CoSyMA: A Tool for Controller Synthesis using Multi-scale Abstractions

Sebti Mouelhi, Antoine Girard, Gregor Gössler

CoSyMA: A Tool for Controller Synthesis using Multi-scale Abstractions*

Sebti Mouelhi
POP ART project
INRIA Grenoble Rhône-Alpes
38334 Saint-Ismier cedex, France

Antoine Girard
Laboratoire Jean Kuntzmann
Université de Grenoble
B.P. 53, 38041 Grenoble, France

Gregor Gössler
POP ART project
INRIA Grenoble Rhône-Alpes
38334 Saint-Ismier cedex, France

ABSTRACT

We introduce CoSyMA, a tool for automatic controller synthesis for incrementally stable switched systems based on multi-scale discrete abstractions. The tool accepts a description of a switched system represented by a set of differential equations and the sampling parameters used to define an approximation of the state-space on which discrete abstractions are computed. The tool generates a controller — if it exists — for the system that enforces a given safety or time-bounded reachability specification. We illustrate by examples the synthesized controllers and the significant performance gains during their computation.

Keywords

Switched systems, Multi-scale abstractions, Controller synthesis, Symbolic Algorithms.

1. INTRODUCTION

Controller synthesis for hybrid systems using discrete abstractions has become an established approach (see [12] and the references therein). In [6], it has been demonstrated that the (sampled) continuous behavior of incrementally stable [1] switched systems are *approximately bisimilar* to some discrete abstractions. The states of these abstractions are elements of lattices that approximate the continuous state-space. Time and space sampling parameters are chosen to achieve a desired precision; the smaller the time sampling parameter, the finer the lattice used for approximating the state-space, and consequently, the larger the number of states in the abstraction. The approach detailed in [4, 3] based on *multi-scale* discrete abstractions can be used to cope with this problem. These abstractions are defined over a set of embedded lattices. The finer lattices are only explored when the specification cannot be met at the coarsest level.

In this paper, we present CoSyMA (*COntroller SYnthesis using Multi-scale Abstractions*), a tool implementing symbolic approaches based on multi-scale abstractions to synthesize controllers for incrementally stable switched systems. CoSyMA accepts as input a switched system defined by differential equations indexed by a set of modes, time and space sampling parameters used to set an approximation of the continuous state-space, and a safety or a time-bounded reachability specification. If it exists, it computes a controller satisfying the specification. The tool is implemented using OCaml [8] and it is available (with documentation) for download at `multiscale-dcs.gforge.inria.fr`.

Approximately bisimilar abstractions are also used in the tool PESSOA [9]. PESSOA handles arbitrary switched or continuous systems (not only incrementally stable ones) and applies thus to a more general class of systems, however it does not feature the multi-scale discrete abstractions, which constitute the core of CoSyMA for which we implemented dedicated algorithms allowing us to reduce the computational effort demanded by controller synthesis.

2. THEORETICAL BACKGROUND

2.1 Incrementally stable switched systems

DEFINITION 2.1. *A* switched system *is a quadruple* $\Sigma = \langle \mathbb{R}^n, P, \mathcal{P}, F \rangle$ *where* $\mathbb{R}^n$ *is the state-space;* $P = \{1, \ldots, m\}$ *is a finite set of modes;* $\mathcal{P}$ *is the set of piecewise constant functions from* $\mathbb{R}^+$ *to* P*, continuous from the right and with a finite number of discontinuities on every bounded interval of* $\mathbb{R}^+$*;* $F = \{f_1, \ldots, f_m\}$ *is a collection of smooth vector fields indexed by* P*. For all modes* $p \in P$*,* $f_p : \mathbb{R}^n \to \mathbb{R}^n$ *is a locally Lipschitz continuous map.*

A *switching signal* of Σ is a function $\mathbf{p} \in \mathcal{P}$. A piecewise $\mathcal{C}^1$ function $\mathbf{x} : \mathbb{R}^+ \to \mathbb{R}^n$ is said to be a *trajectory* of Σ if it is continuous and there exists a switching signal $\mathbf{p} \in \mathcal{P}$ such that, at each $t \in \mathbb{R}^+$ where the function $\mathbf{p}$ is continuous, $\mathbf{x}$ is continuously differentiable and satisfies $\dot{\mathbf{x}}(t) = f_{\mathbf{p}(t)}(\mathbf{x}(t))$. We denote by $\mathbf{x}(t, x, p)$ the point reached at time t, starting from the state x and applying the constant switching signal $\mathbf{p}(s) = p$, for all $s \in [0, t]$. A switched system is δ-GUAS (i.e. globally uniformly asymptotically incrementally stable [1, 6]) if all the trajectories associated with the same switching signal converge asymptotically to the same reference trajectory independently of their initial states.

*This work was supported by the French project VEDECY number ANR 2009 SEGI 015 01 and the project UJF-MSTIC SYMBAD.

HSCC'13, April 8–11, 2013, Philadelphia, Pennsylvania, USA.

