Low-complexity quantized switching controllers using approximate bisimulation

Antoine Girard

Low-Complexity Quantized Switching Controllers using Approximate Bisimulation[☆]

Antoine Girard[a]

[a] *Laboratoire Jean Kuntzmann, Université Joseph Fourier, 51 rue des Mathématiques, B.P. 53, 38041 Grenoble Cedex 9, France*

Abstract

In this paper, we consider the problem of synthesizing low-complexity 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 naturally quantized switching controllers for safety or reachability specifications; these can be pre-computed offline and therefore the online execution time is 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 of the synthesized 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, Controller synthesis

1. Introduction

The use of discrete abstractions or symbolic models has become quite popular for hybrid systems design (see e.g. [1, 2, 3, 4, 5]). In particular, several recent works have focused on the use of symbolic models related to the original system by approximate equivalence relationships (approximate bisimulations [6, 7]; or approximate alternating simulation or bisimulation relations [8, 9]) 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 [10, 11].

[☆]This work was supported by the Agence Nationale de la Recherche (VEDECY project - ANR 2009 SEGI 015 01) and by the pole MSTIC of Université Joseph Fourier (SYMBAD project).

Email address: Antoine.Girard@imag.fr (Antoine Girard)

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 is the first main contribution of the paper, it differs from the original result presented by [7] mainly by the fact that the expression of the approximate bisimulation relation uses a quantized value of the state of the switched system rather than its full value in [7]. This difference is fundamental for the synthesis of controllers with lower complexity. Indeed, the combination of this new result with synthesis techniques for safety or reachability specifications presented in [11] yields quantized switching controllers that can be entirely pre-computed offline. The online execution time is then greatly reduced in comparison to controllers obtained using the previous existing approximation result. The second main contribution of the paper is to 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. [12]) for compact function representation. Also, the non-determinism of the synthesized controllers can be exploited to further simplify the representation of the control law. Finally, we apply our approach to the synthesis of controllers for a simple model of temperature regulation in a building. The results on the synthesis of safety controllers appeared in preliminary form in the conference paper [13], those on reachability controllers are new.

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 [7]. 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. The switching signals $\mathbf{p} : \mathbb{R}^+ \to P$ are assumed to be piecewise constant functions, continuous from the right and with a finite number of discontinuities on every bounded interval. We use $\mathbf{x}(t, x, \mathbf{p})$ to denote the point reached at time $t \in \mathbb{R}_0^+$ from the initial condition x under the switching signal $\mathbf{p}$. We will assume that the switched system Σ is incrementally globally uniformly asymptotically stable [7]:

Definition 1. *The switched system Σ is said to be incrementally globally uniformly asymptotically stable (δ-GUAS) if there exists a KL function[1] β such that for all $t \in \mathbb{R}_0^+$, for all $x, y \in \mathbb{R}^n$, for all switching signals $\mathbf{p} \in \mathcal{P}$, the following condition is satisfied:*

$$\|\mathbf{x}(t, x, \mathbf{p}) - \mathbf{x}(t, y, \mathbf{p})\| \leq \beta(\|x - y\|, t). \tag{1}$$

Intuitively, a switched system is δ-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 [7]:

Definition 2. *A smooth function $\mathcal{V} : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_0^+$ is a common δ-GUAS Lyapunov function for Σ if there exist K_∞ functions $\underline{\alpha}$, $\overline{\alpha}$ 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 has been shown in [7] that the existence of a common δ-GUAS Lyapunov function ensures that the switched system Σ is δ-GUAS.

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

Definition 3. *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 $\text{Enab}(x)$, if $\mathcal{S}(x, u) \neq \emptyset$. If $\text{Enab}(x) \neq \emptyset$, 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 $u \in \text{Enab}(x)$, $\mathcal{S}(x, u)$ has 1 element then the transition system is said to be *deterministic*.

[1] A continuous function $\gamma : \mathbb{R}_0^+ \to \mathbb{R}_0^+$ is said to belong to class K_∞ if it is strictly increasing, $\gamma(0) = 0$ and $\gamma(r) \to \infty$ when $r \to \infty$. A continuous function $\beta : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}_0^+$ is said to belong to class KL if for all fixed s, the map $r \mapsto \beta(r, s)$ belongs to class K_∞ and for all fixed r, the map $s \mapsto \beta(r, s)$ is strictly decreasing and $\beta(r, s) \to 0$ when $s \to \infty$.

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 Σ and a parameter $\tau > 0$, we define a transition system $T_\tau(\Sigma)$ that describes trajectories of Σ of duration τ. This can be seen as a time sampling process, which is natural when the switching in Σ is to be determined by a periodic controller of period τ. 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 labeled transition systems defined by approximate bisimulation relations introduced in [14].

