# Low-Complexity Switching Controllers for Safety using Symbolic Models ⋆

**Antoine Girard** *

* *Laboratoire Jean Kuntzmann, Université de Grenoble, B.P. 53, 38041 Grenoble, France (e-mail: Antoine.Girard@imag.fr).*

**Abstract:** In this paper, we consider the problem of synthesizing low-complexity safety controllers for incrementally stable switched systems. For that purpose, we establish a new approximation result for the computation of symbolic models that are approximately bisimilar to a given switched system. The main advantage over existing results is that it allows us to design quantized switching controllers for safety specifications; these can be computed offline and therefore the online execution time is greatly reduced. Then, we present a technique to reduce the memory needed to store the control law by borrowing ideas from algebraic decision diagrams for compact function representation and by exploiting the non-determinism inherent to safety controllers. We show the merits of our approach by applying it to a simple model of temperature regulation in a building.

Keywords: Switched systems; Symbolic models; Approximate bisimulation; Safety.

## 1. INTRODUCTION

The use of discrete abstractions or symbolic models has become quite popular for hybrid systems design (see e.g. Raisch and O'Young [1998], Moor and Raisch [1999], Tabuada and Pappas [2006], Kloetzer and Belta [2006], Reißig [2009]). In particular, several recent works have focused on the use of symbolic models related to the original system by approximate equivalence relationships (approximate bisimulations, Tazaki and Imura [2008], Girard et al. [2010]; or approximate alternating bisimulation relations, Pola and Tabuada [2009], Mazo Jr. and Tabuada [2010]) which give more flexibility in the abstraction process by allowing the observed behaviors of the symbolic model and of the original system to be different provided they remain close. These approximate behavioral relationships have enabled the development of new abstraction-based controller synthesis techniques (Tabuada [2009], Girard [2011]).

In this paper, we go one step further by pursuing the goal of synthesizing controllers of lower complexity with shorter execution time and more efficient memory usage for their encoding. For that purpose, we establish a new approximation result for the computation of symbolic models that are approximately bisimilar to a given incrementally stable switched system. This result slightly differs from the original result presented by Girard et al. [2010] and this difference is fundamental for the synthesis of controllers with lower complexity. Indeed, the combination of this new result with synthesis techniques safety specifications presented in Girard [2011] yields quantized switching controllers that can be entirely computed offline. The online execution time is then greatly reduced in comparison to controllers obtained using the previous existing approximation result. We then consider the problem of the representation of the control law with the goal of reducing the memory needed for its storage. This is done by using ideas from algebraic decision diagrams (see e.g. Bahar et al. [1993]) for compact function representation. Also, the non-determinism inherent to safety controllers can be exploited to further simplify the representation of the control law. Finally, we apply our approach to the synthesis of a controller for a simple model of temperature regulation in a building.

⋆ This work was supported by the Agence Nationale de la Recherche (VEDECY project - ANR 2009 SEGI 015 01).

## 2. SYMBOLIC MODELS FOR SWITCHED SYSTEMS

In this section, we present an approach for the computation of symbolic models (i.e. discrete abstractions) for a class of switched systems. This problem has been already considered by Girard et al. [2010]. In the following, we present a slightly different abstraction result that will allow us to synthesize controllers with lower complexity.

### *2.1 Switched systems*

In this paper, we consider a class of switched systems of the form:

$$\Sigma : \ \dot{\mathbf{x}}(t) = f_{\mathbf{p}(t)}(\mathbf{x}(t)), \ \mathbf{x}(t) \in \mathbb{R}^n, \ \mathbf{p}(t) \in P$$

where $P$ is a finite set of modes. We will assume that the switched system $\Sigma$ is incrementally globally uniformly asymptotically stable ($\delta$-GUAS, Angeli [2002]). Intuitively, a switched system is $\delta$-GUAS if the distance between any two trajectories associated with the same switching signal $\mathbf{p}$, but with different initial states, converges asymptotically to 0. Incremental stability of a switched system can be characterized using Lyapunov functions (Girard et al. [2010]).

*Definition 1.* A smooth function $\mathcal{V} : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^+$ is a common $\delta$-GUAS Lyapunov function for $\Sigma$ if there exist $\mathcal{K}_\infty$ functions [1] $\underline{\alpha}$, $\overline{\alpha}$ and a real number $\kappa > 0$ such that for all $x, y \in \mathbb{R}^n$, for all $p \in P$:

$$\underline{\alpha}(\|x-y\|) \leq \mathcal{V}(x,y) \leq \overline{\alpha}(\|x-y\|);$$
$$\frac{\partial \mathcal{V}}{\partial x}(x,y) \cdot f_p(x) + \frac{\partial \mathcal{V}}{\partial y}(x,y) \cdot f_p(y) \leq -\kappa \mathcal{V}(x,y).$$

It can be shown that the existence of a common $\delta$-GUAS Lyapunov function ensures that the switched system $\Sigma$ is $\delta$-GUAS.

We now introduce the class of transition systems which will serve as a common modeling framework for switched systems and symbolic models.

*Definition 2.* A *transition system* $T = (X, U, \mathcal{S}, Y, \mathcal{O})$ consists of:

- a set of states $X$;
- a set of inputs $U$;
- a (set-valued) transition map $\mathcal{S} : X \times U \to 2^X$;
- a set of outputs $Y$;
- and an output map $\mathcal{O} : X \to Y$.

$T$ is *metric* if the set of outputs $Y$ is equipped with a metric $d$. If the set of states $X$ and inputs $U$ are finite or countable, $T$ is said *symbolic* or *discrete*.