2.2 Approximate bisimulation

In this section we provide a brief introduction of the notion of approximate bisimulation that relates a switched system to the specific discrete abstraction we construct. Let us consider a class of transition systems of the form $T = \langle Q, L, r, O, H, I\rangle$ consisting of a set of states Q; a set of labels L; a transition relation $r \subseteq Q \times L \times Q$; an output set O; an output function $H : Q \to O$; a set of initial states $I \subseteq Q$. T is said to be *metric* if the output set O is equipped with a metric d, *discrete* if Q and L are finite or countable sets. For $q \in Q$ and $l \in L$ let $succs_l(q) = \{q' \in Q \mid (q, l, q') \in r\}$. An action $l \in L$ belongs to the set of *enabled actions* at the state q, denoted $Enab(q)$, if $succs_l(q) \neq \emptyset$. The transition system is said to be *deterministic* if for all $q \in Q$ and $l \in Enab(q)$, $succs_l(q)$ has only one element denoted by $succ_l(q)$. A *trajectory* of the transition system is a finite or infinite sequence of transitions $\sigma = q_0 l_0 q_1 l_1 q_2 l_2 \ldots$, it is *initialized* if $q_0 \in I$. A state $q \in Q$ is *reachable* if there exists an initialized trajectory reaching q. We denote by $\Phi(T)$ the set of all the trajectories of T.

Transition systems can describe the dynamics of switched systems. Given a switched system $\Sigma = \langle \mathbb{R}^n, P, \mathcal{P}, F\rangle$, let $T(\Sigma) = \langle Q, L, r, O, H, I\rangle$ be the transition system where the set of states is $Q = \mathbb{R}^n$; the set of labels is $L = P \times \mathbb{R}^+$; the transition relation is given by $(x, (p, \tau), x') \in r$ iff $\mathbf{x}(\tau, x, p) = x'$, i.e. the switched system Σ goes from state x to state x' by applying the constant mode p for a duration τ; the set of outputs is $O = \mathbb{R}^n$; the observation map H is the identity map over $\mathbb{R}^n$; the set of initial states is $I = \mathbb{R}^n$. $T(\Sigma)$ is deterministic and metric when the set of outputs $O = \mathbb{R}^n$ is equipped with the metric $d(x, x') = \|x - x'\|$. The relation between the discrete abstractions and $T(\Sigma)$ can be defined by an approximate bisimulation [5].

Definition 2.2. *Let $T_i = \langle Q_i, L_i, r_i, O_i, H_i, I_i\rangle$, for $i \in \{1, 2\}$, be metric transition systems where $L_1 = L_2$ and $O_1 = O_2$, equipped with the metric d, and a precision $\varepsilon \geq 0$. A relation $R \subseteq Q_1 \times Q_2$ is said to be an* ε-approximate bisimulation relation *between T_1 and T_2 if for all $(q_1, q_2) \in R$:*

- $d(H_1(q_1), H_2(q_2)) \leq \varepsilon$;
- $\forall (q_1, l, q_1') \in r_1$, $\exists (q_2, l, q_2') \in r_2$, *such that* $(q_1', q_2') \in R$;
- $\forall (q_2, l, q_2') \in r_2$, $\exists (q_1, l, q_1') \in r_1$, *such that* $(q_1', q_2') \in R$.

T_1 and T_2 are said to be approximately bisimilar with precision ε, denoted $T_1 \sim_\varepsilon T_2$, if for all $q_1 \in I_1$, there exists $q_2 \in I_2$, such that $(q_1, q_2) \in R$, and for all $q_2 \in I_2$, there exists $q_1 \in I_1$, such that $(q_1, q_2) \in R$.

2.3 Multi-scale abstractions

In applications where the switching has to be fast, uniform approximately bisimilar abstractions, as defined in [6], approximate the state-space using fine lattices which results in a huge number of abstract states. In practice, fast switching is generally necessary only on a restricted part of the state space. For instance, for safety specifications, fast switching is needed only when the system gets close to unsafe regions. In order to enable fast switching while using abstractions with a reasonable number of states, we consider discrete abstractions enabling transitions of different durations. For transitions of long duration, it is sufficient to consider abstract states on the coarse lattice. The finer ones are reached by shorter transitions only when the specification cannot be met at the coarsest level.

Let us consider a switched system Σ whose switching is determined by a time-triggered controller with time-periods in the finite set $\Theta_\tau^N = \{2^{-s}\tau \mid s = 0, \ldots, N\}$ that consists of dyadic fractions of a time sampling parameter $\tau > 0$ up to some scale parameter $N \in \mathbb{N}$. The dynamics of a switched system Σ is then described by the transition system $T_\tau^N(\Sigma) = \langle Q_1, P \times \Theta_\tau^N, r_1, O, H_1, I_1\rangle$ where $Q_1 = O = I_1 = \mathbb{R}^n$, H_1 is the identity map over $\mathbb{R}^n$, and $(x, (p, 2^{-s}\tau), x') \in r_1$ iff $\mathbf{x}(2^{-s}\tau, x, p) = x'$.

The discrete abstraction of $T_\tau^N(\Sigma)$ is defined on an approximation of $Q_1 = \mathbb{R}^n$ by a set of embedded lattices $[\mathbb{R}^n]_\eta^s$ defined by

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

where $s = 0, \ldots, N$, $q[i]$ is the i-th coordinate of q and $\eta > 0$ is a state space discretization parameter. By simple geometrical considerations, we can check that for all $x \in \mathbb{R}^n$ and $s = 0, \ldots, N$, there exists $q \in [\mathbb{R}^n]_\eta^s$ such that $\|x - q\| \leq 2^{-s}\eta$. Then, we can define the abstraction of $T_\tau^N(\Sigma)$ as the transition system $T_{\tau,\eta}^N(\Sigma) = \langle Q_2, P \times \Theta_\tau^N, r_2, O, H_2, I_2\rangle$, where the set of states is $Q_2 = [\mathbb{R}^n]_\eta^N$; the set of actions remains $L = P \times \Theta_\tau^N$; r_2 is defined such that $(q, (p, 2^{-s}\tau), q') \in r_2$ iff $q' = \arg\min_{m \in [\mathbb{R}^n]_\eta^s}(\|\mathbf{x}(2^{-s}\tau, q, p) - m\|)$. The approximation principle is illustrated in Figure 1. The observation map H_2 is the natural inclusion map from $[\mathbb{R}^n]_\eta^N$ to $\mathbb{R}^n$; the set of initial states is $I_2 = [\mathbb{R}^n]_\eta^0$.