Definition 4. *Let $T_i = (X_i, U, \mathcal{S}_i, Y, \mathcal{O}_i)$, $i = 1, 2$, be metric labeled 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 ε-approximate bisimulation relation between T_1 and T_2, if for all $(x_1, x_2) \in \mathcal{R}_\varepsilon$:*

1. $d\left(\mathcal{O}_1(x_1), \mathcal{O}_2(x_2)\right) \leq \varepsilon$,
2. $\forall u \in Enab_1(x_1)$, $\forall x_1' \in \mathcal{S}_1(x_1, u)$, $\exists x_2' \in \mathcal{S}_2(x_2, u)$ *such that* $(x_1', x_2') \in \mathcal{R}_\varepsilon$.
3. $\forall u \in Enab_2(x_2)$, $\forall x_2' \in \mathcal{S}_2(x_2, u)$, $\exists x_1' \in \mathcal{S}_1(x_1, u)$ *such that* $(x_1', x_2') \in \mathcal{R}_\varepsilon$.

T_1 and T_2 are approximately bisimilar with precision ε (denoted $T_1 \sim_\varepsilon T_2$), if there exists $\mathcal{R}_\varepsilon$, an ε-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.

We briefly describe an approach similar to that presented in [7] for computing approximately bisimilar discrete abstractions of $T_\tau(\Sigma)$ (i.e. a discrete labeled transition system that is approximately bisimilar to $T_\tau(\Sigma)$). 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

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

It is easy to check that for all $x \in \mathbb{R}^n$, $\|Q_\eta(x) - x\| \leq \eta$. Given a subset $X \subseteq \mathbb{R}^n$ we denote $Q_\eta(X) = \{Q_\eta(x) | x \in X\}$.

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 Σ. In the following, we shall assume that there exists a common δ-GUAS Lyapunov function $\mathcal{V}$ for Σ. We need to make the supplementary assumption on the δ-GUAS Lyapunov function that there exists a K_∞ function γ such that for all $x_1, x_2, y_1, y_2 \in \mathbb{R}^n$

$$|\mathcal{V}(x_1, x_2) - \mathcal{V}(y_1, y_2)| \leq \gamma(\|x_1 - y_1\| + \|x_2 - y_2\|). \tag{2}$$

We can show that this assumption is not restrictive provided $\mathcal{V}$ is smooth and we are interested in the dynamics of Σ 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 Σ, time and state space sampling parameters $\tau, \eta > 0$ and a desired precision $\varepsilon > 0$. If there exists a common δ-GUAS Lyapunov function $\mathcal{V}$ for Σ such that equation (2) holds and*

$$\varepsilon \geq \eta + \underline{\alpha}^{-1}\left(\frac{\gamma(2\eta) + \gamma(\eta)e^{-\kappa\tau}}{1 - e^{-\kappa\tau}}\right) \tag{3}$$

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 ε-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 4 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 of Definition 4 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 δ-GUAS Lyapunov function $\mathcal{V}$ we obtain

$$\begin{aligned}
\mathcal{V}(Q_\eta(x'_1), x'_2) &= \mathcal{V}(Q_\eta(\mathcal{S}_1(x_1, p)), Q_\eta(\mathcal{S}_1(x_2, p))) \\
&\leq \mathcal{V}(\mathcal{S}_1(x_1, p), \mathcal{S}_1(x_2, p)) + \gamma(2\eta) \\
&\leq e^{-\kappa\tau}\mathcal{V}(x_1, x_2) + \gamma(2\eta) \\
&\leq e^{-\kappa\tau}\left(\mathcal{V}(Q_\eta(x_1), x_2) + \gamma(\eta)\right) + \gamma(2\eta) \\
&\leq e^{-\kappa\tau}\underline{\alpha}(\varepsilon - \eta) + \gamma(2\eta) + \gamma(\eta)e^{-\kappa\tau} \\
&\leq \underline{\alpha}(\varepsilon - \eta)
\end{aligned}$$

by equation (3). It follows that $(x'_1, x'_2) \in \mathcal{R}_\varepsilon$ which is consequently an ε-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 (3) 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 in [7]. 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 and only if $\mathcal{V}(x_1, x_2) \leq \underline{\alpha}(\varepsilon)$ in [7], instead of $\mathcal{V}(Q_\eta(x_1), x_2) \leq \underline{\alpha}(\varepsilon - \eta)$ in Theorem 1. We will see in the next section that this difference is fundamental as it will allow us to synthesize quantized controllers. It should also be noted that the relations to be satisfied by the abstraction parameters, τ, η and ε are different: for identical precision and time sampling parameters Theorem 1 generally requires a finer state sampling parameter than the results presented in [7].

Remark 1. When the switched system does not admit a common δ-GUAS function, an approximation result was established in [7], based on the use of multiple Lyapunov functions and under a minimum dwell-time assumption. A result similar to Theorem 1 can also be established in that case.

