ESTIMATING REACHABLE STATES OF HYBRID SYSTEMS VIA l-COMPLETE APPROXIMATIONS

Thomas Moor
Universität der Bundeswehr Hamburg
D - 22039 Hamburg, FR Germany
e-mail: thomas.moor@unibw-hamburg.de
Tel./Fax: +49-40-6541 2121/2822

Jörg Raisch
Max-Planck-Institut für Dynamik komplexer technischer Systeme, Leipziger Str. 44
D-39120 Magdeburg, FR Germany
e-mail: raisch@mpi-magdeburg.mpg.de
Tel./Fax: +49-391-6117 502/501

ABSTRACT

This contribution treats the estimation of reachable states for time invariant hybrid systems. Using the framework provided by *Willems'* behavioural systems theory, we suggest a method based on l-complete approximations, which can be realized by finite state machines. The approximating behaviour is a superset of the original behaviour. Hence, the estimate of reachable states based on an l-complete approximation can be shown to be conservative, i. e. the exact set of reachable states is guaranteed to be contained in the estimate. Because of this property our method is adequate for verification tasks where the state variable has to remain within a certain specification.

KEYWORDS

Hybrid systems, reachable states, verification, behavioural approach, l-complete approximations.

INTRODUCTION

Within the scope of this paper, a hybrid state space is the product of a finite set and an $\mathbb{R}$ vector space. The considered hybrid systems are discrete time state systems with hybrid state space. It is only under very restrictive assumptions that the set $\mathcal{R}$ of states which are reachable within arbitrary time can be computed *exactly*. In general, it is not even possible to explicitly characterize the set of states which are reachable within one time step. It is common practice to approximate the latter set, and to repeatedly apply this one-step procedure (see [1] and [4] for algorithms based on this idea). This results in an increasing sequence of *subsets* of $\mathcal{R}$. The procedure has found the exact solution if and only if two successive sets turn out to be equal. Unfortunately, the algorithm is not guaranteed to terminate; hence the best result achieved within any finite time may happen to be a number of strict subsets of $\mathcal{R}$. Clearly, this is not adequate for verification purposes, where one needs to *guarantee* that the state remains within a certain set X_{spec}. In the sequel, we propose a method based on l-complete approximations that overcomes this problem: it provides a decreasing sequence $\mathcal{R}_l$ of *supersets* of $\mathcal{R}$. $\mathcal{R}_l \subseteq X_{spec}$ implies $\mathcal{R} \subseteq X_{spec}$; hence, the method is well suited for verification tasks.

In general, one obtains a discrete behaviour (i. e. a behaviour with finite signal space) from a system with infinite state space by introducing a suitable finite partition of the state space. For hybrid state systems this can be done by projecting the hybrid state space onto its discrete component. However, the resulting discrete behaviour is no state space system anymore, raising the question of a realization, preferable by a finite state machine. If one succeeds in this task, the analysis of the hybrid state space system can be done by standard methods from the field of finite state machines. When the discrete behaviour turns out to be l-complete, such a realization can be set up in a straightforward manner. Of course, in general it cannot be expected that a finite state machine can represent the discrete dynamics of a hybrid system exactly, hence the discrete behaviour in general will not be l-complete. Therefore, we propose an l-complete approximation representing the discrete dynamics of the underlying hybrid system to "some extent". Our approximation scheme exhibits two crucial properties: first, the approximating behaviour is guaranteed to be a superset of the original behaviour. Second, the method provides a sequence of approximations which is expected to improve and which is guaranteed not to deteriorate. In fact l-complete approximations turn out to be convenient for many purposes; e. g. see [6] for supervisory control based on l-complete approximations.

This paper is organized as follows: in the Section "Hybrid systems", we give a definition of hybrid state machines within the "behavioural approach". In the Section "l-Complete approximations", these are defined and realized by finite state machines. The main results are stated in the section "Estimates of reachable states". In the Section "Example", the results are applied to a thermal switched server system.

HYBRID SYSTEMS

The proposed approximation scheme relies on three basic definitions from *Willems'* "behavioural approach": *dynamical systems*, *time invariance*, and *completeness*. For the reader's convenience, these definitions are collected here:

Definition 1. (See [10], Def. II.1) A *dynamical system* Σ is a triple $(T,\, W,\, \mathfrak{B})$ with $T \subseteq \mathbb{R}$ the *time axis*, W the *signal space*, and $\mathfrak{B} \subseteq W^T := \{f \mid f : T \to W\}$ the *behaviour*. □

The behaviour is viewed as the set of all trajectories which are compatible with the phenomena modelled by the system: trajectories $w \notin \mathfrak{B}$ cannot occur. In the sequel, we restrict ourselves to discrete time systems with finite past, that is $T = \mathbb{N}_0$. Let σ^t denote the *backwards t-shift*, i.e. $(\sigma^t f)(\tau) := f(t+\tau)$ for all $\tau \in \mathbb{N}_0$, and $\sigma := \sigma^1$. Then:

Definition 2. (See [10], Def. II.3) A dynamical system $\Sigma = (\mathbb{N}_0,\, W,\, \mathfrak{B})$ is said to be *time invariant* if $\sigma\mathfrak{B} \subseteq \mathfrak{B}$. □

Implicitly, a system is uniquely determined by its behaviour; we therefore refer to a *behaviour* as being time invariant, if it belongs to a time invariant *system*. This convention is also used with respect to all properties defined in the sequel.