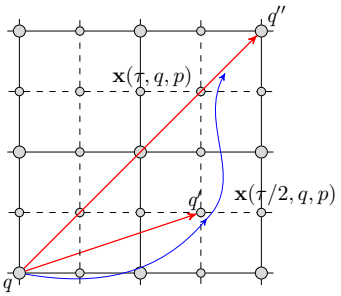

Figure 1: Computation of the discrete abstraction: $q' = succ_2(q, (p, \frac{\tau}{2})) = \arg\min_{m \in [\mathbb{R}^n]_\eta^1}(\|\mathbf{x}(\frac{\tau}{2}, q, p) - m\|)$ and $q'' = succ_2(q, (p, \tau)) = \arg\min_{m \in [\mathbb{R}^n]_\eta^0}(\|\mathbf{x}(\tau, q, p) - m\|)$

The resulting abstraction $T_{\tau,\eta}^N(\Sigma)$ is discrete and deterministic, its set of states and its set of actions are respectively countable and finite. For $N = 0$, we recover the "uniform" abstractions introduced in [6]. In [4], it was proved that for a switched system Σ admitting a common δ-GUAS Lyapunov function, $T_\tau^N(\Sigma) \sim_\varepsilon T_{\tau,\eta}^N(\Sigma)$ where the precision ε can be made arbitrarily small by reducing the state sampling parameter η.

2.4 Controller synthesis using multi-scale abstractions

Before presenting the tool details and our experimental results, we explain briefly how we use multi-scale abstractions for synthesizing safety and time-bounded reachability controllers. Let $T = \langle Q, L, r, O, H, I\rangle$ be a deterministic

transition system, a *controller* for T is a map $\mathcal{S} : Q \to 2^L$ such that for all $q \in Q$, $\mathcal{S}(q) \subseteq Enab(q)$. The system T controlled by $\mathcal{S}$ is $T/\mathcal{S} = \langle Q, L, r_{\mathcal{S}}, O, H, I\rangle$ where the transition relation is given by $(q, l, q') \in r_{\mathcal{S}}$ iff $(l \in \mathcal{S}(q) \wedge (q, l, q') \in r)$. The *support* of $\mathcal{S}$ is defined by $\mathsf{supp}(\mathcal{S}) = \{q \in Q \mid \mathcal{S}(q) \neq \emptyset\}$.

Safety controller synthesis

Given a safety specification $Q_S \subseteq Q$ (obtained from a subset $O_S \subseteq O$ of safe outputs), a state q of T is *controllable with respect to a safety specification* Q_S if $q \in Q_S$ and there exists an infinite trajectory $\sigma \in \Phi(T)$ starting from q and remaining in Q_S. We denote the set of controllable states of T with respect to the safety specification Q_S by $SCont(T, Q_S)$. A *safety controller* $\mathcal{S}$ for T and Q_S is defined such that $\mathsf{supp}(\mathcal{S}) \subseteq SCont(T, Q_S)$ and for all $q \in \mathsf{supp}(\mathcal{S})$: (1) $q \in Q_S$ (safety) and (2) $\forall l \in \mathcal{S}(q)$, $succ_l(q) \in \mathsf{supp}(\mathcal{S})$ (deadend freedom). The set $SCont(T, Q_S)$ is computable for discrete abstractions. However, the larger the number of states, the more expensive the computation. For that reason, we want to capitalize on multi-scale abstractions to propose an efficient algorithm for safety controller synthesis.

The lazy safety synthesis problem consists in controlling a system so as to keep any trajectory starting from some initial state in I within the safe subset of states Q_S, while applying at each state transitions of the longest possible duration for which safety can be guaranteed. For that purpose we define a priority relation on the set of labels $L = P \times \Theta_\tau^N$ giving priority to transitions of longer duration: for $l, l' \in L$ with $l = (p, \tau)$, $l' = (p', \tau')$, $l \preceq l'$ iff $\tau \leq \tau'$, $l \prec l'$ iff $\tau < \tau'$ and $l \cong l'$ iff $\tau = \tau'$. Given a subset of labels $L' \subseteq L$, we define $\max_{\preceq}(L') = \{l' \in L' \mid \forall l \in L', l \preceq l'\}$.

Definition 2.3. *A* maximal lazy safety (MLS) controller $\mathcal{S} : Q \to 2^L$ *for* T *and* Q_S *is a safety controller such that* $I \cap SCont(T, Q_S) \subseteq \mathsf{supp}(\mathcal{S})$ *and for all states* $q \in \mathsf{supp}(\mathcal{S})$*, we have: (1) if* $l \in \mathcal{S}(q)$*, then for any* $l \prec l'$*,* $succ_{l'}(q) \notin SCont(T, Q_S)$ *(laziness), and (2) if* $l \in \mathcal{S}(q)$*, then for any* $l \cong l'$*,* $l' \in \mathcal{S}(q)$ *iff* $succ_{l'}(q) \in SCont(T, Q_S)$ *(maximality).*

The MLS controller exists and is unique as proved in [3].

