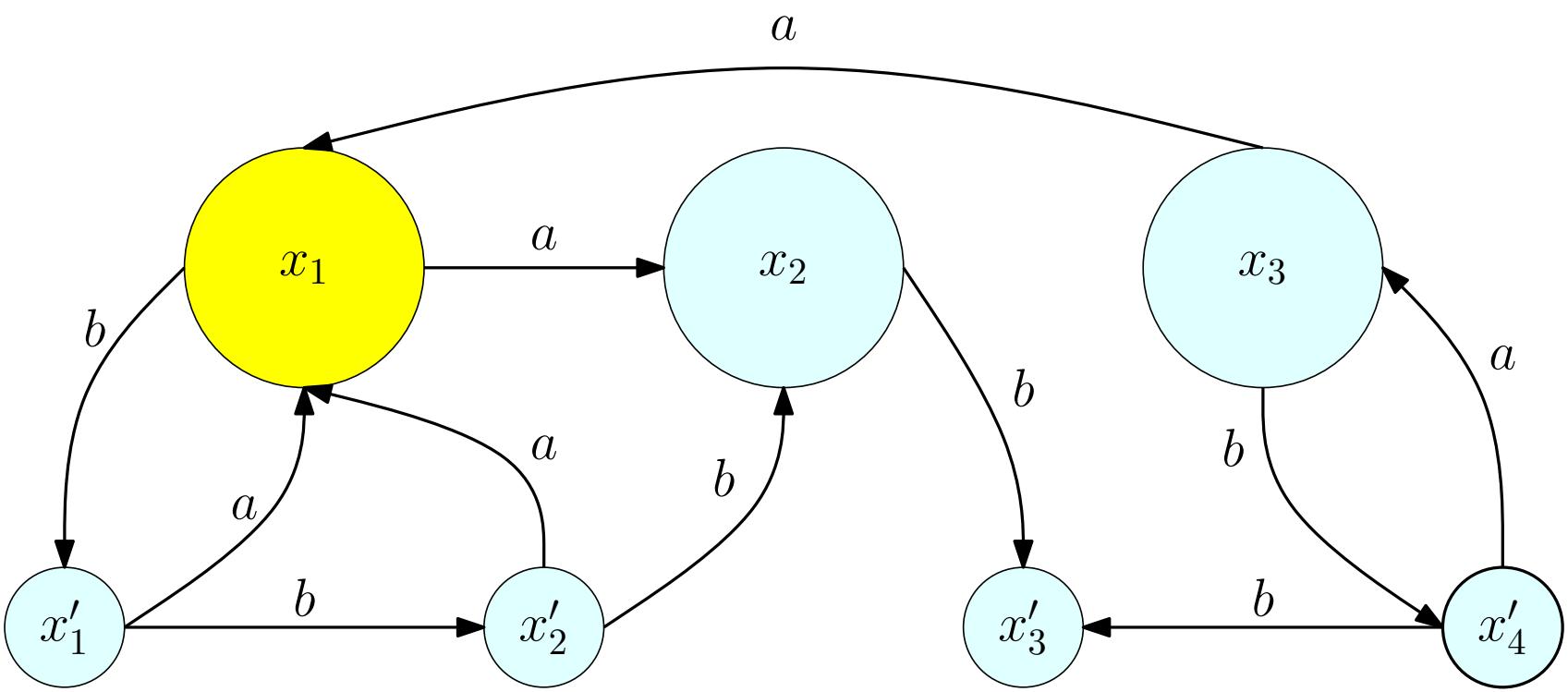


Maximal lazy safety controller

Theorem

There exists a unique MLS controller for T_S.

MLS controller synthesis: $X_0 = \{x_1, x_2, x_3\}$, $b \prec a$.