In the remainder of the paper, we consider a switched system Σ with time and state space sampling parameters τ and η. We shall work with the labeled transition systems $T_\tau(\Sigma)$ and $T_{\tau,\eta}(\Sigma)$ and we shall assume that the assumptions of Theorem 1 hold. We will denote for $x \in \mathbb{R}^n$, $\mathcal{R}_\varepsilon(x) = \{q \in [\mathbb{R}^n]_\eta |\ (x, q) \in \mathcal{R}_\varepsilon\}$. We will also use the relation

$$\overline{\mathcal{R}}_\varepsilon = \{(q, q') \in [\mathbb{R}^n]_\eta \times [\mathbb{R}^n]_\eta |\ \mathcal{V}(q, q') \leq \underline{\alpha}(\varepsilon - \eta)\}$$

and we denote for $q \in [\mathbb{R}^n]_\eta$, $\overline{\mathcal{R}}_\varepsilon(q) = \{q' \in [\mathbb{R}^n]_\eta |\ (q, q') \in \overline{\mathcal{R}}_\varepsilon\}$. Let us remark that for all $x \in \mathbb{R}^n$, $\mathcal{R}_\varepsilon(x) = \overline{\mathcal{R}}_\varepsilon(Q_\eta(x))$.

3. Synthesis of Quantized Switching Controllers

In this section, we present an approach for synthesizing quantized switching controllers for safety or reachability specifications. It is based on the use of Theorem 1 combined with controller synthesis techniques presented in [11]. We start by defining the notion of controller for labeled transition systems:

Definition 5. *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 $\mathcal{C}(x) \subseteq Enab(x)$, for all $x \in X$. The domain of $\mathcal{C}$ is the set $dom(\mathcal{C}) = \{x \in X |\ \mathcal{C}(x) \neq \emptyset\}$. 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 $X \setminus \mathrm{dom}(\mathcal{C})$. Given a subset $X' \subseteq X$, we denote $\mathcal{C}(X') = \bigcup_{x \in X'} \mathcal{C}(x)$.

3.1. Safety controllers

Let $Y_S \subseteq Y$ be a set of outputs associated with safe states. We consider the safety synthesis problem that consists in determining a controller that keeps the output of the system inside the specified safe set Y_S.

Definition 6. *Let $Y_S \subseteq Y$ be a set of safe outputs. A controller $\mathcal{C}$ is a safety controller for $T = (X, U, \mathcal{S}, Y, \mathcal{O})$ and specification Y_S if for all $x \in dom(\mathcal{C})$:*

1. *$\mathcal{O}(x) \in Y_S$ (safety);*
2. *$\forall u \in \mathcal{C}(x)$, $\mathcal{S}(x, u) \subseteq dom(\mathcal{C})$ (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 $T_\tau(\Sigma)$ describing the sampled dynamics of the switched system Σ. Let us consider a safety specification given by a compact set $Y_S \subseteq \mathbb{R}^n$. We shall use a method developed in [11] for synthesizing safety controllers for labeled transition systems using approximately bisimilar abstractions. Let us define the ε-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. *Let $\mathcal{K}_\varepsilon : [\mathbb{R}^n]_\eta \to 2^P$ be a safety controller for the symbolic model $T_{\tau,\eta}(\Sigma)$ and specification $Cont_\varepsilon(Y_S)$. Let $\mathcal{K} : [\mathbb{R}^n]_\eta \to 2^P$ be given for $q \in [\mathbb{R}^n]_\eta$ by*

$$\mathcal{K}(q) = \mathcal{K}_\varepsilon\left(\overline{\mathcal{R}}_\varepsilon(q)\right). \tag{4}$$

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 1 in [11], we have that $\mathcal{C} : \mathbb{R}^n \to 2^P$ given by $\mathcal{C}(x) = \mathcal{K}_\varepsilon(\mathcal{R}_\varepsilon(x))$ is a safety controller for $T_\tau(\Sigma)$ and specification Y_S. Then, using the fact that $\mathcal{R}_\varepsilon(x) = \overline{\mathcal{R}}_\varepsilon(Q_\eta(x))$ we obtain $\mathcal{C} = \mathcal{K} \circ Q_\eta$. ■

It is to be noted that since Y_S is compact, the set of states of the symbolic model $T_{\tau,\eta}(\Sigma)$ 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. [10] for details).

Let us remark that the only non-trivial values of $\mathcal{C}(x)$ are for $x \in Y_S$ since from a state $x \notin Y_S$, the safety specification cannot be met and therefore $\mathcal{C}(x) = \emptyset$. Hence, it is only necessary to compute $\mathcal{K}$ on $Q_\eta(Y_S)$ which is finite since Y_S is a compact subset of $\mathbb{R}^n$. 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 $\mathcal{K}(Q_\eta(x))$. Thus, Theorem 2 gives an effective way to compute a quantized safety controller for $T_\tau(\Sigma)$. Moreover, as shown in [11], it is possible to give guarantees on the distance between the synthesized controller $\mathcal{C}$ and the most permissive controller for the safety specification Y_S.

Let us now discuss the complexity of the synthesized controller[2]. 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 η. 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 $Q_\eta(Y_S)$, that is $O(\eta^{-n})$ which can be quite large in practice. In comparison, using the approximate bisimulation relation given in [7] and Theorem 1 in ([11]), 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

[2] In the following, the notations $O(.)$ must be understood as asymptotic upper-bound estimates when η approaches 0.

see that our new approximation result allows us to synthesize controllers with smaller execution time and comparable memory usage.