Time-bounded reachability controller synthesis

Given a transition system $T = \langle Q, L, r, O, H, I\rangle$, for all transitions $(q, l, q') \in r$, let $\delta(l)$ be the time needed by T to reach q' from q by action l. For all finite trajectories $\sigma = q_0 l_0 q_1 l_1 \dots l_{n-1} q_n$ in $\Phi(T)$, we define its *duration* by $\Delta(\sigma) = \delta(l_0) + \delta(l_1) + \dots + \delta(l_{n-1})$. For instance, for the transition systems $T_\tau^N(\Sigma)$ and $T_{\tau,\eta}^N(\Sigma)$, we have $L = P \times \Theta_\tau^N$ and for all $l = (p, 2^{-s}\tau) \in L$, we have $\delta(l) = 2^{-s}\tau$.

To formally define a time-bounded reachability controller, we define $C(T) = \langle Q_c, L, r_c, O, H_c, I_c\rangle$ the *transition system with clock* of T where $Q_c = Q \times \mathbb{R}^+$ is the set of states Q extended by a clock; for all $((q, c), l, (q', c')) \in r_c$, $(q, l, q') \in r$ and $c' = c + \delta(l)$; $H_c((q, c)) = H(q)$ for all $(q, c) \in Q_c$; $I_c = I \times \{0\}$. The set of reachable states of $C\big(T_{\tau,\eta}^N(\Sigma)\big)$ is countable and defined by $Q \times 2^{-N}\tau\mathbb{N}$. Given a maximal time bound $B \in \mathbb{R}^+$, the state (q, c) of $C(T)$ is controllable with respect to a time-bounded reachability specification (Q_S, Q_T, B), where $Q_T \subseteq Q_S$ if (1) $q \in Q_S$ and there exists a finite trajectory σ of T starting from q, eventually reaching Q_T, and remaining in Q_S until reaching Q_T, such that $c + \Delta(\sigma) \leq B$. The set of these states is denoted by $RCont(C(T), Q_S, Q_T, B)$.

Next we define time-bounded reachability controllers using the notion of safety controllers. We start by defining the notion of *stuttering* ($\circ$) actions. An outgoing transition from a state q labeled by a stuttering action loops on the same state ($succ_\circ(q) = q$ and $\delta(\circ) = 0$).

Let us now define $T_{\circlearrowleft Q'} = \langle Q, L \cup \{\circ\}, r^{\circlearrowleft}, O, H, I\rangle$ for $Q' \subseteq Q$ such that

$$(q, l, q') \in r^{\circlearrowleft} \text{ iff } \begin{cases} q = q' & \text{if } l = \circ \text{ and } q \in Q'; \\ (q, l, q') \in r & \text{if } l \neq \circ \text{ and } q \in Q \setminus Q'. \end{cases}$$

$T_{\circlearrowleft Q'}$ is the transition system derived from T where the only actions enabled from a state in Q' are stuttering.

Since we are not concerned with the evolution of the system after reaching the target Q_T, we will use the transition system $C(T_{\circlearrowleft Q_T}) = \langle Q_c, L, r_c^{\circlearrowleft}, O,\ H_c, I_c\rangle$ rather than $C(T)$. We easily show that $RCont(C(T_{\circlearrowleft Q_T}), Q_S, Q_T, B) = RCont(C(T),\ Q_S, Q_T, B) = SCont(C(T_{\circlearrowleft Q_T}),\ Q_S \times [0, B])$.

A *time-bounded reachability controller* for the transition system $C(T_{\circlearrowleft Q_T})$ and (Q_S, Q_T, B) is a safety controller for $C(T_{\circlearrowleft Q_T})$ and $Q_S \times [0, B]$. We define the maximal lazy time-bounded reachability controller based on Definition 2.3 as follows.

Definition 2.4. *The* maximal lazy time-bounded reachability (MLBR) controller $\mathcal{R}^m : Q \times \mathbb{R}^+ \to 2^L$ *for* $C(T_{\circlearrowleft Q_T})$ *and* (Q_S, Q_T, B) *is the MLS controller for* $C(T_{\circlearrowleft Q_T})$ *and* $Q_S \times [0, B]$.

It is clear, based on the previous definition, that $\mathcal{R}^m$ is unique and that Q_T is reachable within the specified time bound starting from controllable initial states. We can use the algorithm synthesizing MLS controllers proposed in [3] to synthesize MLBR controllers. However, their computation is expensive because dealing with problems of n dimensions amounts to handle the equivalents of $n+1$ dimensions by adding a clock. To avoid this constraint, we can settle for a sub-controller $\mathcal{V}$ of $\mathcal{R}^m$ such that all controllable initial states of $\mathcal{R}^m$ are also controllable by $\mathcal{V}$.