An input $u \in U$ belongs to the set of *enabled inputs* at state $x$, denoted $\mathrm{Enab}(x)$, if $\mathcal{S}(x,u) \neq \emptyset$. If $\mathrm{Enab}(x) \neq \emptyset$, then the state $x$ is said to be *non-blocking*, otherwise it said to be *blocking*. The system is said to be non-blocking if all states are non-blocking. If for all $x \in X$ and for all $u \in \mathrm{Enab}(x)$, $\mathcal{S}(x,u)$ has 1 element then the transition system is said to be *deterministic*.

A *state trajectory* of $T$ is a finite or infinite sequence of states and inputs, $\{(x^i, u^i) |\ i = 0, \ldots, N\}$ (we can have $N = +\infty$) where $x^{i+1} \in \mathcal{S}(x^i, u^i)$ for all $i = 0, \ldots, N-1$. The associated *output trajectory* is the sequence of outputs $\{y^i |\ i = 0, \ldots, N\}$ where $y^i = \mathcal{O}(x^i)$ for all $i = 0, \ldots, N$.

Given a switched system $\Sigma$ and a parameter $\tau > 0$, we define a transition system $T_\tau(\Sigma)$ that describes trajectories of $\Sigma$ of duration $\tau$. This can be seen as a time sampling process, which is natural when the switching in $\Sigma$ is determined by a periodic controller of period $\tau$. Formally, $T_\tau(\Sigma) = (X_1, U, \mathcal{S}_1, Y, \mathcal{O}_1)$ where the set of states is $X_1 = \mathbb{R}^n$; the set of inputs is the set of modes $U = P$; the deterministic transition map is given by $x_1' = \mathcal{S}_1(x_1, p)$ if and only if

$$x_1' = \mathbf{x}(\tau), \text{ where } \dot{\mathbf{x}}(t) = f_p(\mathbf{x}(t)),\ \mathbf{x}(0) = x_1,\ t \in [0, \tau];$$

the set of outputs is $Y = \mathbb{R}^n$; and the observation map $\mathcal{O}_1$ is the identity map over $\mathbb{R}^n$. $T_\tau(\Sigma)$ is non-blocking, deterministic and metric when the set of observations $Y = \mathbb{R}^n$ is equipped with the Euclidean norm.

### *2.2 Symbolic models*

In the following, we present a method to compute discrete abstractions for $T_\tau(\Sigma)$. For that purpose, we consider approximate equivalence relationships for transition systems defined by approximate bisimulation relations introduced by Girard and Pappas [2007].

*Definition 3.* Let $T_i = (X_i, U, \mathcal{S}_i, Y, \mathcal{O}_i)$, $i = 1, 2$, be metric transition systems with the same sets of inputs $U$ and outputs $Y$ equipped with the metric $d$. Let $\varepsilon \geq 0$, a relation $\mathcal{R}_\varepsilon \subseteq X_1 \times X_2$ is called an *$\varepsilon$-approximate bisimulation relation* between $T_1$ and $T_2$, if for all $(x_1, x_2) \in \mathcal{R}_\varepsilon$:

(1) $d(\mathcal{O}_1(x_1), \mathcal{O}_2(x_2)) \leq \varepsilon$,
(2) $\forall u \in \mathrm{Enab}_1(x_1)$, $\forall x_1' \in \mathcal{S}_1(x_1, u)$, $\exists x_2' \in \mathcal{S}_2(x_2, u)$ such that $(x_1', x_2') \in \mathcal{R}_\varepsilon$.
(3) $\forall u \in \mathrm{Enab}_2(x_2)$, $\forall x_2' \in \mathcal{S}_2(x_2, u)$, $\exists x_1' \in \mathcal{S}_1(x_1, u)$ such that $(x_1', x_2') \in \mathcal{R}_\varepsilon$.

$T_1$ and $T_2$ are approximately bisimilar with precision $\varepsilon$ (denoted $T_1 \sim_\varepsilon T_2$), if there exists $\mathcal{R}_\varepsilon$, an $\varepsilon$-approximate bisimulation relation between $T_1$ and $T_2$, such that for all $x_1 \in X_1$, there exists $x_2 \in X_2$ such that $(x_1, x_2) \in \mathcal{R}_\varepsilon$, and conversely.

If $T_1$ is a system we want to control and $T_2$ is a simpler system that we want to use for controller synthesis, then $T_2$ is called an *approximately bisimilar abstraction* of $T_1$.

We briefly describe an approach similar to that presented by Girard et al. [2010] for computing approximately bisimilar discrete abstractions of $T_\tau(\Sigma)$. We start by approximating the set of states $X_1 = \mathbb{R}^n$ by a lattice:

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

where $q_i$ is the $i$-th coordinate of $q$ and $\eta > 0$ is a state space discretization parameter. We associate a quantizer $Q_\eta : \mathbb{R}^n \to [\mathbb{R}^n]_\eta$ defined as follows $q = Q_\eta(x)$ if and only if

$$\forall i = 1, \ldots, n,\ q_i - \tfrac{\eta}{\sqrt{n}} \leq x_i < q_i + \tfrac{\eta}{\sqrt{n}}.$$

By simple geometrical considerations, we can check that for all $x \in \mathbb{R}^n$, $\|Q_\eta(x) - x\| \leq \eta$.

We can then define the abstraction of $T_\tau(\Sigma)$ as the transition system $T_{\tau,\eta}(\Sigma) = (X_2, U, \mathcal{S}_2, Y, \mathcal{O}_2)$, where the set of states is $X_2 = [\mathbb{R}^n]_\eta$; the set of labels remains the same $U = P$; the transition relation is essentially obtained by quantizing the transition relation of $T_\tau(\Sigma)$:

$$\forall x_2 \in [\mathbb{R}^n]_\eta,\ \forall p \in P,\ \mathcal{S}_2(x_2, p) = Q_\eta(\mathcal{S}_1(x_2, p));$$

the set of outputs remains the same $Y = \mathbb{R}^n$; and the observation map $\mathcal{O}_2$ is given by $\mathcal{O}_2(q) = q$. Note that the transition system $T_{\tau,\eta}(\Sigma)$ is discrete since its sets of states and actions are respectively countable and finite. Moreover, it is non-blocking, deterministic and metric when the set of observations $Y = \mathbb{R}^n$ is equipped with the Euclidean norm.