Definition 3. (See [10], Def. II.4) Let $l \in \mathbb{N}$. A time invariant dynamical system $\Sigma = (\mathbb{N}_0,\, W,\, \mathfrak{B})$ is said to be *l-complete* if

$$w \in \mathfrak{B} \quad \Leftrightarrow \quad \sigma^t w\big|_{[0,l]} \in \mathfrak{B}\big|_{[0,l]} \quad \forall\, t \in \mathbb{N}_0\,. \tag{1}$$

□

Here, $w|_{[t_1,t_2]}$ denotes the restriction of the map $w\colon \mathbb{N}_0 \to W$ to the domain $[t_1, t_2]$. To keep notation reasonably compact, we do not distinguish between $w|_{[t_1,t_2]} \in W^{[t_1,t_2]}$ and $(w(t_1), \dots w(t_2)) \in W^{t_2-t_1+1}$. Note that shifting is defined to be of higher priority than restricting: $\sigma^t w|_{[0,l]} = (\sigma^t w)|_{[0,l]} = w|_{[t,t+l]}$.

The following definition provides a link between standard terminology from the field of (finite) state machines and the behavioural approach.

Definition 4. Let the sets X and $\delta \subseteq X \times X$ denote the *state space* and the *next state relation* respectively. The pair $P = (X, \delta)$ is called a *state machine*. If $|X| \in \mathbb{N}$ (X counts only a finite number of elements), P is said to be a *finite state machine*. The behaviour $\mathfrak{B}_s := \{x|\ (x(t), x(t+1)) \in \delta\ \forall\, t \in \mathbb{N}_0\}$ is referred to as the *induced state behaviour*, and $\Sigma_s := (\mathbb{N}_0, X, \mathfrak{B}_s)$ as the *induced state space system*. Further, let the set W and the map $\gamma\colon X \to W$ denote the *external signal space* and the *readout-map*. respectively. The tuple $P_{ex} = (X, W, \delta, \gamma)$ is then called a *state machine with external signals*. The external behaviour of P_{ex} is defined to be the image of $\mathfrak{B}_s$ under γ, that is: $\mathfrak{B}_{ex} := \gamma\,\mathfrak{B}_s := \{w|\ \exists\, x \in \mathfrak{B}_s :\ w(t) = \gamma(x(t))\ \forall\, t \in \mathbb{N}_0\}$. P_{ex} is said to be a *realization* of a system $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$ if $\mathfrak{B} = \mathfrak{B}_{ex}$. □

The interpretation of the external behaviour and the readout-map is slightly different from the typical behavioural point of view: the state machines discussed in this paper are either known by definition or constructed from known quantities. Hence the state variable itself is 'external' and therefore not seen as 'auxiliary' or 'latent'. Within this framework, the readout-map serves only as an instrument to put the focus on certain aspects of the state variable. It may even happen, that the state covers aspects with input characteristics, hence the read*out*-map may be defined to put the focus on *in*puts.

The state system Σ_s is said to be state *trim* if for all $\xi \in X$ there exist an $x \in \mathfrak{B}_s$ and a $t \in \mathbb{N}_0$ such that $x(t) = \xi$; see [10], page 270. Let $P = (X, \delta)$ be a state machine with induced state system Σ_s. Then P is said to be trim whenever Σ_s is trim. Since in our framework the initial state is not restricted by P itself, state trimness is equivalent to P being temporally nonblocking.

Henceforth, W is assumed to be a set holding a finite number $|W| \in \mathbb{N}$ of elements, while $X \subseteq \mathbb{R}^n \times D$, $|D| \in \mathbb{N}$. This implies that we focus on hybrid state systems with discrete external behaviour. Note that both the state behaviour $\mathfrak{B}_s$ and the external behaviour $\mathfrak{B}_{ex}$ are time invariant. $\mathfrak{B}_s$ is 1-complete, whereas $\mathfrak{B}_{ex}$ is not guaranteed to be l-complete for any $l \in \mathbb{N}$. As an example, take the widely discussed switched-server systems (see e. g. [2]), which do not exhibit a complete external behaviour when the discrete portion of the state serves as external signal.

l-COMPLETE APPROXIMATIONS

The construction of an l-complete superset $\mathfrak{B}_l$ of $\mathfrak{B}_{ex}$ as an approximation is done in terms of sets of states compatible with certain finite strings of external signals.

Definition 5. Let $P_{ex} = (X, W, \delta, \gamma)$ be a trim state machine with induced state behaviour $\mathfrak{B}_s$. By $\mathcal{X}(\bar{w}|_{[0,l]}) \subseteq X$ we denote the set of all states that are compatible with the sequence of external signals $\bar{w}|_{[0,l]} \in W^{l+1}$ at time $l \in \mathbb{N}_0$:

$$\mathcal{X}(\bar{w}\big|_{[0,l]}) := \{\xi|\ \exists\, x \in \mathfrak{B}_s :\ x(l) = \xi,\ \gamma\, x\big|_{[0,l]} = \bar{w}\big|_{[0,l]}\}\,. \qquad (2)$$

□

The sets of compatible states can be obtained by a recursive formula, given in the following proposition.