Let $\mathcal{R}^m$ be the MLBR controller for $C(T_{\circlearrowleft Q_T})$ and $(Q_S,\ Q_T, B)$. A *sub-controller* $\mathcal{V}$ of $\mathcal{R}^m$ is a time-bounded reachability controller for $C(T_{\circlearrowleft Q_T})$ and (Q_S, Q_T, B) such that for all $(q, c) \in \mathsf{supp}(\mathcal{V})$, $\mathcal{V}((q, c)) \subseteq \mathcal{R}^m((q, c))$. The sub-controller $\mathcal{V}$ is *complete* if $\{i \in I \mid (i, 0) \in \mathsf{supp}(\mathcal{R}^m)\} = \{i \in I \mid \exists 0 \leq c \leq B \mid (i, c) \in \mathsf{supp}(\mathcal{V})\}$. We can now define static reachability controllers based on the previous definition.

Definition 2.5. *Consider a complete sub-controller* $\mathcal{V}$ *of* $\mathcal{R}^m$*. The* static reachability controller $\mathcal{R}_{\mathcal{V}}^{ls} : Q \to 2^L$ *for* $T_{\circlearrowleft Q_T}$ *and* (Q_S, Q_T, B) *obtained from* $\mathcal{V}$ *is the controller such that for all* $(q, c) \in \mathsf{supp}(\mathcal{V})$*,* $q \in \mathsf{supp}(\mathcal{R}_{\mathcal{V}}^{ls})$ *and for all* $q \in \mathsf{supp}(\mathcal{R}_{\mathcal{V}}^{ls})$*,* $\mathcal{R}_{\mathcal{V}}^{ls}(q) = \mathcal{V}\big((q, c_{max}(q))\big)$ *where* $c_{max}(q) = max\{c' \mid (q, c') \in \mathsf{supp}(\mathcal{V})\}$.

It can be shown that using $\mathcal{R}_{\mathcal{V}}^{ls}$, Q_T is reachable within the specified time bound starting from all controllable initial states (see [10]). For time-bounded reachability specifications CoSyMA synthesizes static reachability controllers. In the next section, we present some details about the tool.

3. TOOL DETAILS

In this section, we present the internal architecture of CoSyMA, its description language, and our implementation

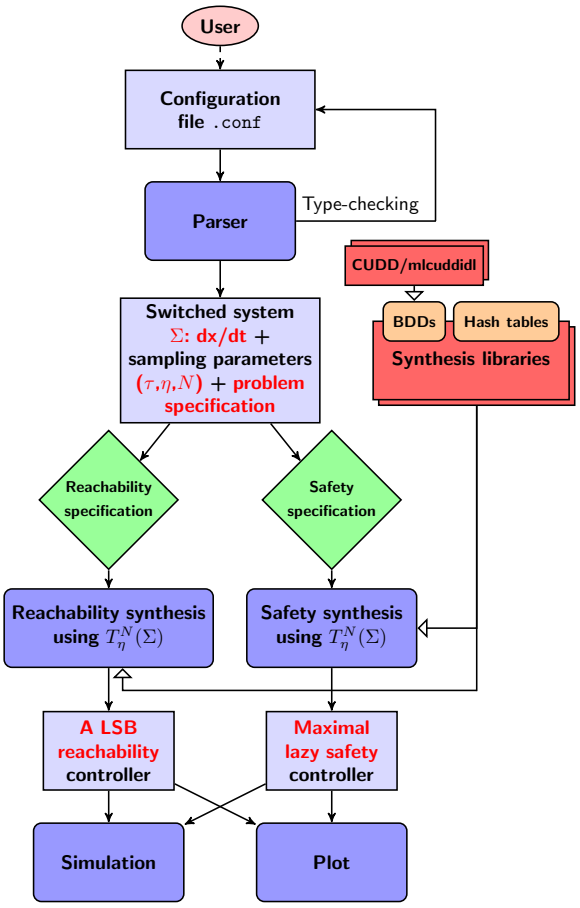

Figure 2: Execution flow of CoSyMA

choices. CoSyMA accepts a configuration (`.conf`) file describing the system and the synthesis parameters. It contains in the order: the description of a switched system Σ in terms of differential equations $\dot{\mathbf{x}}(t) = f_{\mathbf{p}(t)}(\mathbf{x}(t))$; time τ and space η sampling parameters, and the scale N used to compute the finer lattice $[\mathbb{R}]^N_\eta$ that approximates the continuous state-space; a safety specification Q_S or a time-bounded reachability specification (Q_S, Q_T, B); the plot parameters. The grammar is detailed in the reference manual of the tool.

The execution flow of the tool, shown in Figure 2, represents the different steps by which the tool synthesizes the controllers of the described system according to the given safety or a time-bounded reachability specification. After the parsing of the configuration file, the tool represents the vector fields f_p for each switching mode p by an OCaml function of type `float -> float array -> float array`. It computes the successor of a state q under a label $l = (p, 2^{-s}\tau)$ by solving $\dot{\mathbf{x}}(t) = f_p(\mathbf{x}(t))$ for $t \in [0, \delta(l)]$ and $\mathbf{x}(0) = q$ using the common fourth-order Runge-Kutta method. The tool synthesizes the controllers based on $T^N_{\tau,\eta}$ approximately bisimilar to T^N_τ (cf. Section 2.3). For safety specifications Q_S, the tool synthesizes the MLS controller based on the algorithm presented in [3] which computes the abstraction $T^N_{\tau,\eta}$ on the fly.