The approximate bisimilarity of $T_\tau(\Sigma)$ and $T_{\tau,\eta}(\Sigma)$ is related to the incremental stability of switched system $\Sigma$. In the following, we shall assume that there exists a common $\delta$-GUAS Lyapunov function $\mathcal{V}$ for $\Sigma$. We need to make the supplementary assumption on the $\delta$-GUAS Lyapunov function that there exists a $\mathcal{K}_\infty$ function $\gamma$ such that for all $x_1, x_2, y_1, y_2 \in \mathbb{R}^n$

$$|\mathcal{V}(x_1, x_2) - \mathcal{V}(y_1, y_2)| \leq \gamma(\|x_1 - y_1\|) + \gamma(\|x_2 - y_2\|). \quad (1)$$

We can show that this assumption is not restrictive provided $\mathcal{V}$ is smooth and we are interested in the dynamics

[1] A continuous function $\gamma : \mathbb{R}^+ \to \mathbb{R}^+$ is said to belong to class $\mathcal{K}_\infty$ if it is strictly increasing, $\gamma(0) = 0$ and $\gamma(r) \to \infty$ when $r \to \infty$.

of $\Sigma$ on a compact subset of $\mathbb{R}^n$, which is often the case in practice.

We are now able to present a new approximation result for determining an approximate bisimulation relation between $T_\tau(\Sigma)$ and $T_{\tau,\eta}(\Sigma)$:

*Theorem 1.* Consider a switched system $\Sigma$, time and state space sampling parameters $\tau, \eta > 0$ and a desired precision $\varepsilon > 0$. If there exists a common $\delta$-GUAS Lyapunov function $\mathcal{V}$ for $\Sigma$ such that equation (1) holds and

$$\varepsilon \geq \eta + \underline{\alpha}^{-1}\left(\frac{2+e^{-\kappa\tau}}{1-e^{-\kappa\tau}}\gamma(\eta)\right) \tag{2}$$

then

$$\mathcal{R}_\varepsilon = \{(x_1, x_2) \in X_1 \times X_2 |\ \mathcal{V}(Q_\eta(x_1), x_2) \leq \underline{\alpha}(\varepsilon - \eta)\}$$

is an $\varepsilon$-approximate bisimulation relation between $T_\tau(\Sigma)$ and $T_{\tau,\eta}(\Sigma)$. Moreover, $T_\tau(\Sigma) \sim_\varepsilon T_{\tau,\eta}(\Sigma)$.

**Proof.** Let $(x_1, x_2) \in \mathcal{R}_\varepsilon$, then

$$\begin{aligned}\|x_1 - x_2\| &\leq \|Q_\eta(x_1) - x_2\| + \eta \\ &\leq \underline{\alpha}^{-1}\left(\mathcal{V}(Q_\eta(x_1), x_2)\right) + \eta \\ &\leq \underline{\alpha}^{-1}\left(\underline{\alpha}(\varepsilon - \eta)\right) + \eta = \varepsilon.\end{aligned}$$

Thus, the first condition of Definition 3 holds. Let us remark that $\mathrm{Enab}_1(x_1) = \mathrm{Enab}_2(x_2) = P$ and since $T_\tau(\Sigma)$ and $T_{\tau,\eta}(\Sigma)$ are deterministic, the second and third conditions are equivalent. Then, let $p \in P$, let $x_1' = \mathcal{S}_1(x_1, p)$ and $x_2' = \mathcal{S}_2(x_2, p)$ then using the properties of $\delta$-GUAS Lyapunov function $\mathcal{V}$ we obtain

$$\begin{aligned}\mathcal{V}(Q_\eta(x_1'), x_2') &= \mathcal{V}(Q_\eta(\mathcal{S}_1(x_1, p)), Q_\eta(\mathcal{S}_1(x_2, p))) \\ &\leq \mathcal{V}(\mathcal{S}_1(x_1, p), \mathcal{S}_1(x_2, p)) + 2\gamma(\eta) \\ &\leq e^{-\kappa\tau}\mathcal{V}(x_1, x_2) + 2\gamma(\eta) \\ &\leq e^{-\kappa\tau}\left(\mathcal{V}(Q_\eta(x_1), x_2) + \gamma(\eta)\right) + 2\gamma(\eta) \\ &\leq e^{-\kappa\tau}\underline{\alpha}(\varepsilon - \eta) + (2 + e^{-\kappa\tau})\gamma(\eta) \\ &\leq \underline{\alpha}(\varepsilon - \eta)\end{aligned}$$

by equation (2). It follows that $(x_1', x_2') \in \mathcal{R}_\varepsilon$ which is consequently an $\varepsilon$-approximate bisimulation relation between $T_\tau(\Sigma)$ and $T_{\tau,\eta}(\Sigma)$. Now, let $x_1 \in \mathbb{R}^n$ and let $x_2 \in [\mathbb{R}^n]_\eta$ given by $x_2 = Q_\eta(x_1)$. Then, $\mathcal{V}(Q_\eta(x_1), x_2) = 0$ and $(x_1, x_2) \in \mathcal{R}_\varepsilon$. Conversely, let $x_2 \in [\mathbb{R}^n]_\eta$ and let $x_1 \in \mathbb{R}^n$ given by $x_1 = x_2$, let us remark that $Q_\eta(x_1) = x_2$ then $\mathcal{V}(Q_\eta(x_1), x_2) = 0$ and $(x_1, x_2) \in \mathcal{R}_\varepsilon$. Hence, it follows that $T_\tau(\Sigma) \sim_\varepsilon T_{\tau,\eta}(\Sigma)$. ■

We would like to point out that for given $\tau > 0$ and $\varepsilon > 0$, it is always possible to find $\eta > 0$ such that equation (2) holds. Hence, it is possible for any time sampling parameter $\tau > 0$ to compute symbolic models for switched systems of arbitrary precision $\varepsilon > 0$ by choosing a sufficiently small state space sampling parameter $\eta > 0$.