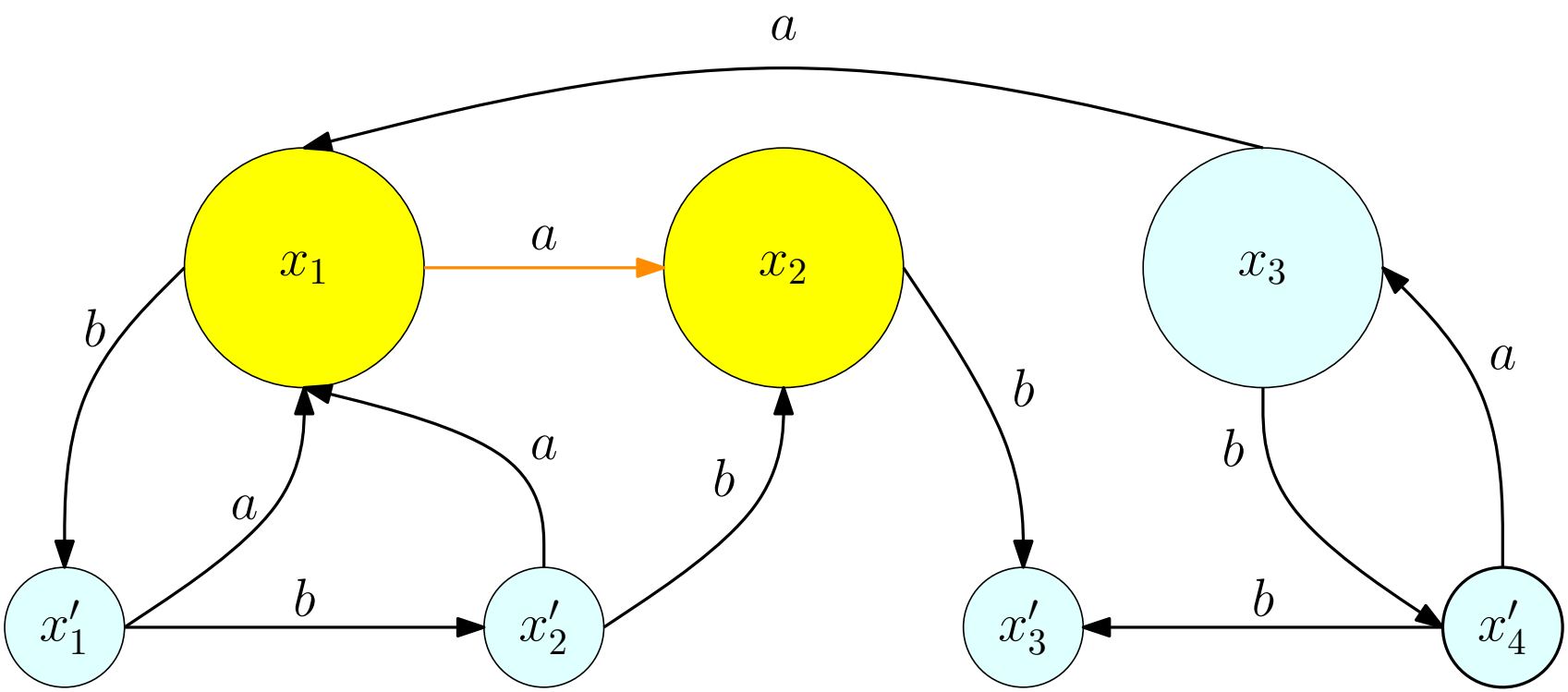


Maximal lazy safety controller

Theorem

There exists a unique MLS controller for T_S.

MLS controller synthesis: $X_0 = \{x_1, x_2, x_3\}$, $b \prec a$.

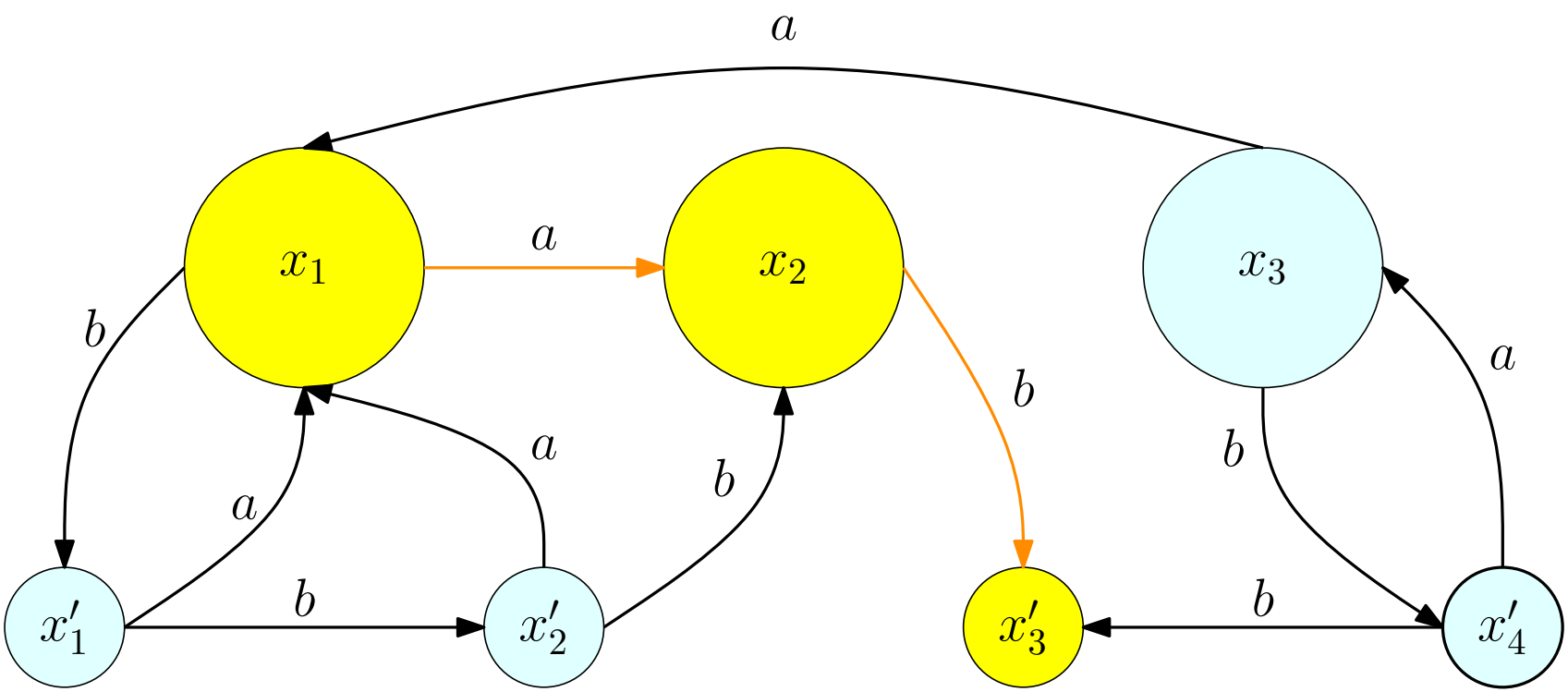


Maximal lazy safety controller

Theorem

There exists a unique MLS controller for T_S.

MLS controller synthesis: $X_0 = \{x_1, x_2, x_3\}$, $b \prec a$.