For time-bounded reachability specifications (Q_S, Q_T, B), it uses a new algorithm computing the static reachability controller $\mathcal{R}^{ls}_{\mathcal{V}}$ where $\mathcal{V}$ is a complete sub-controller of the MLBR controller $\mathcal{R}^m$ for $C(T_{\circlearrowleft Q_T})$ and (Q_S, Q_T, B) (with $T = T^N_{\tau,\eta}(\Sigma)$). The algorithm is a depth-first traversal of paths $\sigma \in \Phi(T^N_{\tau,\eta}(\Sigma))$ starting from initial states I until reaching Q_T to keep track of the clocks of the states reached by σ. From an operational point of view, the complete sub-controller $\mathcal{V} \subseteq \mathcal{R}^m$, according to which the static reachability controller $\mathcal{R}^{ls}_{\mathcal{V}}$ is defined, is computed according to the order of exploration of initial states I. By keeping the problem at its original dimension, the synthesis complexity is significantly reduced. The algorithm details are given in the reference manual [10].

The user has the choice to represent the system abstractions either by *enumerated types* or *boolean functions*. The tool uses *hash tables* as an enumerated type to operate on the system abstractions. Hash tables turn out to be more efficient than search trees or other table lookup structures, especially for large numbers of entries. Alternatively, the tool can use BDDs (*Binary Decision Diagrams*) [2] to represent the system abstractions. BDDs are able to represent sets and relations compactly in memory as boolean functions. We implement BDDs using the modules `Cudd.Man` and `Cudd.Bdd` of the OCaml IDL interface MLCUDDIDL [7] of the CUDD (*CU Decision Diagram*) package [11]. However, using BDDs makes the controller synthesis algorithms presented above more costly than hash tables since the symbolic abstraction is constructed by enumerating the states and computing their successors using the Runge-Kutta method.

The Plot backend of CoSyMA uses its own TikZ/Pgf scripts [13] used to generate plots for controllers and their simulation.

4. EXPERIMENTAL RESULTS

DC-DC Converter

As a first case study, we apply our approach to a boost DC-DC converter. It is a switched system with two modes, the two dimensional dynamics associated with both modes are affine of the form $\dot{\mathbf{x}}(t) = a_p\mathbf{x}(t) + b$ for $p \in \{1, 2\}$ (see [6] for numerical values). It can be shown that it is incrementally stable and thus approximately bisimilar discrete abstractions can be computed. We consider the problem of keeping the state of the system in a desired region of operation given by the safe set $O_S = [1.15, 1.55] \times [5.45, 5.85]$.

We use approximately bisimilar abstractions to synthesize MLS controllers for the DC-DC converter. We compare the cost of controller synthesis for the uniform abstraction $T^0_{\tau_1,\eta_1}$ for parameters $\tau_1 = 0.5s$ and $\eta_1 = 10^{-3}\sqrt{2}/4$ (containing transitions of duration 0.5s) and the multi-scale abstractions $T^2_{\tau_2,\eta_2}$ for parameters $\tau_2 = 4\tau_1$ and $\eta_2 = 4\eta_1$ (containing transitions of durations in $\Theta^2_\tau = \{2s, 1s, 0.5s\}$). These two abstractions have the same precision. Table 1 details the experimental results obtained for the synthesis of the controllers for $T^0_{\tau_1,\eta_1}$ and $T^2_{\tau_2,\eta_2}$. We can see that there is a noteworthy reduction of the time used to compute the controller using multi-scale abstractions instead of using uniform ones (up to a 86% improvement between $T^0_{\tau_1,\eta_1}$ and $T^2_{\tau_2,\eta_2}$). This is due to the fact that the size of uniform abstractions grows exponentially with higher resolutions, whereas using multi-scale abstractions are refined only when we get close to unsafe regions (reduction of more than 91% between $T^0_{\tau_1,\eta_1}$ and

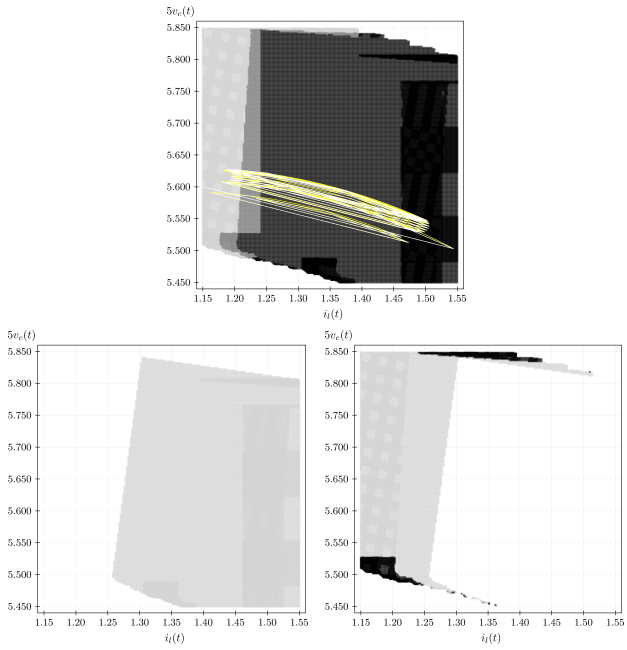

Figure 3: The MLS controller for $T^2_{\tau_2,\eta_2}$ and Q_S. Top: mode 1 is activated (light gray); mode 2 is activated (black); modes 1 and 2 (gray); Bottom (Left): actions of 2s are enabled (light gray); Bottom (right): actions of 1s are enabled (light gray), actions of 0.5s are enabled (black).