We would like to emphasize the differences between Theorem 1 and the original approximation result presented by Girard et al. [2010]. The computation of the abstractions are essentially the same. The main difference lies in the expression of the approximate bisimulation relation: $(x_1, x_2) \in \mathcal{R}_\varepsilon$ if $\mathcal{V}(x_1, x_2) \leq \underline{\alpha}(\varepsilon)$ in the work by Girard et al. [2010], instead of $\mathcal{V}(Q_\eta(x_1), x_2) \leq \underline{\alpha}(\varepsilon - \eta)$ in Theorem 1. This difference will be very important in the following section as it will allow us to synthesize controllers that are simpler than those obtained using the previous existing result. It should also be noted that the different forms of approximate bisimulation relations imply that the relations to be satisfied by the abstraction parameters, $\tau$, $\eta$ and $\varepsilon$ are also quite different.

## 3. LOW-COMPLEXITY SAFETY CONTROLLERS

In this section, we present an approach for synthesizing low complexity safety controllers for switched systems. Our approach consists of two steps. First, using Theorem 1 and a result of Girard [2011], we show how to synthesize quantized safety controllers. Then, as the practical storage of these control laws might require a lot of memory, we present an approach to reduce the size of their encoding borrowing ideas from algebraic decision diagrams (ADD's, see e.g. in Bahar et al. [1993]) for compact function representation, and exploiting the non-determinism inherent to safety controllers.

### *3.1 Synthesis of quantized controllers*

We start by defining the notions of controllers and of safety controllers for transition systems.

*Definition 4.* A controller for transition system $T = (X, U, \mathcal{S}, Y, \mathcal{O})$ is a set-valued map $\mathcal{C} : X \to 2^U$ such that $\mathcal{C}(x) \subseteq \mathrm{Enab}(x)$, for all $x \in X$. The domain of $\mathcal{C}$ is the set $\mathrm{dom}(\mathcal{C}) = \{x \in X |\ \mathcal{C}(x) \neq \emptyset\}$. The dynamics of the controlled system is described by the transition system $T/\mathcal{C} = (X, U, \mathcal{S}_\mathcal{C}, Y, \mathcal{O})$ where the transition map is given by $x' \in \mathcal{S}_\mathcal{C}(x, u)$ if and only if $u \in \mathcal{C}(x)$ and $x' \in \mathcal{S}(x, u)$.

We would like to emphasize the fact that the controllers are set-valued maps, at a given state $x$ it enables a set of admissible inputs $\mathcal{C}(x) \subseteq U$. A controller essentially executes as follows. The state $x$ of $T$ is measured, an input $u \in \mathcal{C}(x)$ is selected and actuated. Then, the system takes a transition $x' \in \mathcal{S}(x, u)$. The blocking states of $T/\mathcal{C}$ are the elements of $X \setminus \mathrm{dom}(\mathcal{C})$.

*Definition 5.* Let $Y_S \subseteq Y$ be a set of *s*afe outputs. A controller $\mathcal{C}$ is a safety controller for $T$ and specification $Y_S$ if for all $x \in \mathrm{dom}(\mathcal{C})$:

(1) $\mathcal{O}(x) \in Y_S$ (safety);
(2) $\forall u \in \mathcal{C}(x)$, $\mathcal{S}(x, u) \subseteq \mathrm{dom}(\mathcal{C})$ (deadend freedom).

It is easy to verify from the previous definition that for any initial state $x^0 \in \mathrm{dom}(\mathcal{C})$, the controlled system $T/\mathcal{C}$ will never reach a blocking state (because of the deadend freedom condition) and its outputs will remain in the safe set $Y_S$ forever (because of the safety condition).

We now consider the problem of synthesizing a safety controller for a switched system $\Sigma$. Let us consider a time sampling parameter $\tau$ and a safety specification given by a compact set $Y_S \subseteq \mathbb{R}^n$. We shall use a method developed by Girard [2011] for synthesizing safety controllers for transition systems using approximately bisimilar abstractions. Let us define the $\varepsilon$-contraction of $Y_S$ as

$$\mathrm{Cont}_\varepsilon(Y_S) = \{y \in Y_S |\ \forall y' \in \mathbb{R}^n, \|y - y'\| \leq \varepsilon \Rightarrow y' \in Y_S\}.$$

*Theorem 2.* Consider a switched system $\Sigma$ and let us assume that there exists a common $\delta$-GUAS Lyapunov

function $\mathcal{V}$ for $\Sigma$ such that equation (1) holds. Let the time and state space sampling parameters $\tau, \eta > 0$ and the desired precision $\varepsilon > 0$ be such that (2) holds. Let $\mathcal{K}_\varepsilon : [\mathbb{R}^n]_\eta \to 2^P$ be a safety controller for $T_{\tau,\eta}(\Sigma)$ and specification $\mathrm{Cont}_\varepsilon(Y_S)$. Let $\mathcal{K} : [\mathbb{R}^n]_\eta \to 2^P$ be given by

$$\mathcal{K}(q) = \bigcup_{q' \in [\mathbb{R}^n]_\eta,\ \mathcal{V}(q,q') \leq \underline{\alpha}(\varepsilon - \eta)} \mathcal{K}_\varepsilon(q'). \tag{3}$$

Then, the map $\mathcal{C} : \mathbb{R}^n \to 2^P$ given by $\mathcal{C} = \mathcal{K} \circ Q_\eta$ is a safety controller for $T_\tau(\Sigma)$ and specification $Y_S$.