Proposition 1. For any trim state machine $P_{ex} = (X, W, \delta, \gamma)$ with induced state behaviour $\mathfrak{B}_s$ and any trajectory $\bar{w} \in W^{\mathbb{N}_0}$, the following equations hold:

$$\mathcal{X}(\bar{w}\big|_{[0,0]}) = \{\xi|\ \xi \in X,\ \gamma(\xi) = \bar{w}(0)\} = \gamma^{-1}\, w(0)\,, \qquad (3)$$

$$\mathcal{X}(\bar{w}\big|_{[0,l+1]}) = \{\xi|\ \exists\, \xi^- \in \mathcal{X}(\bar{w}\big|_{[0,l]}) :\ (\xi^-, \xi) \in \delta,\ \gamma(\xi) = \bar{w}(l{+}1)\}\,. \qquad (4)$$

Proof. It is obvious that any ξ in one of the left hand side sets in (3) or (4) satisfies the conditions stated on the respective right hand side. Hence the left hand side sets are subsets of those right hand side. To show the converse, pick any ξ from the right hand side set of equation (3). State trimness implies that there exist trajectories $x \in \mathfrak{B}_s$, $x(0) = \xi$. Hence $\xi \in \mathcal{X}(\bar{w}|_{[0,0]})$, implying equation (3). Now, pick any ξ from the right hand side set in equation (4). As $\xi^- \in \mathcal{X}(\bar{w}|_{[0,l]})$, we know a trajectory $x^- \in \mathfrak{B}_s$ to exist such that $\gamma\, x^-|_{[0,l]} = \bar{w}|_{[0,l]}$ and $x^-(l) = \xi^-$. Again state trimness implies a trajectory $x^+ \in \mathfrak{B}_s$, $x^+(0) = \xi$, to exist. Now let $x(t) := x^-(t)$ for all $t \le l$ and $x(t) := x^+(t - l - 1)$ for all $t > l$. Observe that $x \in \mathfrak{B}_s$, $x(l+1) = \xi$ and $\gamma\, x|_{[0,l+1]} = \bar{w}|_{[0,l+1]}$. This implies $\xi \in \mathcal{X}(\bar{w}|_{[0,l+1]})$, hence Equation (4) has been shown. □

By equation (4), $\mathcal{X}(\bar{w}|_{[0,l+1]})$ can be seen as the intersection of the set of all states which are reachable from $\mathcal{X}(\bar{w}|_{[0,l]})$ within one time step and the inverse image of $\bar{w}(l)$ under γ. This operation can be performed exactly for certain classes of hybrid systems, e. g. linear hybrid automata. However, for more general hybrid systems, it is hardly possible to explicitly characterize the set of states reachable in one time step. In these cases, a common approach is to compute an approximation, where the particular approximation technique depends on δ. In the following, this is formalized by a map $E\colon 2^X \to 2^X$, where 2^X denotes the set of all subsets of X. Hence, $E(X')$ represents the approximation of the subset $X' \subseteq X$. In the sequel, E is referred to as a *monotone conservative approximation scheme* if $X' \subseteq E(X') \subseteq E(X'')$ holds for all $X' \subseteq X'' \subseteq X$.

Definition 6. Let $P_{ex} = (X, W, \delta, \gamma)$ denote a trim state machine with external signals. Let $E\colon 2^X \to 2^X$ be a conservative monotone approximation scheme. Then, the estimate $\mathcal{E}(\bar{w}|_{[0,l]}) \subseteq X$ of the set of states that are compatible with $\bar{w} \in W^{\mathbb{N}_0}$ at time l is defined by:

$$\mathcal{E}(\bar{w}\big|_{[0,0]}) := E(\mathcal{X}(\bar{w}\big|_{[0,0]}))\,, \qquad (5)$$

$$\mathcal{E}(\bar{w}\big|_{[0,l+1]}) := E(\{\xi|\ \exists\, \xi^- \in \mathcal{E}(\bar{w}\big|_{[0,l]}) :\ (\xi^-, \xi) \in \delta,\ \gamma(\xi) = \bar{w}(l{+}1)\}) \qquad (6)$$

□

Indeed $\mathcal{E}(\bar{w}|_{[0,l]})$ turns out to be a conservative estimate of $\mathcal{X}(\bar{w}|_{[0,l]})$:

Proposition 2. In the above notation $\mathcal{E}(\bar{w}|_{[0,l]}) \supseteq \mathcal{X}(\bar{w}|_{[0,l]})$ holds for all $l \in \mathbb{N}_0$ and all $\bar{w} \in W^{\mathbb{N}_0}$.

Proof. The prove is done by induction. The claim clearly holds when $l = 0$. Now assume $\mathcal{E}(\bar{w}|_{[0,l]}) \supseteq \mathcal{X}(\bar{w}|_{[0,l]})$ to hold for some fixed $l \in \mathbb{N}_0$. From E being monotone and from equations (6) and (4) it follows $\mathcal{E}(\bar{w}|_{[0,l+1]}) \supseteq E(\mathcal{X}(\bar{w}|_{[0,l+1]}))$, hence $\mathcal{E}(\bar{w}|_{[0,l+1]}) \supseteq \mathcal{X}(\bar{w}|_{[0,l+1]})$. □

As an immediate consequence it can be observed that $\bar{w}|_{[0,l]} \in \mathfrak{B}_{ex}$ implies $\mathcal{E}(\bar{w}|_{[0,l]}) \neq \emptyset$, where $\mathfrak{B}_{ex}$ is the external behaviour of the discussed state machine P_{ex}:

Theorem 1. Let $P_{ex} = (X, W, \delta, \gamma)$ denote a trim state machine with induced state behaviour $\mathfrak{B}_s$ and external behaviour $\mathfrak{B}_{ex}$. Let $E\colon 2^X \to 2^X$ be a conservative monotone approximation scheme, leading to estimates $\mathcal{E}(\,\cdot\,)$ of compatible states. For $l \in \mathbb{N}_0$ define

$$\mathfrak{B}_l := \{w |\, \mathcal{E}(w\big|_{[t,t+l]}) \neq \emptyset \;\forall\; t \in \mathbb{N}_0\}\;. \tag{7}$$

Then the following holds for all $l \in \mathbb{N}_0$:

(i) $\mathfrak{B}_l$ is l-complete.