$T^2_{\tau_2,\eta_2}$). Interestingly, this reduction in computation time and size does not affect the performance of the multi-scale controllers, which yield a ratio of controllable initial states[1] (CR) over the safety specification comparable to that of their its uniform counterparts. It is worth emphasizing that using CoSyMA there is a remarkable reduction of the computation times compared to those reported in [3] obtained by a prototype implementation of the algorithm. Figure 3 depicts the maximal lazy safety controller for $T^2_{\tau_2,\eta_2}$ and Q_S and the trace of its simulation starting from the state (1.15,5.6).

	Abstractions $T^N_{\tau,\eta}$	
	$N=0, \tau=0.5s$, $\eta=10^{-3}\sqrt{2}/4$, $\varepsilon=0.1$	$N=2, \tau=2s$, $\eta=10^{-3}\sqrt{2}$, $\varepsilon=0.1$
Time	8.32s	1.10s
Size	599 294	53 479
$\delta(l)$	0.5s (100%)	2s (63.61%) 1s (31.67%) 0.5s (4.72%)
CR	93.52%	93.51%

Table 1: Experimental results for the MLS controller synthesis for the boost DC-DC converter

Now, we consider the time-bounded reachability specification (Q_S, Q_T, B) where $Q_S = [0.65, 1.65] \times [4.95, 5.95]$, $Q_T = [1.1, 1.6] \times [5.4, 5.9]$ and $B = 20s$. We synthesize static reachability controllers respectively for $T^0_{\tau_1,\eta_1}$ where $\tau_1 = 0.25$ and $\eta_1 = 10^{-3}\sqrt{2}/4$, and $T^2_{\tau_2,\eta_2}$ where $\tau_2 = 4\tau_1$ and $\eta_2 = 4\eta_1$, and the specification (Q_S, Q_T, B).

As shown in Section 2.4, the MLBR controller for the abstraction $C(T_{\circlearrowleft Q_T})$ and (Q_S, Q_T, B) where T equal to $T^0_{\tau_1,\eta_1}$ or $T^2_{\tau_2,\eta_2}$ is the maximal lazy safety controller for $C(T_{\circlearrowleft Q_T})$ and the safety specification $Q_S \times [0, B]$. Its computation is costly because the problem is grown from 2 to 3 dimensions by considering the supplementary clock parameter. Synthesizing a static reachability controller rather than an MLB reachability controller significantly reduces complexity. In Table 2, we observe a considerable reduction of the size of the controlled abstraction of $T^2_{\tau_2,\eta_2}$ of more than 91.46% compared to that of $T^0_{\tau_1,\eta_1}$ with comparable controllability ratios of initial states. Also, the computation time of the controller of $T^2_{\tau_2,\eta_2}$ is slightly shorter than that of $T^0_{\tau_1,\eta_1}$.

	Abstractions $T^N_{\tau,\eta}$	
	$N=0, \tau=0.5s$, $\eta=10^{-3}\sqrt{2}/4$, $\varepsilon=0.1$	$N=2, \tau=2s$, $\eta=10^{-3}\sqrt{2}$, $\varepsilon=0.1$
Time	658 s	223 s
Size	3 149 538	262 593
$\delta(l)$	0.5s (100%)	2s (72.26%) 1s (15.77%) 0.5s (11.97%)
CR	89.97%	90.30%

Table 2: Experimental results for the static reachability controller for the boost DC-DC converter

Building Temperature Regulation

The second case study deals with temperature regulation in a circular building. Each room is equipped with a heater and at a given instant at most one heater is switched on. The temperature t_i of the room i is defined by the differential equation $\dot{t_i} = \alpha(t_{i+1} + t_{i-1} - 2t_i) + \beta(t_e - t_i) + \gamma(t_h - t_i)u_i(t)$ where t_{i-1} is the temperature of the room $i-1$; t_{i+1} is the temperature of the room $i+1$; t_e is the temperature of the external environment of the building; t_h is the temperature of the heater; α is the temperature transfer ratio between the rooms $i \pm 1$ and the room i; β is the temperature transfer ratio between the external environment and the room i; γ is the temperature transfer ratio between the heater and the room i; $u_i(t)$ equals to 1 if the room i is heated, or 0 otherwise. Given a number $n \geq 2$ of rooms, we distinguish $n+1$ switching modes. For $1 \leq i \leq n$, the mode p_i represents the mode of activating the heater of room i. The mode p_{n+1} represents that no heater is activated. The values of α, β, γ, t_e, and t_h are respectively 1/20, 1/200, 1/100, 10, and 50. We will increase the system dimension to test the limits of the tool in terms of memory usage and computation time. Given the safety specification $Q_S = [20.0, 22.0]^n$ for $n \in \{3, 4, 5\}$, we synthesize safety controllers for buildings of three, four, and five rooms. The values of τ and η are given in Table 3. By looking to the results, we can see the combinatorial explosion of the size of abstractions by increasing the system dimension from 3 to 5. Also, it makes sense that the ratio of controllability of initial states decreases by increasing the number of rooms. On our machine equipped with a Core i5-2430M and 4GB of RAM, synthesis fails for the 6-dimensional instance due to running out of memory. Figure 4 shows the MLS controller for the transition sys-

[1]The ratio of controllable initial states for a controller $\mathcal{S} : Q \to 2^L$ and a system $T = (Q, L, \to, O, H, I)$ is computed as $|\{q \in I | \mathcal{S}(q) \neq \emptyset\}|/|I|$.