**Proof.** By Theorem 3.6 in (Girard [2011]), we have that $\mathcal{C} : \mathbb{R}^n \to 2^P$ given by

$$\mathcal{C}(x) = \bigcup_{q' \in [\mathbb{R}^n]_\eta,\ (x,q') \in \mathcal{R}_\varepsilon} \mathcal{K}_\varepsilon(q')$$

is a safety controller for $T_\tau(\Sigma)$ and specification $Y_S$. Then, using the form of $\mathcal{R}_\varepsilon$ given by Theorem 1, it is easy to show that $\mathcal{C} = \mathcal{K} \circ Q_\eta$. ■

Let us remark that Theorem 2 gives an effective way to compute a *quantized* safety controller for $T_\tau(\Sigma)$. It is to be noted that since $Y_S$ is compact, the set of states of the discrete abstraction $T_{\tau,\eta}(\Sigma)$ with associated outputs in $\mathrm{Cont}_\varepsilon(Y_S)$ is finite. As a consequence, the synthesis of the safety controller $\mathcal{K}_\varepsilon$ can be done by a simple fixed-point algorithm which is guaranteed to terminate in a finite number of steps (see e.g. the book by Tabuada [2009] for details).

*Lemma 3.* For all $q \in [\mathbb{R}^n]_\eta$, $\mathcal{K}(q) \neq \emptyset \Rightarrow q \in Y_S$.

**Proof.** If $\mathcal{K}(q) \neq \emptyset$ then there exists $q' \in [\mathbb{R}^n]_\eta$, such that $\mathcal{V}(q,q') \leq \underline{\alpha}(\varepsilon - \eta)$ and $\mathcal{K}_\varepsilon(q') \neq \emptyset$. Since $\mathcal{K}_\varepsilon$ is a safety controller for $T_{\tau,\eta}(\Sigma)$ and specification $\mathrm{Cont}_\varepsilon(Y_S)$, this implies that $q' \in \mathrm{Cont}_\varepsilon(Y_S)$. Moreover, $\mathcal{V}(q,q') \leq \underline{\alpha}(\varepsilon - \eta)$ gives $\|q - q'\| \leq \varepsilon - \eta \leq \varepsilon$. By definition of $\mathrm{Cont}_\varepsilon(Y_S)$, we obtain $q \in Y_S$. ■

Since $Y_S$ is a compact subset of $\mathbb{R}^n$, the set $Y_S \cap [\mathbb{R}^n]_\eta$ is a finite set. Hence, it is possible to entirely pre-compute offline the discrete map $\mathcal{K}$. Then, for a state $x \in \mathbb{R}^n$ the computation of the inputs enabled by $\mathcal{C}$ only requires quantizing the state $x$ and evaluating $\mathcal{K}(Q_\eta(x))$.

The online execution time of the controller defined in Theorem 2 is in $O(n)$ (cost of a quantization) and does not depend on the state space sampling parameter $\eta$. However, the memory space needed to store naively the control law (that is the map $\mathcal{K}$) is proportional to the number of states in $Y_S \cap [\mathbb{R}^n]_\eta$, that is $O(\eta^{-n})$ which can be quite large in practice.

In comparison, using the approximate bisimulation relation given in Girard et al. [2010] and Theorem 3.6 in (Girard [2011]), the synthesized controller would have been given by

$$\mathcal{C}(x) = \bigcup_{q' \in [\mathbb{R}^n]_\eta,\ \mathcal{V}(x,q') \leq \underline{\alpha}(\varepsilon)} \mathcal{K}_\varepsilon(q')$$

It is to be noted that the continuous state $x$ is not quantized and therefore the union cannot be computed offline for all possible values of $x$ as previously but has to be computed online. In practice, the number of elements $q' \in [\mathbb{R}^n]_\eta$ such that $\mathcal{V}(x,q') \leq \underline{\alpha}(\varepsilon)$ is in $O((\varepsilon/\eta)^{-n})$ which can be quite large. Also the memory space needed for the storage of the map $\mathcal{K}_\varepsilon$ is also in $O(\eta^{-n})$. Hence, we can see that our new approximation result allows us to synthesize controllers with smaller execution time and comparable memory usage.

### *3.2 Complexity reduction*

We now consider the problem of representing the discrete map $\mathcal{K}$ more efficiently in order to reduce the memory space needed for its storage. To reduce the memory needed to store the control law, we will not encode the (set-valued) map $\mathcal{K}$ but a *determinization* of $\mathcal{K}$.

*Definition 6.* A *determinization* of the set-valued map $\mathcal{K}$ is a univalued map $\mathcal{K}_d : [\mathbb{R}^n]_\eta \cap Y_S \to P$ such that

$$\forall q \in [\mathbb{R}^n]_\eta \cap Y_S,\ \mathcal{K}(q) \neq \emptyset \Rightarrow \mathcal{K}_d(q) \in \mathcal{K}(q).$$

If $\mathcal{K}(q) = \emptyset$, we do not impose any constraint on the value of $\mathcal{K}_d(q)$. This will allow us to reduce further the complexity of our control law.