(ii) $\mathfrak{B}_l \supseteq \mathfrak{B}_{ex}$.

(iii) $\mathfrak{B}_l \supseteq \mathfrak{B}_{l+1}$.

Proof. From equation (7), (i) follows immediately. To prove (ii), choose any $w \in \mathfrak{B}_{ex}$. Hence there exists an $x \in \mathfrak{B}_s$ such that $\gamma\, x = w$ and therefore $\mathcal{X}(w\big|_{[t,t+l]}) \neq \emptyset$ for all $t \in \mathbb{N}_0$. Now, Proposition 2 yields $w \in \mathfrak{B}_l$. To prove (iii), choose any $w \in \mathfrak{B}_{l+1}$. Then, $\mathcal{E}(w\big|_{[t,t+l+1]}) \neq \emptyset$ holds for all $t \in \mathbb{N}_0$. This implies by Definition 6, equation (6), that $\mathcal{E}(w\big|_{[t,t+l]}) \neq \emptyset$ for all $t \in \mathbb{N}_0$ and therefore $w \in \mathfrak{B}_l$. □

The system $\Sigma_l := (\mathbb{N}_0, W, \mathfrak{B}_l)$ is called an *l-complete approximation* of the system $\Sigma_{ex} := (\mathbb{N}_0, W, \mathfrak{B}_{ex})$. If E is the identity mapping (i. e. the sets of compatible states can be computed exactly), the approximation $\mathfrak{B}_l$ is essentially equivalent to the "discrete abstraction A_{l+1}" defined in [7], to the "abstraction A_l" in [8], or to the "condensed model of order l" in [5]. In this case the behaviour $\mathfrak{B}_l$ becomes the smallest l-complete superset of $\mathfrak{B}_{ex}$, and is therefore referred to as the *strongest l-complete approximation* of Σ_{ex}.

In order to construct a realization of Σ_l, we set up a suitable state space Z_l and a next state relation δ_l. The procedure is based on memorizing the last $l+1$ external signals $(w(t-l), \ldots\ w(t))$ as state $z(t) \in Z$ at time $t \geq l$, similar to [9], section 2.4.9. Since our time axis is $\mathbb{N}_0$ we need to take into account the effect of shorter strings for $t < l$.

$$Z_l := \bigcup_{1 \leq r \leq l+1} W^r\;. \tag{8}$$

The next state relation is given by:

$$\delta_l := \bigcup_{0 \leq r \leq l} \delta_l^r \subseteq Z_l \times Z_l\;, \tag{9}$$

where

$$\begin{aligned}\delta_l^r := \{&((w_0, \ldots\ w_r),\ (w_0, \ldots\ w_{r+1}))| \\ &\mathcal{E}(w_0, \ldots\ w_{r+1}) \neq \emptyset\}\;,\ 0 \leq r < l,\end{aligned} \tag{10}$$

$$\begin{aligned}\delta_l^l := \{&((w_0, \ldots\ w_l),\ (w_1, \ldots\ w_{l+1}))| \\ &\mathcal{E}(w_1, \ldots\ w_{l+1}) \neq \emptyset\}\;.\end{aligned} \tag{11}$$

As external signal we select the very right entry of the state:

$$\gamma_l(z) := w_r \quad \forall\; r \leq l,\ z = (w_0, \ldots\ w_r) \in W^r\;. \tag{12}$$

This defines a state machine with external signals

$$P_l := (Z_l,\, W,\, \delta_l,\, \gamma_l) \tag{13}$$

to be a realization of Σ_l:

Theorem 2. Let $\mathfrak{B}_{ex}$ denote an external behaviour of a trim state machine. Let $\mathfrak{B}_l$ be an l-complete approximation of $\Sigma_{ex} = (\mathbb{N}_0,\, W,\, \mathfrak{B}_{ex})$, as defined in Theorem 1, eq. (7). Then, $\mathfrak{B}_l$ is realized by the *finite* state machine $P_l := (Z_l,\, W,\, \delta_l,\, \gamma_l)$, defined by equations (8) – (13).

Proof. Let $\mathfrak{B}_{s,l}$ denote the state behaviour induced by P_l and $\mathfrak{B}_{ex,l}$ the corresponding external behaviour. We need to show $\mathfrak{B}_l = \mathfrak{B}_{ex,l}$. Choose an arbitrary but fixed $w \in W^{\mathbb{N}_0}$ and let

$$z(t) := \begin{cases} (w(0), \ldots, w(t)) \text{ if } 0 \leq t < l, \\ (w(t-l), \ldots, w(t)) \text{ if } t \geq l. \end{cases} \tag{14}$$