3.2. Reachability controllers

Let $Y_S \subseteq Y$ be a set of outputs associated with safe states, let $Y_T \subseteq Y_S$ be a set of outputs associated with target states. We consider the reachability synthesis problem that consists in determining a controller steering the output of the system to Y_T while keeping the output in Y_S along the way. For simplicity, we assume that the labeled transition systems we consider are non-blocking. Let us remark that this is the case for transitions systems $T_\tau(\Sigma)$ and $T_{\tau,\eta}(\Sigma)$ considered in this paper.

Definition 7. *Let $\mathcal{C}$ be a controller for $T = (X, U, \mathcal{S}, Y, \mathcal{O})$ such that for all $x \in X$, $\mathcal{C}(x) \neq \emptyset$. The entry time of $T/\mathcal{C}$ from $x^0 \in X$ for reachability specification (Y_S, Y_T) is the smallest $N \in \mathbb{N}$ such that for all state trajectories of $T/\mathcal{C}$, of length N and starting from x^0, $(x^0, u^0), (x^1, u^1), \ldots, (x^{N-1}, u^{N-1}), (x^N, u^N)$, there exists $K \in \{0, \ldots, N\}$ such that*

1. $\forall k \in \{0, \ldots, K\}$, $\mathcal{O}(x^k) \in Y_S$;
2. $\mathcal{O}(x^K) \in Y_T$.

The entry time is denoted by $J(T/\mathcal{C}, Y_s, Y_t, x^0)$. If such a $N \in \mathbb{N}$ does not exist, then we define $J(T/\mathcal{C}, Y_S, Y_T, x^0) = +\infty$.

It is clear from the previous definition that for any initial state x^0 with finite entry time, the outputs of the controlled system $T/\mathcal{C}$ will remain in the safe set Y_S until one output eventually reaches the target set Y_T in a number of transitions bounded by $J(T/\mathcal{C}, Y_S, Y_T, x^0)$. Hence, for those states, the reachability specification is met. It should be noted that for all $x^0 \in X$, $J(T/\mathcal{C}, Y_S, Y_T, x^0) = 0$ if and only if $\mathcal{O}(x^0) \in Y_T$ and that for all $x^0 \in X$ such that $\mathcal{O}(x^0) \notin Y_S$, $J(T/\mathcal{C}, Y_S, Y_T, x^0) = +\infty$. Also for all $x \in X$, such that $0 < J(T/\mathcal{C}, Y_S, Y_T, x) < +\infty$, it is easy to show that

$$J(T/\mathcal{C}, Y_S, Y_T, x) = 1 + \max_{u \in \mathcal{C}(x), x' \in \mathcal{S}(x,u)} J(T/\mathcal{C}, Y_S, Y_T, x'). \tag{5}$$

We now consider the problem of synthesizing a reachability controller for $T_\tau(\Sigma)$ describing the sampled dynamics of the switched system Σ. Let us consider a reachability specification given by compact sets $Y_S \subseteq \mathbb{R}^n$ and $Y_T \subseteq Y_S$.

Theorem 3. *Let $\mathcal{K}_\varepsilon : [\mathbb{R}^n]_\eta \to 2^P$ be a controller for the symbolic model $T_{\tau,\eta}(\Sigma)$, let the map $\mathcal{K} : [\mathbb{R}^n]_\eta \to 2^P$ be given for $q \in [\mathbb{R}^n]_\eta$ by* [3]

$$\mathcal{K}(q) = \mathcal{K}_\varepsilon \left(\arg \min_{q' \in \overline{\mathcal{R}}_\varepsilon(q)} J(T_{\tau,\eta}(\Sigma)/\mathcal{K}_\varepsilon, \mathit{Cont}_\varepsilon(Y_S), \mathit{Cont}_\varepsilon(Y_T), q') \right). \tag{6}$$

[3] The function arg min is to be understood as a set-valued map: it returns the set of minimizers.

Then, the map $\mathcal{C} : \mathbb{R}^n \to 2^P$ *given by* $\mathcal{C} = \mathcal{K} \circ Q_\eta$ *satisfies for all* $x \in \mathbb{R}^n$*:*

$$J(T_\tau(\Sigma)/\mathcal{C}, Y_S, Y_T, x) \leq \tilde{J}(Q_\eta(x)) \tag{7}$$

where $\tilde{J} : [\mathbb{R}^n]_\eta \to \mathbb{N}$ *is the map given for* $q \in [\mathbb{R}^n]_\eta$ *by*

$$\tilde{J}(q) = \min_{q' \in \overline{\mathcal{R}}_\varepsilon(q)} J(T_{\tau,\eta}(\Sigma)/\mathcal{K}_\varepsilon, Cont_\varepsilon(Y_S), Cont_\varepsilon(Y_T), q').$$