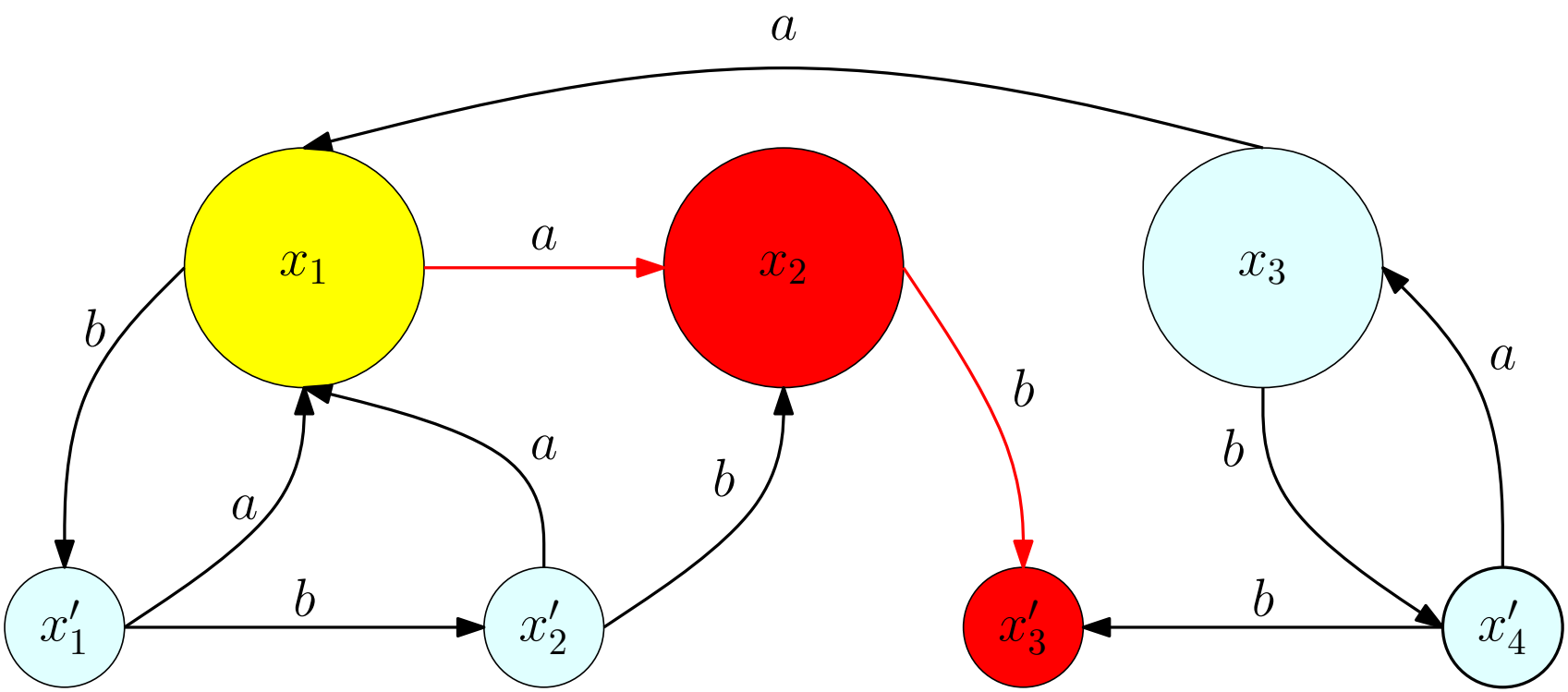


Maximal lazy safety controller

Theorem

There exists a unique MLS controller for T_S.

MLS controller synthesis: $X_0 = \{x_1, x_2, x_3\}$, $b \prec a$.