In order to prove $w \in \mathfrak{B}_{ex,l} \Leftrightarrow w \in \mathfrak{B}_l$ we first assume $w \in \mathfrak{B}_{ex,l}$. Hence there must exist a $z' \in \mathfrak{B}_{s,l}$ such that $\gamma\, z' = w$. From the definition of δ_l it follows by induction that $z(t) = z'(t)$ for all $t \geq l$ and therefore $(z(t),\ z(t+1)) \in \delta_l$ for all $t \geq l$. Furthermore, the definition of δ_l implies $\mathcal{E}(z(t)) \neq \emptyset$ for all $t \geq l$. By equation (14), $w|_{[t-l,t]} = z(t)$; hence $\mathcal{E}(w|_{[t-l,t]}) \neq \emptyset$ for all $t \geq l$ and therefore $w \in \mathfrak{B}_l$. We now assume $w \in \mathfrak{B}_l$. It is obvious that $(z(t),\ z(t+1)) \in \delta_l$ for all $t \in \mathbb{N}_0$. Hence $z \in \mathfrak{B}_{s,l}$ and therefore $w \in \mathfrak{B}_{ex,l}$. □

ESTIMATES OF REACHABLE STATES

The computation of the set $\mathcal{R} := \mathcal{R}(\Sigma_s,\ X_0)$ of states reachable from a certain set of initial states X_0 is a crucial point whenever specifications are subject to verification: if the specifications require that the system state remains within X_{spec}, one has to figure out, whether $\mathcal{R}$ is a subset of X_{spec}.

Definition 7. Let $\Sigma_s = (\mathbb{N}_0,\ X,\ \mathfrak{B}_s)$ be a state space system. A state $\xi_1 \in X$ is *reachable from a state* $\xi_0 \in X$, if there exists a trajectory $x \in \mathfrak{B}_s$, such that $x(0) = \xi_0,\ x(t) = \xi_1$ for some $t \in \mathbb{N}_0$. ξ_1 is *reachable from the set of initial states* $X_0 \subseteq X$, if it is reachable from some state $\xi_0 \in X_0$. The set of all states reachable from X_0 is denoted by $\mathcal{R}(\Sigma_s,\ X_0) := \{\xi_1 |\ \exists\, \xi_0 \in X_0 :\ \xi_1 \text{ is reachable from } \xi_0\}$. □

When state trimness is assumed, a state ξ_1 is reachable from ξ_0 if and only if there exists a finite sequence of transitions from δ connecting ξ_0 with ξ_1. This corresponds to the standard definition of reachability within the state machine framework.

Since the realization P_l of an l-complete approximation $\mathfrak{B}_l$ is a finite state machine, the set of states $\mathcal{R}(\Sigma_{s,l},\ W_0)$ reachable from $W_0 \subseteq W \subseteq Z_l$ can be computed by standard methods. From the approximation property of $\mathfrak{B}_l$ one then obtains an estimate of reachable states for the original system Σ_s.

Theorem 3. Let $P_{ex} = (X, W, \delta, \gamma)$ denote a trim state machine with induced state space system $\Sigma_s = (\mathbb{N}_0,\ X,\ \mathfrak{B}_s)$ and external behaviour $\mathfrak{B}_{ex}$. Let $P_l = (Z_l,\ W,\ \delta_l,\ \gamma_l)$ denote the realization of an l-complete approximation $\Sigma_l = (\mathbb{N}_0,\ W,\ \mathfrak{B}_l)$ as derived in the previous section. For a given subset $X_0 \subseteq X$ of initial states let $W_0 := \gamma\ X_0 \subseteq W \subseteq Z_l$. Then the following holds:

$$\mathcal{E}(\mathcal{R}(\Sigma_{s,l},\ W_0)) \supseteq \mathcal{R}(\Sigma_s,\ X_0)\;, \tag{15}$$

$$\gamma_l\, \mathcal{R}(\Sigma_{s,l},\ W_0) \supseteq \gamma\, \mathcal{R}(\Sigma_s,\ X_0)\;. \tag{16}$$

Proof. In order to show equation (15) choose any $\xi_1 \in \mathcal{R}(\Sigma_s,\, X_0)$. Then there exists a trajectory $x \in \mathfrak{B}_s$, $x(0) \in X_0$, $x(t) = \xi_1$ for some $t \in \mathbb{N}_0$. Let $w := \gamma x$ yielding $x \in \mathfrak{B}_{ex}$ and therefore $w \in \mathfrak{B}_l$. From the definition of W_0 observe $w(0) \in W_0$. Let z be defined as in equation (14), implying $z \in \mathfrak{B}_{s,l}$, $\gamma_l\, z = w$, $z(0) = w(0) \in W_0$, $z(t) \in \mathcal{R}(\Sigma_{s,l},\, W_0)$. Finally let $r := \min\{l, t\}$ and observe $z(t) = (w(t-r), \ldots w(t))$. From the definition of compatible states $\xi_1 \in \mathcal{E}(z(t))$ holds, hence $\xi_1 \in \mathcal{E}(\mathcal{R}(\Sigma_{s,l},\, W_0))$. This completes the proof of equation (15). We now show equation (16). Choose any $\omega_1 \in \gamma\ \mathcal{R}(\Sigma_s,\, X_0)$. Then there exists a trajectory $x \in \mathfrak{B}_s$, $x(0) \in X_0$, $\gamma\ x(t) = \omega_1$ for some $t \in \mathbb{N}_0$. As above, let $w := \gamma x$ and z as in (14). Hence $z(t) \in \mathcal{R}(\Sigma_{s,l},\, W_0)$. From $\gamma_l\ z(t) = w(t) = \gamma\ x(t) = \omega_1$, equation (16) follows. □

From Theorem 1 the approximation $\mathfrak{B}_l$ of $\mathfrak{B}_{ex}$ is expected to improve when l is increased. This result carries over to the estimate $\mathcal{E}(\mathcal{R}(\Sigma_{s,l},\, W_0))$ of reachable states.