Proof. By Theorem 3 in [11], we have that $\mathcal{C} : \mathbb{R}^n \to 2^P$ given by

$$\mathcal{C}(x) = \mathcal{K}_\varepsilon \left(\arg \min_{q' \in \mathcal{R}_\varepsilon(x)} J(T_{\tau,\eta}(\Sigma)/\mathcal{K}_\varepsilon, \mathrm{Cont}_\varepsilon(Y_S), \mathrm{Cont}_\varepsilon(Y_T), q') \right). \tag{8}$$

satisfies

$$J(T_\tau(\Sigma)/\mathcal{C}, Y_S, Y_T, x) \leq \min_{q' \in \mathcal{R}_\varepsilon(x)} J(T_{\tau,\eta}(\Sigma)/\mathcal{K}_\varepsilon, \mathrm{Cont}_\varepsilon(Y_S), \mathrm{Cont}_\varepsilon(Y_T), q'). \tag{9}$$

Then, using the fact that $\mathcal{R}_\varepsilon(x) = \overline{\mathcal{R}}_\varepsilon(Q_\eta(x))$, equation (8) gives $\mathcal{C} = \mathcal{K} \circ Q_\eta$ and equation (9) gives (7). ■

Similarly to safety controllers, the synthesis of a reachability controller $\mathcal{K}_\varepsilon$ for the symbolic model $T_{\tau,\eta}(\Sigma)$ can be done by a simple fixed-point algorithm (e.g. using dynamic programming) which is guaranteed to terminate in a finite number of steps since Y_S is compact. It should be noted that we are only interested in the values of $\mathcal{C}(x)$ for $x \in Y_S$ since from $x \notin Y_S$ the reachability specification cannot be met. Hence, it is only necessary to compute $\mathcal{K}$ on $Q_\eta(Y_S)$ which is finite since Y_S is a compact subset of $\mathbb{R}^n$. Therefore, the map $\mathcal{K}$ can be pre-computed offline. Thus, Theorem 3 gives an effective way to compute a quantized reachability controller for $T_\tau(\Sigma)$. Moreover, it is possible to give guarantees on the distance between the performances of the synthesized controller $\mathcal{C}$ and the time optimal controller for the reachability specification (Y_S, Y_T) [11]. The complexity of the synthesized controller in terms of execution time and memory consumption is similar to that of the safety controllers discussed in the previous section.

Remark 2. We would like to highlight some relations between the control problems under consideration in this paper and some problems in viability theory [15]. For the safety controller $\mathcal{K}$ defined in Theorem 2, it can be shown that $\mathrm{dom}(\mathcal{K})$ is an under-approximation of the viability kernel of $\mathcal{O}_1^{-1}(Y_S)$ under the dynamics of Σ. As for the reachability controller $\mathcal{K}$ defined in Theorem 3, it can be shown that the set $\{x \in \mathbb{R}^n | \tilde{J}(Q_\eta(x)) < +\infty\}$ is an under-approximation of the viable capture basin of $\mathcal{O}_1^{-1}(Y_T)$ in $\mathcal{O}_1^{-1}(Y_S)$ under the dynamics of Σ.

4. Complexity Reduction

We now consider the problem of representing the discrete maps $\mathcal{K}$ defined in Theorems 2 and 3 more efficiently in order to reduce the memory space needed for their storage. To reduce the memory needed to store the control law, we will not encode the (set-valued) maps $\mathcal{K}$ but *determinizations* of $\mathcal{K}$.

4.1. Determinization of safety controllers

We first explain our approach for safety controllers. Let $\mathcal{K}$ be the map defined in Theorem 2 and let $\mathcal{C} = \mathcal{K} \circ Q_\eta$.

Definition 8. *A determinization of the set-valued map $\mathcal{K}$ is a univalued map $\mathcal{K}_d : Q_\eta(Y_S) \to P$ such that*

$$\forall q \in Q_\eta(Y_S),\ \mathcal{K}(q) \neq \emptyset \Rightarrow \mathcal{K}_d(q) \in \mathcal{K}(q).$$

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*

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

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 $x^0 \in dom(\mathcal{C})$, 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. Since $\mathcal{C}$ is a safety controller we have $\mathrm{dom}(\mathcal{C}) \subseteq Y_S = \mathrm{dom}(\mathcal{C}_d)$. Let $x \in \mathrm{dom}(\mathcal{C})$, then $x \in \mathrm{dom}(\mathcal{C}_d)$ and therefore x is a non-blocking state of $T_\tau(\Sigma)/\mathcal{C}_d$. Let $p \in \mathcal{C}_d(x)$, since $\mathcal{K}(Q_\eta(x)) = \mathcal{C}(x) \neq \emptyset$, Definition 8 implies that $p = \mathcal{K}_d(Q_\eta(x)) \in \mathcal{K}(Q_\eta(x)) = \mathcal{C}(x)$. 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, since $\mathcal{C}$ 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 6 because there might be states in $\mathrm{dom}(\mathcal{C}_d)$ for which the safety specification is not met. 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.

4.2. Determinization of reachability controllers

We now do a similar work for reachability controllers. Let $\mathcal{K}$ and $\tilde{J}$ be the maps defined in Theorem 3 and let $\mathcal{C} = \mathcal{K} \circ Q_\eta$.