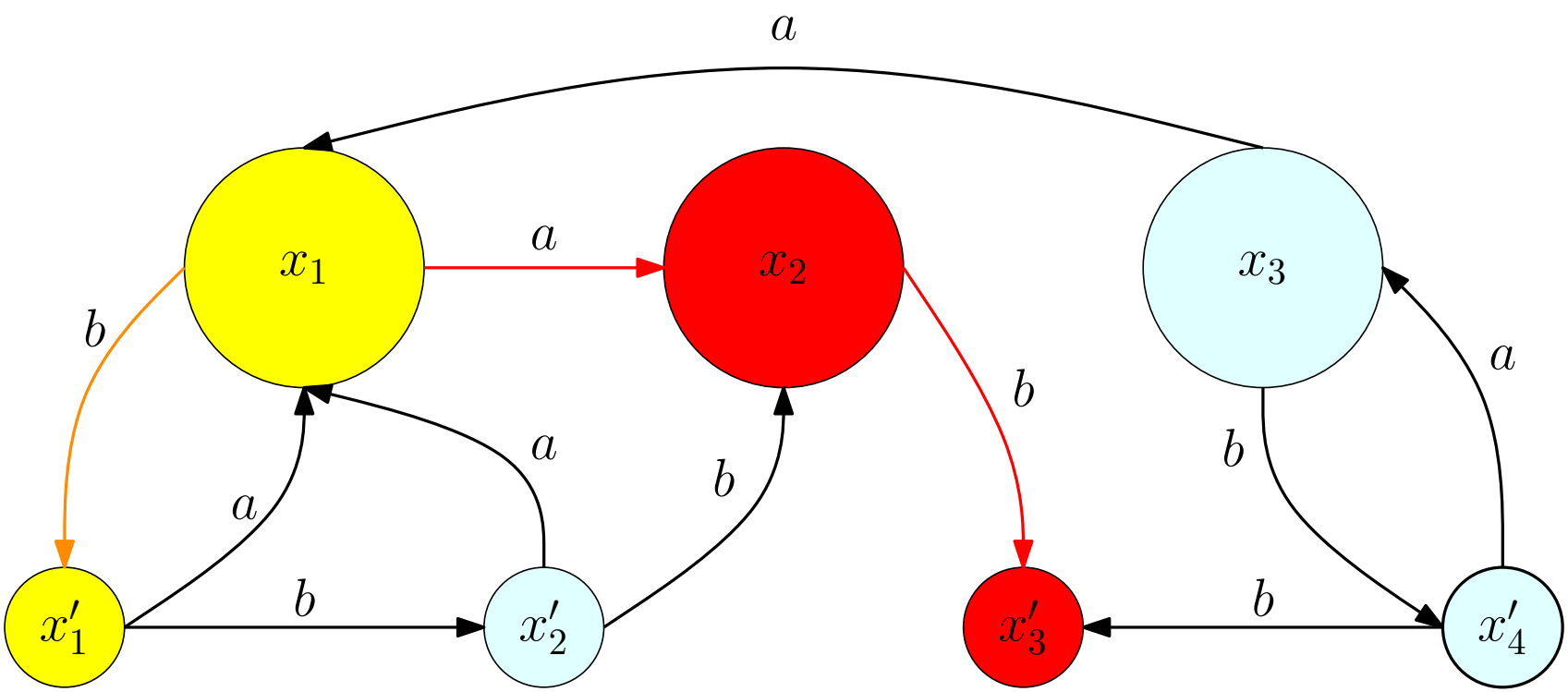


Maximal lazy safety controller

Theorem

There exists a unique MLS controller for T_S.

MLS controller synthesis: $X_0 = \{x_1, x_2, x_3\}$, $b \prec a$.

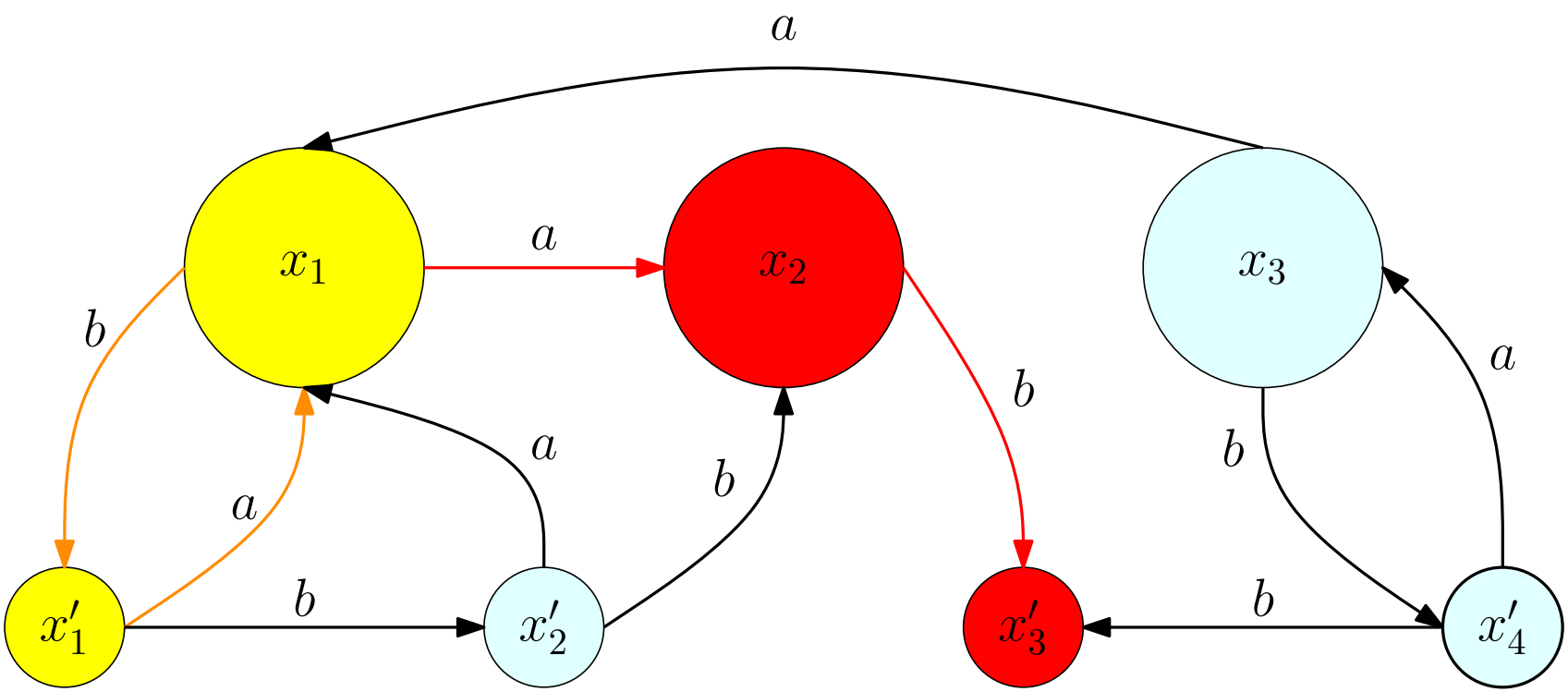


Maximal lazy safety controller

Theorem

There exists a unique MLS controller for T_S.

MLS controller synthesis: $X_0 = \{x_1, x_2, x_3\}$, $b \prec a$.