Theorem 4. Let E denote a conservative monotone approximation scheme and P_{ex} a trim state machine with induced state space system Σ_s. Further, let $\Sigma_l,\ \Sigma_{s,l},\ P_l$ denote l-complete approximations of Σ_s based on E and realizations of those respectively. Then

$$\mathcal{E}(\mathcal{R}(\Sigma_{s,l},\, W_0)) \supseteq \mathcal{E}(\mathcal{R}(\Sigma_{s,l+1},\, W_0)) \tag{17}$$

holds for any subset $W_0 \subseteq W \subseteq Z_l$ and any $l \in \mathbb{N}$.

Proof. Choose an $\xi_1 \in \mathcal{E}(\mathcal{R}(\Sigma_{s,l+1},\, W_0))$. Then there exists a trajectory $z' \in \mathfrak{B}_{s,l+1}$ such that $z'(0) \in W_0$ and $\xi_1 \in \mathcal{E}(z'(t))$ for some $t \in \mathbb{N}_0$. Let $w := \gamma_{l+1}\ z'$. From the definition of δ_{l+1} in equations (9)–(11) and from $z' \in \mathfrak{B}_{s,l+1}$, it follows that $\mathcal{E}(z'(\tau)) \neq \emptyset$ for all $\tau \in \mathbb{N}_0$. Define $z\colon \mathbb{N}_0 \to Z_l$ as in equation (14). From $z'(0) \in W(0)$ observe

$$z'(t) := \begin{cases} (w(0), \ldots, w(t)) \text{ if } 0 \leq t < l+1, \\ (w(t-l-1), \ldots, w(t)) \text{ if } t \geq l+1. \end{cases} \tag{18}$$

By equation (6) this implies $\mathcal{E}(z(\tau)) \neq \emptyset$ for all $\tau \in \mathbb{N}_0$, hence $z \in \mathfrak{B}_{s,l}$. Two cases are distinguished. First, if $t \leq l$ then $z(t) = z'(t)$ holds, hence $\xi_1 \in \mathcal{E}(z(t))$ and therefore $\xi_1 \in \mathcal{E}(\mathcal{R}(\Sigma_{s,l},\, W_0))$. Second, if $t > l$ then $z(t) = (w(t-l), \ldots, w(t))$. From $\mathcal{E}(w|_{[t-l,l]}) \supseteq \mathcal{E}(w|_{[t-l-1,l]})$ it again follows that $\xi_1 \in \mathcal{E}(\mathcal{R}(\Sigma_{s,l},\, W_0)$. □

In other words: we can generate a conservative estimate $\mathcal{E}(\mathcal{R}(\Sigma_{s,l},\, W_0)$ for the unknown set $\mathcal{R}(\Sigma_s,\, X_0)$ from the finite state machine P_l. If we replace P_l by P_m, $m > l$, the estimate can be expected to improve, and is guaranteed not to deteriorate.

EXAMPLE

We consider a hybrid switched-server system consisting of three plates and a radiator, as described in [3]. The radiator can either be switched off or on, heating a single plate depending on its position. The switching strategy proposed in [3] is applied to keep the temperatures of all plates in a specified range.

The following parameters are assumed to be known: the radiator and the environment temperatures $\nu_r \in \mathbb{R}$ and $\nu_e \in \mathbb{R}$ respectively; the corresponding normalized heat transfer coefficients $\alpha_r,\ \alpha_e \in \mathbb{R}^+$; the specified range of allowed temperatures $[\nu_-,\, \nu_+] \subset \mathbb{R}$; it is assumed that the initial temperatures lie within $(\nu_0, \nu_+) \subset \mathbb{R}$. A temperature of a plate, v, is modelled either by eq. (19) when it is heated or by eq. (20) when it is not heated:

$$\dot{v} = \alpha_r\ (\nu_r - v) + \alpha_e\ (\nu_e - v)\,, \tag{19}$$

$$\dot{v} = 2\ \alpha_e\ (\nu_e - v)\,. \tag{20}$$

Observe $v \equiv \nu_m := (\alpha_r\ \ \nu_r + \alpha_e\ \ \nu_e)/(\alpha_r + \alpha_e)$ to be a stable equilibrium for a heated plate, and $v \equiv \nu_e$ for one which is not heated. We assume parameter values such that $\nu_e < \nu_- < \nu_0 < \nu_+ < \nu_m$ holds.

Whenever a plate temperature equals either ν_0 or ν_+, an event is generated. In response to such an event, a controller may change the control input (i. e. change the radiator position, switch the radiator on or off). In particular, our controller is a Boolean switching table realizing the following rule base:

(i) Once the reheating process of a plate has been started, it will be continued until the plate temperature reaches ν_+, but not any longer.

(ii) If at least one plate temperature is below ν_0 *and* if no other plate is being heated, the radiator is positioned at the plate with the lowest temperature, starting a reheating process.