Definition 9. *A determinization of the set-valued map $\mathcal{K}$ is a univalued map $\mathcal{K}_d : Q_\eta(Y_S) \to P$ such that*

$$\forall q \in Q_\eta(Y_S \setminus Y_T),\ \tilde{J}(q) < +\infty \Rightarrow \mathcal{K}_d(q) \in \mathcal{K}(q).$$

If $\tilde{J}(q) = +\infty$, or if $q \notin Q_\eta(Y_S \setminus Y_T)$, 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 5. *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*

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

Then, for all $x \in \mathbb{R}^n$,

$$J(T_\tau(\Sigma)/\mathcal{C}_d, Y_S, Y_T, x) \leq \tilde{J}(Q_\eta(x)). \tag{10}$$

Proof. If $x \notin Y_S$, it follows that $J(T_\tau(\Sigma)/\mathcal{C}_d, Y_S, Y_T, x) = +\infty$ and that $J(T_\tau(\Sigma)/\mathcal{C}, Y_S, Y_T, x) = +\infty$. Then, equation (7) gives $\tilde{J}(Q_\eta(x)) = +\infty$ and (10) holds. If $x \in Y_S$ and $\tilde{J}(Q_\eta(x)) = +\infty$ then (10) clearly holds as well. The only remaining case is $x \in Y_S$ and $\tilde{J}(Q_\eta(x)) < +\infty$. We now proceed by induction to show that

$$J(T_\tau(\Sigma)/\mathcal{C}_d, Y_S, Y_T, x) \leq J(T_\tau(\Sigma)/\mathcal{C}, Y_S, Y_T, x) \tag{11}$$

which together with equation (7) gives (10). The induction is on the value of $J(T_\tau(\Sigma)/\mathcal{C}_d, Y_S, Y_T, x)$. Let x be such that $J(T_\tau(\Sigma)/\mathcal{C}_d, Y_S, Y_T, x) = 0$, then $x \in Y_T$ and $J(T_\tau(\Sigma)/\mathcal{C}, Y_S, Y_T, x) = 0$ as well. Let us assume that there exists $N \in \mathbb{N}$ such that for all x such that $J(T_\tau(\Sigma)/\mathcal{C}_d, Y_S, Y_T, x) \leq N$, equation (11) holds. We have shown that it is satisfied for $N = 0$. Then, let x such that $J(T_\tau(\Sigma)/\mathcal{C}_d, Y_S, Y_T, x) = N + 1$. Then, we have $0 < J(T_\tau(\Sigma)/\mathcal{C}_d, Y_S, Y_T, x) < +\infty$ which implies that $x \in Y_S \setminus Y_T$. Moreover, since $\tilde{J}(Q_\eta(x)) < +\infty$, we have by Definition 9 and by construction of $\mathcal{C}_d$, that $\mathcal{C}_d(x) \subseteq \mathcal{C}(x)$. Let $p \in \mathcal{C}_d(x)$ and $x' \in \mathcal{S}_1(x, p)$, then equation (5) gives that $J(T_\tau(\Sigma)/\mathcal{C}_d, Y_S, Y_T, x') \leq N$. Then, the induction assumption gives $J(T_\tau(\Sigma)/\mathcal{C}_d, Y_S, Y_T, x') \leq J(T_\tau(\Sigma)/\mathcal{C}, Y_S, Y_T, x')$. Then, equation (5) yields

$$\begin{aligned} J(T_\tau(\Sigma)/\mathcal{C}_d, Y_S, Y_T, x) &= 1 + \max_{p \in \mathcal{C}_d(x), x' \in \mathcal{S}(x,p)} J(T_\tau(\Sigma)/\mathcal{C}_d, Y_S, Y_T, x') \\ &\leq 1 + \max_{p \in \mathcal{C}_d(x), x' \in \mathcal{S}(x,p)} J(T_\tau(\Sigma)/\mathcal{C}, Y_S, Y_T, x') \\ &\leq 1 + \max_{p \in \mathcal{C}(x), x' \in \mathcal{S}(x,p)} J(T_\tau(\Sigma)/\mathcal{C}, Y_S, Y_T, x') \\ &\leq J(T_\tau(\Sigma)/\mathcal{C}, Y_S, Y_T, x). \end{aligned}$$

This completes the induction. ■

The previous result essentially states that using the controller $\mathcal{C}_d$, the reachability specification will be met for all initial states $x^0 \in Y_S$, such that $\tilde{J}(Q_\eta(x)) < +\infty$. Moreover, equation (11) shows that from those initial states, the entry time using the controller $\mathcal{C}_d$ cannot be larger than the entry time using the controller $\mathcal{C}$.

4.3. Efficient representation using algebraic decision diagrams

We now consider the problem of choosing an appropriate determinization $\mathcal{K}_d$ of $\mathcal{K}$ and a representation which requires little memory for its storage. We

explain our approach for safety controllers but it can be extended in a straightforward manner to handle reachability controllers as well. 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 $q \in Q_\eta(Y_S)$, $\mathcal{K}(q) = \emptyset$ or $p \in \mathcal{K}(q)$, we can choose $\mathcal{K}_d$ to be the map with constant value p on $Q_\eta(Y_S)$. The memory space needed to store $\mathcal{K}_d$ is then $O(1)$. If such an input value does not exist, then we can split (typically using a hyperplane) the set $Q_\eta(Y_S)$ 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.