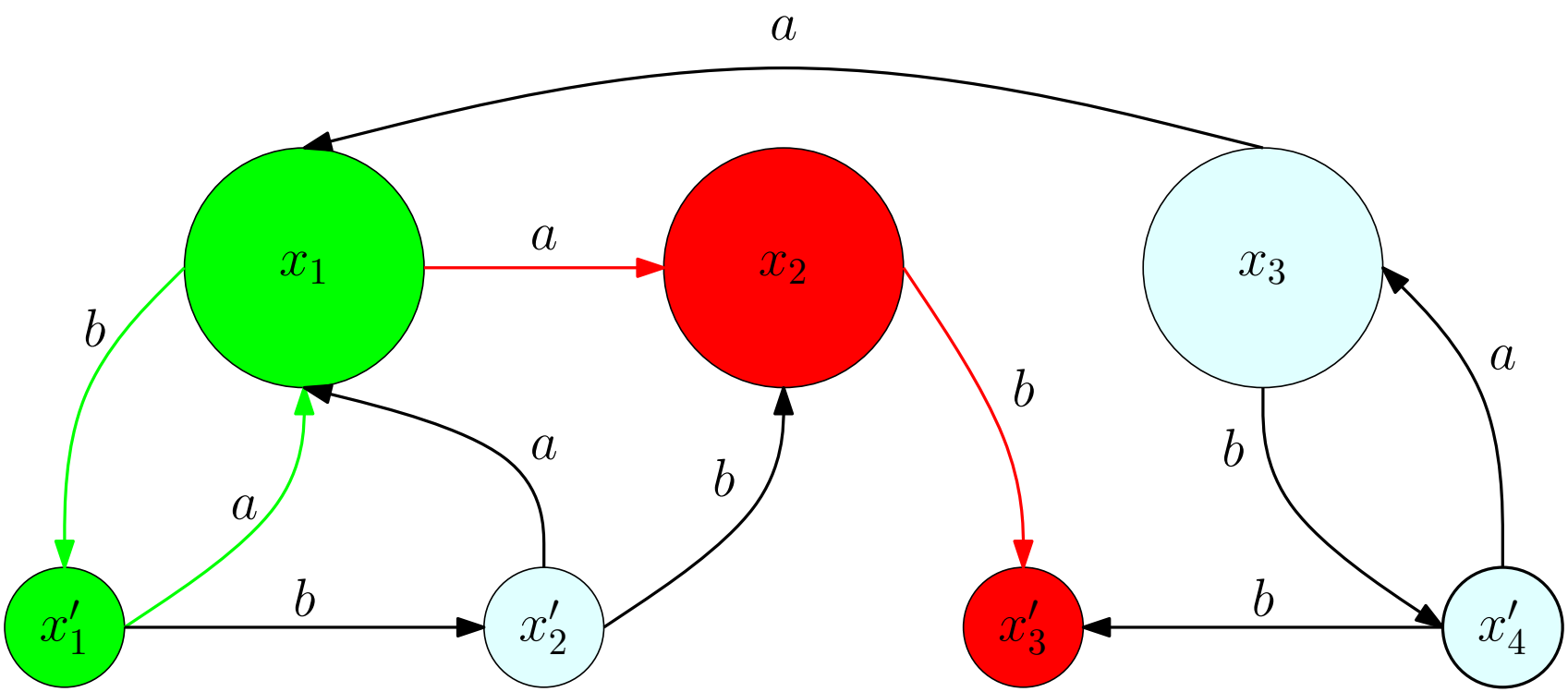


Maximal lazy safety controller

Theorem

There exists a unique MLS controller for T_S.

MLS controller synthesis: $X_0 = \{x_1, x_2, x_3\}$, $b \prec a$.