(iii) No reheating process will be started as long as all temperatures are above ν_0

In order to obtain a discrete time axis, we consider the closed system at those moments where the control input is changed. As hybrid state variable we choose the pair $(c,\, d)$ where: $c \in \mathbb{R}^3$ represents the plate temperatures in ascending order; $d = d_{on}$ when the radiator is going to reheat the plate with the lowest temperature; $d = d_{off}$ when the radiator is switched off. Note, that by (i) and (iii) the plate temperatures are guaranteed not to exceed ν_+. This leads to the hybrid state space

$$\begin{aligned} X :=& \{c|\ c \in \mathbb{R}^3,\, \nu_e \leq c^{(1)} \leq c^{(2)} \leq c^{(3)} \leq \nu_+\} \\ & \times \{d_{on},\, d_{off}\}\,. \end{aligned} \tag{21}$$

We define $h(v_1,\ v_2)$ as an abbreviation for the following scenario: a plate is reheated from temperature v_2 up to ν_+. Meanwhile some other plate will cool down from v_1 to $h(v_1,\ v_2)$. Analogous we define $g(v_1,\ v_2)$: while a plate cools down from v_2 to ν_0, some other plate will cool down from v_1 to $g(v_1,\ v_2)$. Solving the above ODEs it can be seen that

$$h(v_1,\ v_2) = \nu_e + (v_1 - \nu_e)\left(\frac{\nu_m - \nu_+}{\nu_m - v_2}\right)^{\frac{2\ \alpha_e}{\alpha_e + \alpha_r}}\,, \tag{22}$$

$$g(v_1,\ v_2) = \nu_e + (v_1 - \nu_e)\frac{\nu_0 - \nu_e}{v_2 - \nu_e}\,. \tag{23}$$

The next state relation of the closed loop is then given by $\delta := \{((c,d),\ (c^+,d^+))|\ F(c,d) = (c^+,d^+)\}$ where

$$F(c, d_{off}) := ((\nu_0,\ g(c^{(2)}, c^{(1)}),\ g(c^{(3)}, c^{(1)})),\ d_{on}) \tag{24}$$

and, if $h(c^{(2)}, c^{(1)}) \leq \nu_0$,

$$F(c, d_{on}) := ((h(c^{(2)}, c^{(1)}),\ h(c^{(3)}, c^{(1)}),\ \nu_+),\ d_{on}) \tag{25}$$

or else

$$F(c, d_{on}) := ((h(c^{(2)}, c^{(1)}),\ h(c^{(3)}, c^{(1)}),\ \nu_+),\ d_{off})\,. \tag{26}$$

As readout map we choose $\gamma\colon X \to W := \{\gamma_{id},\, \gamma_{op}\}$ defined by $\gamma(c,\, d) := \gamma_{id}$ if $c(1) > \nu_0,\ d = d_{off}$ and $\gamma(c,\, d) := \gamma_{op}$ else. The hybrid states in $X_0 := \gamma^{-1}(\gamma_{id})$ are exactly those where all temperatures are above ν_0 and the radiator is switched off.

We now define a monotone conservative approximation scheme E. For this purpose, we introduce operators representing lower bounds of subsets $X' \subset X$ w. r. t. a given discrete component. For any $\beta_{off},\ \beta_{on} \in \mathbb{R}^3 \cup \{\infty\},\ X' \subset X$ let

$$b_{off}(X') := \inf\{c |\ (c,\, d_{off}) \in X'\} \in \mathbb{R}^3 \cup \{\infty\}\ , \quad (27)$$

$$b_{on}(X') := \inf\{c |\ (c,\, d_{on}) \in X'\} \in \mathbb{R}^3 \cup \{\infty\}\ , \quad (28)$$

$$A(\beta_{off},\, \beta_{on}) := (\{(c,\, d_{off}) |\ c \geq \beta_{off}\} \cup \{(c,\, d_{on}) |\ c \geq \beta_{on}\}) \cap X\ , \quad (29)$$

$$E(X') := A(b_{off}(X'),\, b_{on}(X'))\ . \quad (30)$$

Hence, the approximation $E(X')$ is represented by the two vectors $b_{off}(X')$ and $b_{on}(X')$, containing the lower bounds of the continuous components for each of the two possible values of the discrete component. In the above equations, the infimum and the greater or equal relation are componentwise. Furthermore, the infimum of an empty set is considered as ∞.

As the estimate of states compatible with strings of external signals consisting of one single symbol only, we obtaine by Definition 6, eq. (5):

$$\mathcal{E}(\gamma_{id}) = A((\nu_0,\, \nu_0,\, \nu_0),\, \infty)\ , \quad (31)$$

$$\mathcal{E}(\gamma_{op}) = A((\nu_e,\, \nu_e,\, \nu_e),\, (\nu_e,\, \nu_e,\, \nu_e)) = X\ . \quad (32)$$

Let $\bar{w} \in W^{\mathbb{N}_0}$, $l \in \mathbb{N}$, $\beta_{off} := b_{off}(\mathcal{E}(\bar{w}|_{[0,l]}))$ and $\beta_{on} := b_{on}(\mathcal{E}(\bar{w}|_{[0,l]}))$. Define β^+_{off} and β^+_{on} according to eq. (6):

(i) If $\bar{w}(l+1) = \gamma_{id}$:
Let $\beta^+_{on} := \infty$. If $\beta_{on} = \infty$ then let $\beta^+_{off} := \infty$; else let

$$\beta^+_{off} := (\max(\nu_0,\, h(\beta^{(2)}_{on}, \beta^{(1)}_{on})),\ \max(\nu_0,\, h(\beta^{(3)}_{on}, \beta^{(1)}_{on})),\, \nu_+)\ . \quad (33)$$

(ii) If $\bar{w}(l+1) = \gamma_{op}$:
Let $\beta^+_{off} := \infty$. If $\beta_{off} = \infty$ and $h(\beta^{(2)}_{on}, \beta^{(1)}_{on}) > \nu_0$ then let $\beta^+_{on} := \infty$; else let

$$\beta^+_{on} := (\min(\nu_0,\, h(\beta^{(2)}_{on}, \beta^{(1)}_{on})),\ \min(g(\beta^{(2)}_{off}, \beta^{(1)}_{off}),\, h(\beta^{(3)}_{on}, \beta^{(1)}_{on})),\ \min(g(\beta^{(3)}_{off}, \beta^{(1)}_{off}),\, \nu_+))\ . \quad (34)$$