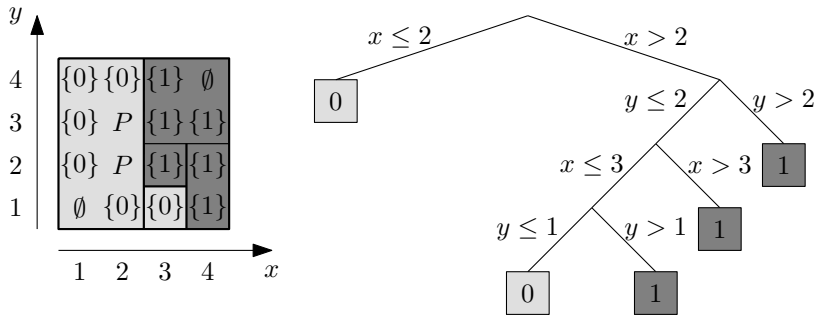

Figure 1: A set valued map $\mathcal{K} : \{1,2,3,4\}^2 \to 2^P$ where $P = \{0,1\}$ and a determinization given by colors (dark gray for 1, light gray for 0) and its representation using a tree structure.

Remark 3. For reachability controllers, the approach is essentially the same except that for all region in our partition there must be a mode $p \in P$ such that for all q in the region $\tilde{J}(q) = +\infty$ or $q \notin Q_\eta(Y_S \setminus Y_T)$ or $p \in \mathcal{K}(q)$.

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 execution time of 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 binary decision diagrams (a special class of ADD's) for representing control laws synthesized through symbolic models has already been considered in [16]. However, as far as we know, the idea of determinizing controllers in such a way that their determinization reduces the memory needed for its storage is new.

5. Example

For illustration purpose, we consider a simple thermal model of a two-room building (see e.g [17]):

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

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 $\mathcal{V} : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}_0^+$ given by $\mathcal{V}(T, T') = \|T - T'\|^2$ is a δ-GUAS Laypunov function for Σ with $\underline{\alpha}(r) = \overline{\alpha}(r) = r^2$ and $\kappa = 0.0084$. Moreover, equation (2) holds with $\gamma(r) = r^2$.

We first 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 (3), 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 (4), which is shown in the left part of 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 $\mathcal{K}$ represented by an array would require about 1 million memory units (this is the number of elements in $Q_\eta(Y_S)$). We computed a determinization $\mathcal{K}_d$ of $\mathcal{K}$ following the approach described in the previous section.

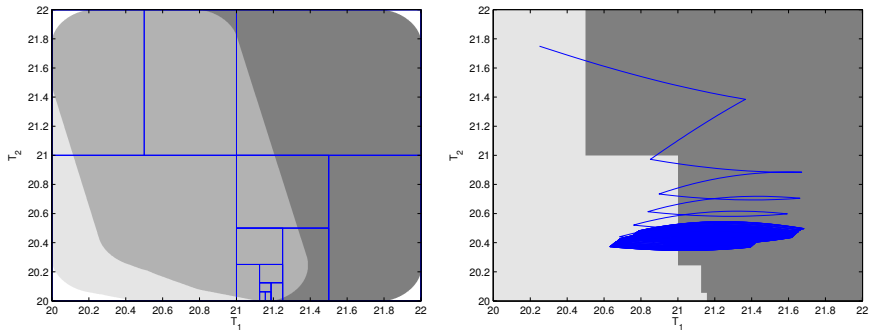

Figure 2: Left: Set-valued map $\mathcal{K} : Q_\eta(Y_S) \to 2^P$ (white: $\emptyset$, light gray: $\{1\}$, medium gray: P, dark gray: $\{0\}$). The number of elements in $Q_\eta(Y_S)$ is about 1 million. In blue, we represented the partition used for the representation of $\mathcal{K}_d$, a determinization of $\mathcal{K}$; the resulting tree structure has only 27 nodes. Right: Determinization $\mathcal{K}_d$ of the map $\mathcal{K}$ shown on the left (light gray: 1, dark gray: 0). In blue, a trajectory of the switched system controlled using the controller $\mathcal{C}_d = \mathcal{K}_d \circ Q_\eta$.

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 the right part of Figure 2 where we have also represented a trajectory of the switched system controlled using the controller $\mathcal{C}_d$. 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".

We now consider the problem of setting the temperature in the rooms between 20 and 22 degrees Celsius while keeping it between 17.5 and 22.5 along the way. This a reachability specification with $Y_S = [17.5, 22.5]^2$ and $Y_T = [20, 22]^2$. For the synthesis of the controller, we shall use an approximately bisimilar symbolic abstraction of $T_\tau(\Sigma)$ of precision $\varepsilon = 0.5$. According to equation (3), we can choose a state-space sampling parameter $\eta = 0.0035$ for the computation of the symbolic abstraction $T_{\tau,\eta}(\Sigma)$.