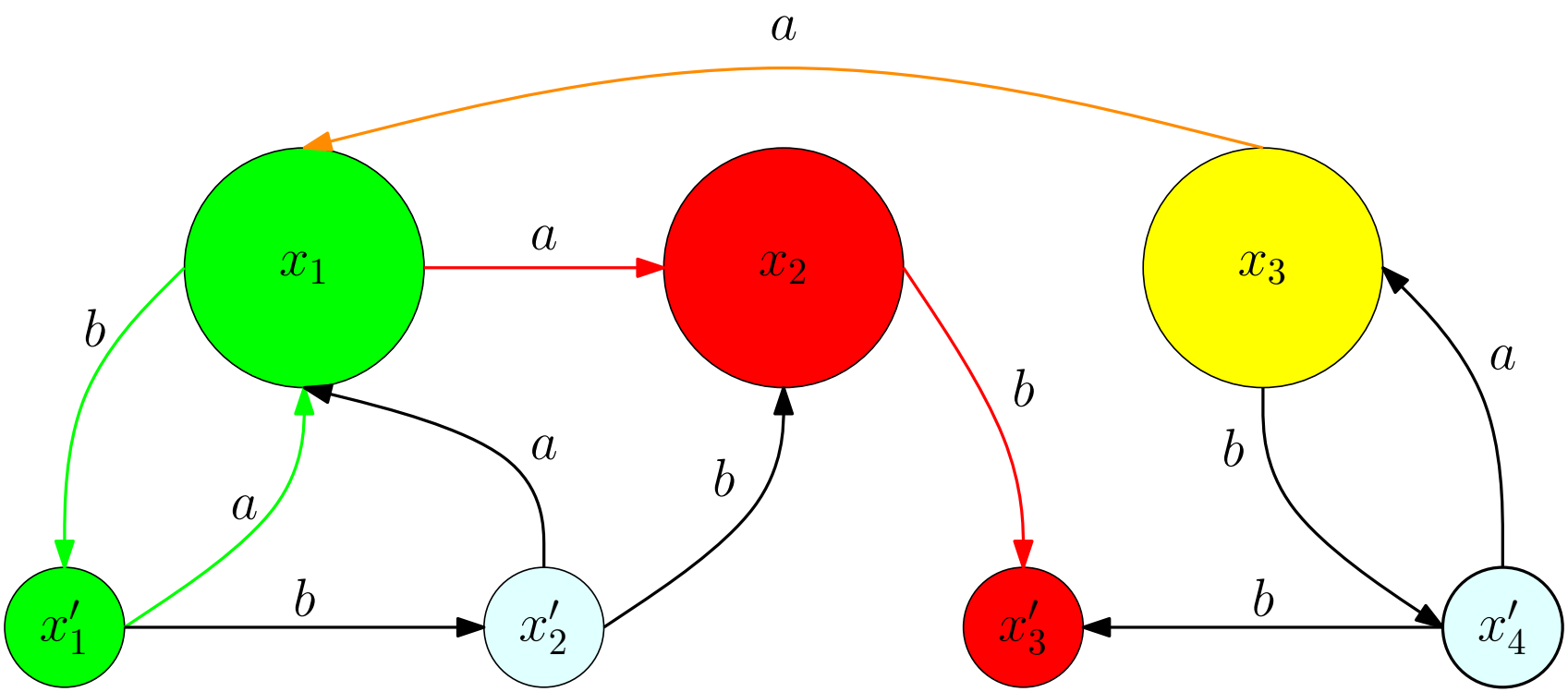


Maximal lazy safety controller

Theorem

There exists a unique MLS controller for T_S.

MLS controller synthesis: $X_0 = \{x_1, x_2, x_3\}$, $b \prec a$.

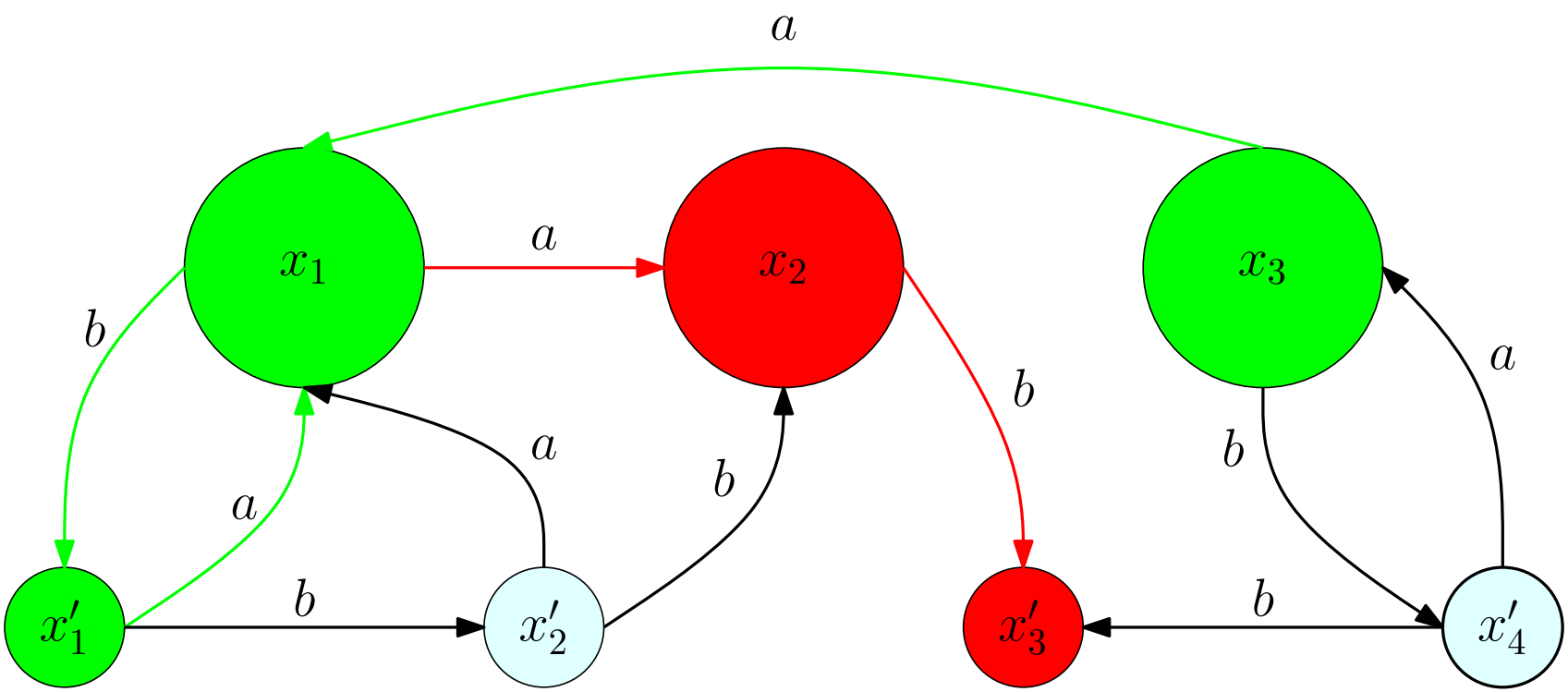


Maximal lazy safety controller

Theorem

There exists a unique MLS controller for T_S.

MLS controller synthesis: $X_0 = \{x_1, x_2, x_3\}$, $b \prec a$.