Then $\mathcal{E}(\bar{w}|_{[0,l+1]}) = A(\beta^+_{off},\, \beta^+_{on})$ holds, hence the estimates of compatible states can be computed by the above formulas. Starting at $Z_0 = \{\gamma_{id}\}$ the reachable states $\mathcal{R}(\Sigma_{s,l},\, Z_0)$ can be established by iteratively appending signals from W. If a string, after appending, has length $l+2$ the leftmost signal is to be discarded. Strings $z \in Z_l$ with $b_{off}(\mathcal{E}(z)) = b_{on}(\mathcal{E}(z)) = \infty$ are to be ignored when proceeding. In case this happens to all newly generated strings the procedure terminates and all reachable states have been found. By Theorem 3, the minimum temperature which can occur for an initial state in X_0 is guaranteed to be above the smallest first entry of the lower bounds $b_{on}(\,\cdot\,)$ and $b_{off}(\,\cdot\,)$ computed by the above procedure.

Numerical results are given in the table below, where the parameter values $\nu_e = 0.1$, $\nu_0 = 0.8$, $\nu_+ = 1.0$, $\nu_- = 0.5$, $\nu_r \in \{2.0,\, 2.5,\, 3.0\}$, $\alpha_e = 0.5$, and $\alpha_r = 1$ are assumed. Verification goes through positively for $\nu_r = 2.5$ and $\nu_r = 3.0$ at $l = 6$ and $l = 5$ respectively. In the case $\nu_r = 2.0$ no verification based on l-complete approximations for $l \leq 20$ is possible. However, when $\nu_r = 2.0$, it can be seen from simulation that a plate temperature indeed is below the specified minimum $\nu_- = 0.5$.

Guaranteed lower bounds on the plate temperatures						
ν_r	$l \leq 3$	$l = 4$	$l = 5$	$l = 6$	$l = 10$	$l = 20$
2.0	0.10	0.27	0.29	0.31	0.32	0.32
2.5	0.10	0.40	0.44	0.50	0.56	0.56
3.0	0.10	0.49	0.55	0.63	0.63	0.63

CONCLUSIONS

We have proposed a general framework for computing reliable estimates of sets of reachable states. The estimates are guaranteed to form a (not necessarily strictly) decreasing sequence of *supersets* of the exact solution. While the sequence is not guaranteed to converge to the true solution, we have the benefit of the superset property; this allows us to perform verification based on any set from the sequence generated by the proposed method: if any of the sets $\mathcal{R}_l := \mathcal{E}(\mathcal{R}(\Sigma_{s,l},\, Z_0))$ is a subset of the specification set X_{spec}, the state of the underlying hybrid system is guaranteed to remain within X_{spec}. Note, that this is not a contradiction to the semidecidability property stated in [1], since it is possible that $\mathcal{R}(\Sigma_s,\, X_0) \subseteq X_{spec}$ while $\mathcal{R}_l \not\subseteq X_{spec}$ for all $l \in \mathbb{N}$.

REFERENCES

[1] Alur, R., Courcoubetis, C., Henzinger, T. A., Ho, P.-H.: "Hybrid automata: an algorithmic approach to the specification and verification of hybrid systems", in Grossman R. L., Nerode, A., Ravn, A. P., Rischel, H. (Eds.): *Hybrid systems*, LNCS 736, pp. 209-229, Springer, Berlin, 1993.

[2] Chase, C., Serano, J., Ramadge P.: "Periodicity and chaos from switched flow systems: Contrasting examples of discretely controlled continuous systems", *IEEE Transactions on Automatic Control*, Vol. 38, no. 1, pp. 70-83, 1993.

[3] Franke, D., Moor, T.: "Combined rule- and model-based design of a hybrid thermal process", *Proc. CESA98*, pp. 630-634, Nabeul-Hammamet, Tunesia, 1998.

[4] Henzinger, T. A., Ho, P.-H.: "A note on abstract interpretation strategies for hybrid automata", in Antsaklis, P., Kohn, W., Nerode, A., Sastry, S. (Eds.): *Hybrid systems II*, LNCS 999, pp. 252-264, Springer, Berlin, 1995.

[5] Moor, T.: "Event driven control of switched-integrator-systems", *Proc. ADPM98*, pp. 271-277, Reims, 1998.

[6] Moor, T., Raisch, J., O'Young, S. D.: "Supervisory control of hybrid systems via l-complete approximations", *Proc. WODES98*, 1998.

[7] Raisch, J., O'Young, S. D.: "A totally ordered set of discrete abstractions for a given hybrid or continuous system", in Antsaklis, P., Kohn, W., Nerode, A., Sastry, S. (Eds.): *Hybrid Systems IV*, LNCS 1273, pp. 342-360, 1997.

[8] Raisch, J.: "A hierarchy of discrete abstractions for a given hybrid plant", *Proc. ADPM98*, pp. 55-62, Reims, 1998.

[9] Willems, J.C.: "Models for dynamics", *Dynamics Reported*, Vol. 2, pp. 172-269, 1989.

[10] Willems, J.C.: "Paradigms and puzzles in the theory of dynamic systems", *IEEE Transactions on Automatic Control*, Vol. 36, No. 3, pp. 258-294, 1991.