*Theorem 4.* Let the controller $\mathcal{C}_d : \mathbb{R}^n \to 2^P$ for $T_\tau(\Sigma)$ be given for all $x \in \mathbb{R}^n$ by

$$\mathcal{C}_d(x) = \begin{cases} \{\mathcal{K}_d \circ Q_\eta(x)\} & \text{if } Q_\eta(x) \in Y_S \\ \emptyset & \text{otherwise.} \end{cases}$$

Then, for all state trajectories $\{(x^i, u^i) |\ i = 0, \ldots, N\}$ of the controlled system $T_\tau(\Sigma)/\mathcal{C}_d$ such that $x^0 \in \mathrm{dom}(\mathcal{C})$, we have $\mathcal{O}_1(x^i) \in Y_S$ for all $i = 0, \ldots, N$ and if $N$ is finite $x_N$ is a non-blocking state of $T_\tau(\Sigma)/\mathcal{C}_d$.

**Proof.** Let $x \in \mathrm{dom}(\mathcal{C})$, then $\mathcal{C}(x) = \mathcal{K}(Q_\eta(x)) \neq \emptyset$. By Lemma 3, $\mathcal{K}(Q_\eta(x)) \neq \emptyset$ gives $Q_\eta(x) \in [\mathbb{R}^n]_\eta \cap Y_S$. Therefore, $\mathcal{C}_d(x) = \{\mathcal{K}_d(Q_\eta(x))\} \neq \emptyset$. Hence, $x \in \mathrm{dom}(\mathcal{C}_d)$ and therefore $x$ is a non-blocking state of $T_\tau(\Sigma)/\mathcal{C}_d$. Moreover, let $p \in \mathcal{C}_d(x)$, then $p = \mathcal{K}_d(Q_\eta(x)) \in \mathcal{K}(Q_\eta(x)) = \mathcal{C}(x)$. Since $\mathcal{C}$ is a safety controller, it follows that $x' = \mathcal{S}_1(x,p) \in \mathrm{dom}(\mathcal{C})$. From the previous discussion, it follows by induction that for all $i = 0, \ldots, N$, $x^i \in \mathrm{dom}(\mathcal{C})$. Moreover, if $N$ is finite $x_N$ is a non-blocking state of $T_\tau(\Sigma)/\mathcal{C}_d$. Finally, $\mathcal{C}$ is a safety controller, $x^i \in \mathrm{dom}(\mathcal{C})$ gives $\mathcal{O}_1(x^i) \in Y_S$ for all $i = 0, \ldots, N$. ■

Let us remark that the controller $\mathcal{C}_d$ is generally not a safety controller for $T_\tau(\Sigma)$ and specification $Y_S$ in the sense of Definition 5. However, the previous result shows that for an initial state $x^0 \in \mathrm{dom}(\mathcal{C})$, the controlled system $T_\tau(\Sigma)/\mathcal{C}_d$ will never reach a blocking state and its outputs will remain forever in the safe set $Y_S$.

We now consider the problem of choosing a determinization $\mathcal{K}_d$ of $\mathcal{K}$ and a representation which requires little memory for its storage. A natural representation for $\mathcal{K}_d$ would be to use an array which would require $O(\eta^{-n})$ memory space. We propose a more efficient representation inspired by algebraic decision diagrams (ADD's). The main idea is to use a tree structure which exploits redundant information to represent the map in a more compact way. Also in our case, when $\mathcal{K}(q)$ is empty or when it has more than 2 elements, we have some flexibility for the choice of $\mathcal{K}_d(q)$ which can be used to reduce the size of the representation.

The proposed method for choosing $\mathcal{K}_d$ essentially works as follows: if there exists $p \in P$ such that for all $q \in [\mathbb{R}^n]_\eta \cap Y_S$,

$\mathcal{K}(q) = \emptyset$ or $p \in \mathcal{K}(q)$, we can choose $\mathcal{K}_d$ to be the map with constant value $p$ on $[\mathbb{R}^n]_\eta \cap Y_S$. The memory space needed to store $\mathcal{K}_d$ is then $O(1)$. If such an input value does not exists, then we can split (typically using a hyperplane) the set $[\mathbb{R}^n]_\eta \cap Y_S$ into 2 subsets of similar sizes. This process can then be repeated iteratively: we try to find a suitable constant value on each of the subsets and if this is not possible these sets can be split further.

In Figure 1, we show an example of representation using a tree structure of a determinization of a set-valued map $\mathcal{K} : \{1,2,3,4\}^2 \to 2^P$ where $P = \{0,1\}$. We cannot find a suitable constant value on the whole set $\{1,2,3,4\}^2$. Thus, it is split into two subsets $\{1,2\} \times \{1,2,3,4\}$ and $\{3,4\} \times \{1,2,3,4\}$. For $q \in \{1,2\} \times \{1,2,3,4\}$ we can choose $\mathcal{K}_d(q) = 0$. On $\{3,4\} \times \{1,2,3,4\}$, there is no suitable value. This set is split further into the subsets $\{3,4\} \times \{1,2\}$ and $\{3,4\}^2$. For $q \in \{3,4\}^2$, we can choose $\mathcal{K}_d(q) = 1$. On $\{3,4\} \times \{1,2\}$, there is no suitable value and this set has to be split futher... By repeating this process, we obtain the determinization $\mathcal{K}_d$ represented by the tree structure in Figure 1.

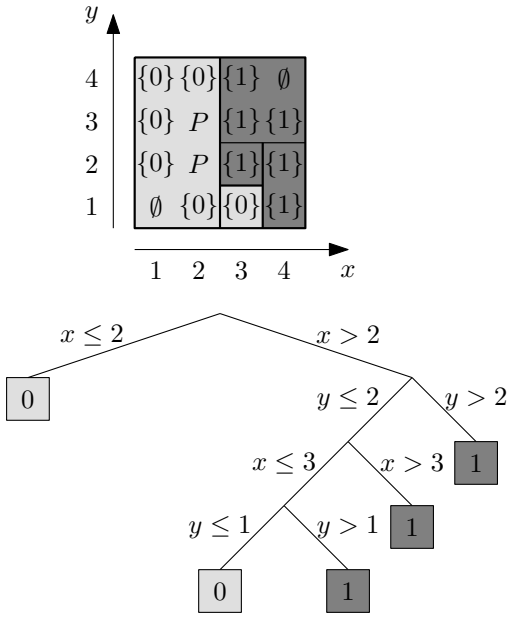


Fig. 1. A set valued map $\mathcal{K} : \{1,2,3,4\}^2 \to 2^P$ where $P = \{0,1\}$ and a determinization given by colors (dark gray for 1, light gray for 0) and its representation using a tree structure.