	Abstractions $T^N_{\tau,\eta}$		
	$n=3,\ N=2,$ $\eta=50\times10^{-3}$ $\tau=20s$ $\varepsilon=0.2$	$n=4,\ N=2,$ $\eta=50\times10^{-3}$ $\tau=20s$ $\varepsilon=0.2$	$n=5,\ N=1$ $\eta=0.1$ $\tau=10s$ $\varepsilon=0.4$
Time	2.40s	595 s	571 s
Size	55 564	3 927 564	6 135 218
$\delta(l)$	20s (20.06%) 10s (79.94%) 5s (0%)	20s (8.77%) 10s (86.99%) 5s (4.24%)	10s (86.44%) 5s (13.56%)
CR	99.99%	99.89%	99.79%

Table 3: Comparison of experimental results for the safety synthesis for the temperature regulator system of three, four, and five dimensions

tem $T^2_{20,0.05}$ of three dimensions and the safety specification $Q_S = [20.0, 22.0]^3$. The plots are slices of the state space in the dimensions (t_1, t_2) for a fixed $t_3 \approx 20^\circ$ (left) and $t_3(t) \approx 22^\circ$ (right), respectively. The plots on the top depict scales and those in the middle and the bottom depicts modes. We can remark the predominance of the mode p_4 (no heater is activated) by increasing the temperature of third room.

5. CONCLUSION

In this paper we have introduced CoSyMA, a tool that automatically synthesizes controllers for incrementally stable switched systems based on multi-scale discrete abstractions. We have illustrated by examples the synthesized controllers for safety and time-bounded reachability problems. The benchmarks provide evidence that the use of multi-scale abstractions leads to a substantial reduction of synthesis time and size of the obtained controller while maintaining coverage of the state space.

6. REFERENCES

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

[2] R. E. Bryant. Graph-based algorithms for Boolean function manipulation. *IEEE Transactions on Computers*, 35(8):677–691, 1986.

[3] J. Cámara, A. Girard, and G. Gössler. Safety controller synthesis for switched systems Using multi-scale symbolic models. In *IEEE Conference on Decision and Control and European Control Conference*, pages 520–525. IEEE, 2011.

[4] J. Cámara, A. Girard, and G. Gössler. Synthesis of switching controllers using approximately bisimilar multiscale abstractions. In *Hybrid Systems: Computation and Control*, pages 191–200. ACM, 2011.

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

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

[7] B. Jeannet. MLCUDDIDL: OCaml interface for CUDD library, version 2.2.0, 2011. `http://pop-art.inrialpes.fr/~bjeannet/mlxxidl-forge/mlcuddidl/html/Cudd.html`.

[8] X. Leroy, D. Doligez, A. Frisch, J. Garrigue, D. Rémy, and J. Vouillon. The Objective Caml system release 3.12. Documentation and user manual, 2010.

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

[10] S. Mouelhi, G. Gössler, and A. Girard. Synthesizing controllers for switched systems using COSYMA. Technical report, INRIA, 2012.

[11] F. Somenzi. CUDD: CU decision diagram package. `http://vlsi.colorado.edu/~fabio/CUDD`.

[12] P. Tabuada. *Verification and control of hybrid systems: a symbolic approach*. Springer, 2009.

[13] T. Tantau. The TikZ and PGF packages, manual for version 2.10, 2010.

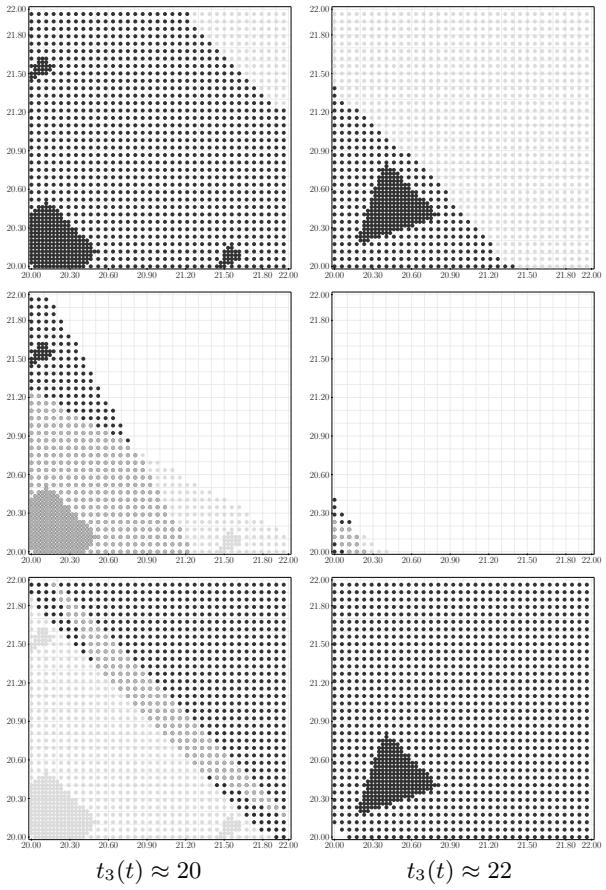

Figure 4: MLS controller for $T^2_{20,0.05}$ of three dimensions and Q_S; Horizontal axis: $t_1(t)$; Vertical axis: $t_2(t)$; Top: actions of 20s are enabled (black); actions of 10s are enabled (gray); Middle: mode p_1 (black); mode p_2 (light gray); p_1 and p_2 (gray); Bottom: mode p_4 (black); mode p_3 (light gray); p_3 and p_4 (gray).