Outline

1. Incrementally stable switched systems
2. Multiscale symbolic models
3. Safety controller synthesis using multiscale symbolic models
4. Computational experiments

Switched system with dwell-time

- We consider the switched system:

$$\dot{\mathbf{x}}(t) = A_{\mathbf{p}(t)}\mathbf{x}(t) + b_{\mathbf{p}(t)},\ \mathbf{p}(t) \in \{1, 2\},\ \text{with}$$

$$A_1 = \begin{bmatrix} -0.25 & 1 \\ -2 & -0.25 \end{bmatrix},\ A_2 = \begin{bmatrix} -0.25 & 2 \\ -1 & -0.25 \end{bmatrix},\ b_1 = \begin{bmatrix} -0.25 \\ -2 \end{bmatrix},\ b_2 = \begin{bmatrix} 0.25 \\ 1 \end{bmatrix}.$$

- The switched system admits multiple δ-GUAS Lyapunov functions and is incrementally stable for switching signals with minimum dwell-time $\tau_d = 2$.
- Multiscale abstraction with parameters $\tau = 4$, $\eta = \frac{8}{100\sqrt{2}}$, $N = 3$
  Uniform abstraction with parameters $\tau = \frac{1}{2}$, $\eta = \frac{1}{100\sqrt{2}}$
  $\Longrightarrow$ precision $\varepsilon = 0.4$.
- Safe set: $S = [-6, 6] \times [-4, 4] \setminus [-1.5, 1.5] \times [-1, 1]$.

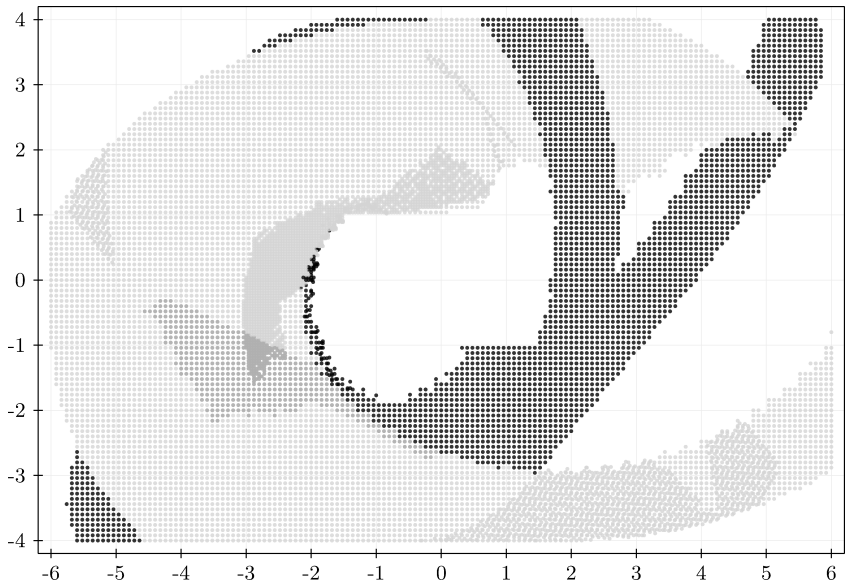
Switched system with dwell-time

Controller synthesis:

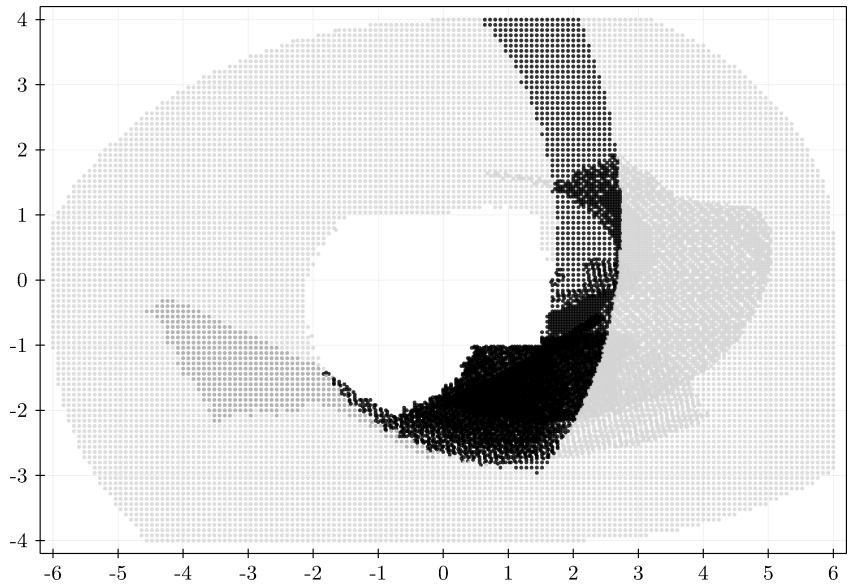
	Uniform symbolic model	Multiscale symbolic model
Time	160s	7.3s
Size (10^3)	5228	33
Durations	0.5 (100%)	4 (26%) 2 (54%) 1 (11% 0.5 (9%)

Switched system with dwell-time

MLS Controller:



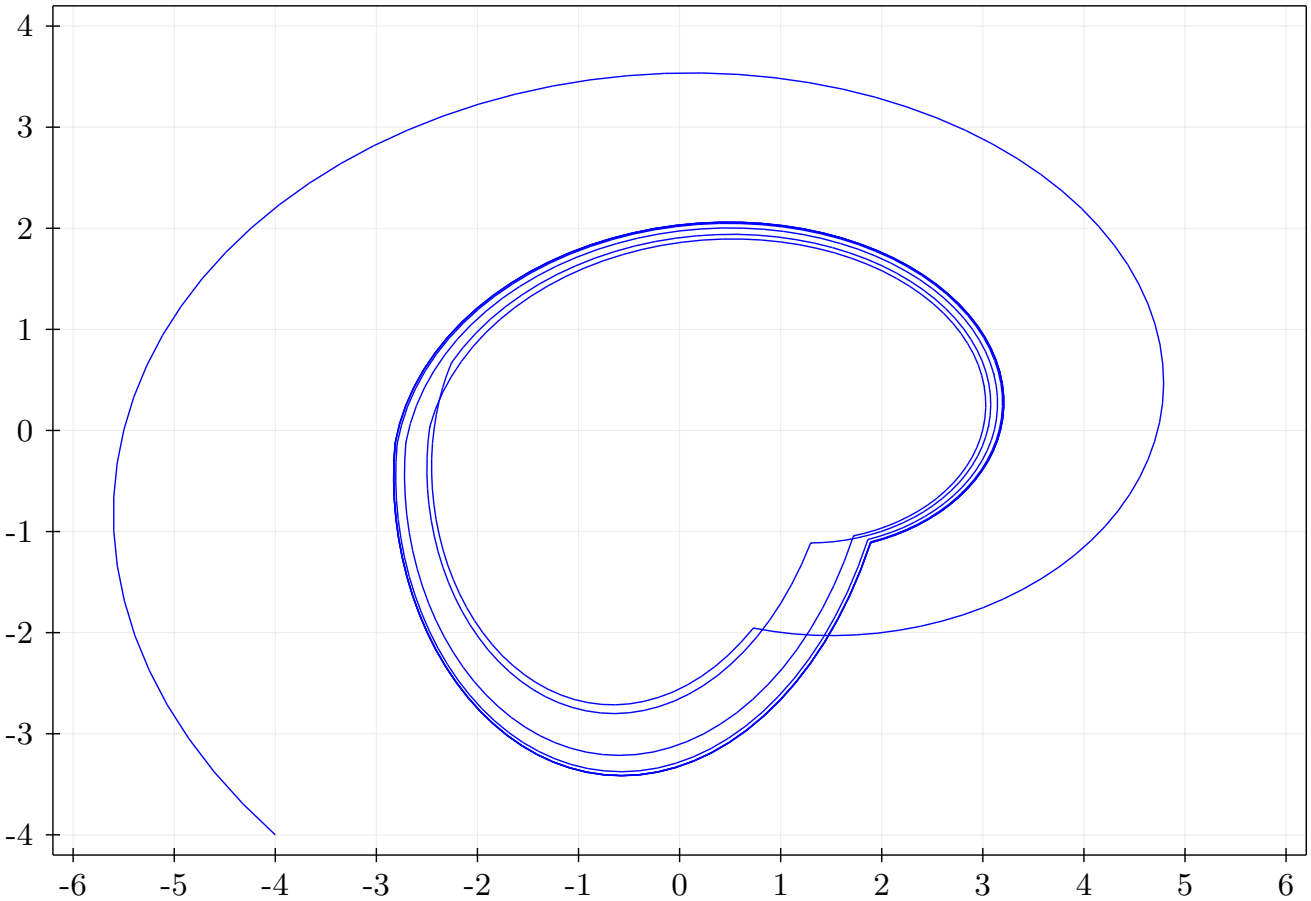
Mode 1 is active



Mode 2 is active

Switched system with dwell-time

Controlled switched system:



Circular n-room building

- We consider the system:

$$\begin{aligned}\dot{\mathbf{T}}_i(t) &= \alpha(\mathbf{T}_{i+1}(t) + \mathbf{T}_{i-1}(t) - 2\mathbf{T}_i(t)) \\ &\quad +\beta(t_e - \mathbf{T}_i(t)) + \gamma(t_h - \mathbf{T}_i(t))\mathbf{u}_i(t)\end{aligned}$$

  where:
  - $\mathbf{T}_i(t)$ is the temperature of room i, $1 \leq i \leq n$, $\mathbf{T}_0(t) = \mathbf{T}_n(t)$ and $\mathbf{T}_{n+1}(t) = \mathbf{T}_1(t)$.
  - $\mathbf{u}_i(t) = 1$ if room i is heated, $\mathbf{u}_i(t) = 0$ otherwise and $\sum_{i=1}^{n} \mathbf{u}_i(t) \leq 1$.
- n-dimensional switched system with $n+1$ modes admits a common Lyapunov function and is incrementally stable.
- Multiscale abstraction with parameters $\tau = 80$, $\eta = 0.28$, $N = 4$ $\Longrightarrow$ Precision $\varepsilon = 0.4$.
- Safe set: $S = [19, 21.5]^n$.

Circular n-room building

Controller synthesis:

	Multiscale symbolic models		
	$n = 3$	$n = 4$	$n = 5$
Time	0.2s	6s	312s
Size (10^3)	2	45	1 077
Durations	40 (1%) 20 (37%) 10 (62%)	20 (25%) 10 (73%) 5 (2%)	20 (6%) 10 (92%) 5 (2%)

Computational complexity increases with dimension:

- State and input space are larger.
- The control problem is also intrinsically more complex in higher dimension because of the constraint:

$$\sum_{i=1}^{n} \mathbf{u}_i(t) \leq 1.$$

Conclusions

- Multiscale approximately bisimilar symbolic models for incrementally stable switched systems:
  - Based on multiscale sampling of time and space;
  - Allow significant complexity reduction for controller synthesis.
- Multiscale safety controller synthesis:
  - Based on the notion of maximal lazy safety controller;
  - Partial exploration of the symbolic abstractions;
  - Can be extended to more general safety properties, e.g. specified by a hybrid automaton.
- Future work:
  - MLS controller synthesis algorithm for non-deterministic systems;
  - Consider other types of specifications, e.g. reachability: maximal lazy reachability controller may not be unique.

Girard, Gössler and Mouelhi, *Safety controller synthesis for incrementally stable switched systems using multiscale symbolic models*. IEEE TAC, 2016.