Using this representation for the determinization $\mathcal{K}_d$, the online execution time of the controller $\mathcal{C}_d$ is given by the longest path in the tree which is in $O(-n\log(\eta))$. This is a little bit more than the controller $\mathcal{C}$. The memory space needed to store the control law is given by the number of nodes in the tree which is $O(\eta^{-n})$, in the worst case. However, in practice, we can expect much less as an example will show in the next section.

Finally, we would like to mention that the use of ADD's for representing control laws synthesized through symbolic models has already been considered in Mazo et al. [2010]. However, as far as we know, the idea of determinizing safety controllers in such a way that their determinization reduces the memory needed for its storage is new.

## 4. EXAMPLE

For illustration purpose, we consider a simple thermal model of a two-room building (see e.g Deng et al. [2010]):

$$\begin{cases} \dot{T}_1 = \alpha_{21}(T_2 - T_1) + \alpha_{e1}(T_e - T_1) + \alpha_f(T_f - T_1)p \\ \dot{T}_2 = \alpha_{12}(T_1 - T_2) + \alpha_{e2}(T_e - T_2) \end{cases}$$

where $T_1$ and $T_2$ denote the temperature in each room, $T_e = 10$ is the external temperature and $T_f$ stands for the temperature of a heating device which can switched on ($p = 1$) or off ($p = 0$). The system parameters are chosen as follows $\alpha_{21} = \alpha_{12} = 5 \times 10^{-2}$, $\alpha_{e1} = 5 \times 10^{-3}$, $\alpha_{e2} = 3.3 \times 10^{-3}$ and $\alpha_f = 8.3 \times 10^{-3}$. Let $T = (T_1, T_2)^\top$, then the system can be written as a switched affine system of the form

$$\Sigma : \ \dot{\mathbf{T}}(t) = A_{\mathbf{p}(t)}\mathbf{T}(t) + b_{\mathbf{p}(t)}, \ \mathbf{p}(t) \in P = \{0,1\}.$$

It is easily to verify that the function $\mathcal{V} : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^+$ given by $\mathcal{V}(T,T') = \|T - T'\|$ is a $\delta$-GUAS Laypunov function for $\Sigma$ with $\underline{\alpha}(r) = \overline{\alpha}(r) = r$ and $\kappa = 0.0042$. Moreover, equation (1) holds with $\gamma(r) = r$.

We consider the problem of keeping the temperature in the rooms between 20 and 22 degrees Celsius. This is a safety property specified by the safe set $Y_S = [20,22]^2$. We want to use a periodic controller with a period of $\tau = 5$ time units. For the synthesis of the controller, we shall use an approximately bisimilar symbolic abstraction of $T_\tau(\Sigma)$ of precision $\varepsilon = 0.25$. According to equation (2), we can choose a state-space sampling parameter $\eta = 0.0014$ for the computation of the symbolic abstraction $T_{\tau,\eta}(\Sigma)$.

We computed a safety controller $\mathcal{K}_\varepsilon$ for the symbolic abstraction $T_{\tau,\eta}(\Sigma)$ and the specification $\mathrm{Cont}_\varepsilon(Y_S) = [20.25, 21.75]^2$. Then, we computed the map $\mathcal{K}$ given by equation (3), which is shown in Figure 2. Then, according to Theorem 2, the controller $\mathcal{C} = \mathcal{K} \circ Q_\eta$ is a safety controller for $T_\tau(\Sigma)$ and specification $Y_S$. For a practical implementation of the controller, the storage of the map

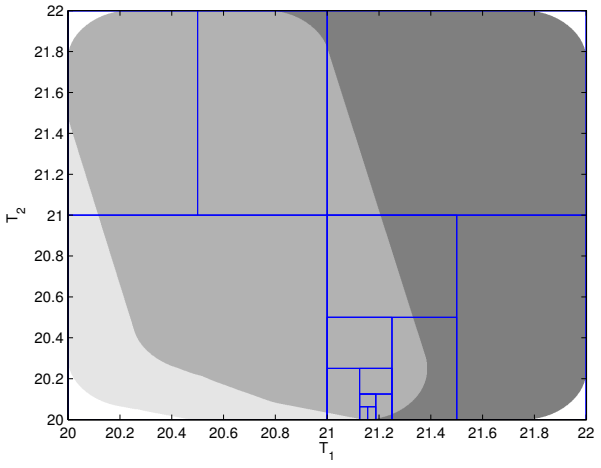


Fig. 2. Set-valued map $\mathcal{K} : [\mathbb{R}^2]_\eta \cap Y_S \to 2^P$ (white: $\emptyset$, light gray: $\{1\}$, medium gray: $P$, dark gray: $\{0\}$). The number of elements in $[\mathbb{R}^2]_\eta \cap Y_S$ is about 1 million. In blue, we represented the partition used for the representation of $\mathcal{K}_d$, a determinization of $\mathcal{K}$; the resulting tree structure has only 27 nodes.