We computed a reachability controller $\mathcal{K}_\varepsilon$ for the symbolic abstraction $T_{\tau,\eta}(\Sigma)$ and the specification $\mathrm{Cont}_\varepsilon(Y_S) = [18, 22]^2$, $\mathrm{Cont}_\varepsilon(Y_T) = [20.5, 21.5]^2$. Then, we computed the map $\mathcal{K}$ given by equation (6), which is shown in the left part of Figure 3. For a practical implementation of the controller, the storage of the map $\mathcal{K}$ represented by an array would require about 1 million memory units.

We computed a determinization $\mathcal{K}_d$ of $\mathcal{K}$ following the approach described in the previous section. In Figure 3, we show the partition used for the repre-

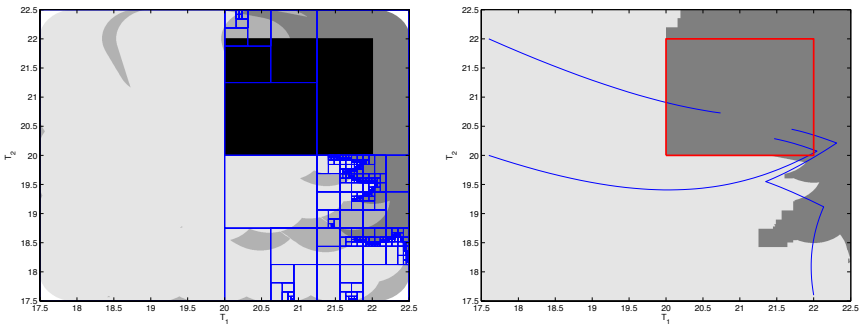

Figure 3: Left: Set-valued map $\mathcal{K} : Q_\eta(Y_S) \to 2^P$ (light gray: $\{1\}$, medium gray: P, dark gray: $\{0\}$, white: $\tilde{J}(q) = +\infty$, black: $q \notin Q_\eta(Y_S \setminus Y_T)$). The number of elements in $Q_\eta(Y_S)$ is about 1 million. In blue, we represented the partition used for the representation of $\mathcal{K}_d$, a determinization of $\mathcal{K}$; the resulting tree structure has 2249 nodes. Right: Determinization $\mathcal{K}_d$ of the map $\mathcal{K}$ shown on the left (light gray: 1, dark gray: 0). In blue, a trajectory of the switched system controlled using the controller $\mathcal{C}_d = \mathcal{K}_d \circ Q_\eta$.

sentation of $\mathcal{K}_d$. The map $\mathcal{K}_d$ is represented in the right part of Figure 2 where we have also represented a trajectory of the switched system controlled using the controller $\mathcal{C}_d$. For a practical implementation of the controller, the storage of the map $\mathcal{K}_d$ represented by a tree structure only requires 2249 memory units (this is the number of nodes in the tree). Though the compression is not as spectacular as in the previous example 2249 is still much less than 1 million. Morover, Theorem 5 gives insurance of "correctness by design".

6. Conclusion

In this paper, we have addressed the problem of synthesizing low-complexity quantized controllers for switched systems for safety and reachability specifications. 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 using other types of symbolic models such as multi-scale symbolic models introduced in [18].

References

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

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

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

[4] M. Kloetzer, C. Belta, A fully automated framework for control of linear systems from LTL specifications, in: Hybrid Systems: Computation and Control, Vol. 3927 of LNCS, Springer, 2006, pp. 333–347.

[5] G. Reißig, Computation of discrete abstractions of arbitrary memory span for nonlinear sampled systems, in: Hybrid Systems: Computation and Control, Vol. 5469 of LNCS, Springer, 2009, pp. 306–320.

[6] Y. Tazaki, J. I. Imura, Finite abstractions of discrete-time linear systems and its application to optimal control, in: 17th IFAC World Congress, 2008, pp. 10201–10206.

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

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

[9] M. Mazo Jr., P. Tabuada, Approximate time-optimal control via approximate alternating simulations, in: American Control Conference, 2010, pp. 10201–10206.

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

[11] A. Girard, Controller synthesis for safety and reachability via approximate bisimulation, Automatica 48 (5) (2012) 947–953.

[12] R. Bahar, E. Frohm, C. Gaona, G. Hachtel, E. Macii, A. Pardo, F. Somenzi, Algebraic decision diagrams and their applications, in: International Conference on Computer-Aided Design, 1993, pp. 188–191.

[13] A. Girard, Low-complexity switching controllers for safety using symbolic models, in: Analysis and Design of Hybrid Systems, 2012, pp. 82–87.

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

[15] J. Aubin, Viability kernels and capture basins of sets under differential inclusions, SIAM Journal of Control and Optimization 40 (3) (2001) 853–881.

[16] M. Mazo, A. Davitian, P. Tabuada, Pessoa: A tool for embedded controller synthesis, in: Computer Aided Verification, Vol. 6174/2010 of LNCS, 2010, pp. 566–569.

[17] K. Deng, P. Barooah, P. Mehta, S. Meyn, Building thermal model reduction via aggregation of states, in: American Control Conference, 2010, pp. 5118–5123.

[18] J. Camara, A. Girard, 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, pp. 520–525.