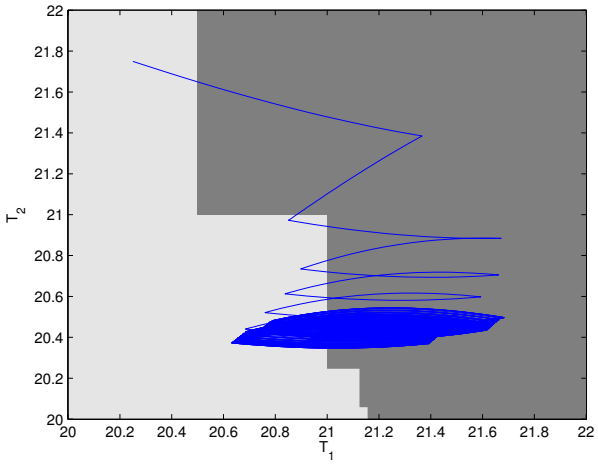


Fig. 3. Determinization $\mathcal{K}_d$ of the map $\mathcal{K}$ shown in Figure 2 (light gray: 1, dark gray: 0). In blue, a trajectory of the switched system controlled using the controller $\mathcal{C}_d = \mathcal{K}_d \circ Q_\eta$.

$\mathcal{K}$ represented by an array would require about 1 million memory units (this is the number of elements in $[\mathbb{R}^2]_\eta \cap Y_S$).

We computed a determinization $\mathcal{K}_d$ of $\mathcal{K}$ following the approach described in the previous section. In Figure 2, we show the partition used for the representation of $\mathcal{K}_d$, it is to be noted that in each region all values of $\mathcal{K}$ are either $\emptyset$, $\{0\}$, $P$ (which corresponds to value 0 for $\mathcal{K}_d$) or $\emptyset$, $\{1\}$, $P$ (which corresponds to value 1 for $\mathcal{K}_d$). The map $\mathcal{K}_d$ is represented in Figure 3 where we have also represented a trajectory of the switched system controlled using the controller $\mathcal{C}_d = \mathcal{K}_d \circ Q_\eta$. For a practical implementation of the controller, the storage of the map $\mathcal{K}_d$ represented by a tree structure only requires 27 memory units (this is the number of nodes in the tree).

We can see with this example that a lot of memory can be saved using an efficient representation and by determinizing the controllers in such a way that their determinization can be represented in a more compactly. Guarantees of safety for these controllers are still available by Theorem 4 which gives insurance of "correctness by design".

## 5. CONCLUSION

In this paper, we have addressed the problem of synthesizing low-complexity safety controllers for switched systems. By following a rigorous approach based on the use of symbolic models we obtain controllers that are correct by design. Determinization of the safety controllers together with an adequate data structure can reduce drastically the memory needed to store the control law and can lead to quantized controllers that can be efficiently implemented in practice.

In future work, we should address the problem of synthesizing low-complexity controllers for other types of specifications as well as consider other types of symbolic models such as multi-scale symbolic models introduced in Camara et al. [2011].

## REFERENCES


D. Angeli. A Lyapunov approach to incremental stability properties. *IEEE Trans. on Automatic Control*, 47(3): 410–421, March 2002.

R.I. Bahar, E.A. Frohm, C.M. Gaona, G.D. Hachtel, E. Macii, A. Pardo, and F. Somenzi. Algebraic decision diagrams and their applications. In *International Conference on Computer-Aided Design*, pages 188–191, 1993.

J. Camara, A. Girard, and G. Goessler. Safety controller synthesis for switched systems using multi-scale symbolic models. In *Joint IEEE Conference on Decision and Control and European Control Conference*, 2011.

K. Deng, P. Barooah, P.G. Mehta, and S.P. Meyn. Building thermal model reduction via aggregation of states. In *American Control Conference*, 2010.

A. Girard. Controller synthesis for safety and reachability via approximate bisimulation. *Automatica*, 2011. To appear, `arXiv:1010.4672v2`.

A. Girard and G. J. Pappas. Approximation metrics for discrete and continuous systems. *IEEE Trans. on Automatic Control*, 52(5):782–798, 2007.

A. Girard, G. Pola, and P. Tabuada. Approximately bisimilar symbolic models for incrementally stable switched systems. *IEEE Trans. on Automatic Control*, 55(1):116–126, 2010.

M. Kloetzer and C. Belta. A fully automated framework for control of linear systems from ltl specifications. In *Hybrid Systems: Computation and Control*, volume 3927 of *LNCS*, pages 333–347. Springer, 2006.

M. Mazo, A. Davitian, and P. Tabuada. Pessoa: A tool for embedded controller synthesis. In *Computer Aided Verification*, volume 6174/2010 of *LNCS*, pages 566–569, 2010.

M. Mazo Jr. and P. Tabuada. Approximate time-optimal control via approximate alternating simulations. In *American Control Conference*, pages 10201–10206, 2010.

T. Moor and J. Raisch. Supervisory control of hybrid systems within a behavioral framework. *Systems and Control Letters*, 38(3):157–166, 1999.

G. Pola and P. Tabuada. Symbolic models for nonlinear control systems: Alternating approximate bisimulations. *SIAM J. on Control and Optimization*, 48(2):719–733, 2009.

J. Raisch and S. O'Young. Discrete approximation and supervisory control of continuous systems. *IEEE Trans. on Automatic Control*, 43(4):569–573, 1998.

G. Reißig. Computation of discrete abstractions of arbitrary memory span for nonlinear sampled systems. In *Hybrid Systems: Computation and Control*, volume 5469 of *LNCS*, pages 306–320. Springer, 2009.

P. Tabuada. *Verification and Control of Hybrid Systems - A Symbolic Approach*. Springer, 2009.

P. Tabuada and G. J. Pappas. Linear time logic control of discrete-time linear systems. *IEEE Trans. on Automatic Control*, 51(12):1862–1877, 2006.

Y. Tazaki and J. I. Imura. Finite abstractions of discrete-time linear systems and its application to optimal control. In *17th IFAC World Congress*, pages 10201–10206, 2008.