ELSEVIER

Systems & Control Letters 38 (1999) 157–166

SYSTEMS & CONTROL LETTERS

www.elsevier.com/locate/sysconle

Supervisory control of hybrid systems within a behavioural framework

T. Moor[a,*], J. Raisch[b]

[a] *Fachbereich Elektrotechnik, Universität der Bundeswehr Hamburg, D-22769 Hamburg, Germany*
[b] *Max-Planck-Institut für Dynamik komplexer technischer Systeme, D-39120 Magdeburg, Germany*

Abstract

This contribution addresses the synthesis of supervisory control for hybrid systems Σ with discrete external signals. Such systems are in general neither l-complete nor can they be represented by finite state machines. We find an l-complete approximation (abstraction) Σ_l for Σ, represent it by a finite state machine, and investigate the control problem for the approximation. If a solution exists, we synthesize the maximally permissive supervisor for Σ_l. We show that it also solves the control problem for the hybrid system Σ. If no solution exists, approximation accuracy can be increased by computing a k-complete abstraction Σ_k, $k > l$. This paper is entirely set within the framework on *Willems*' behavioural systems theory.

Keywords: Hybrid systems; Supervisory control; Behavioural approach; l-complete approximations

1. Introduction

The topic of this paper is supervisory control of time-invariant hybrid systems with discrete external (input and output) signals. In general, the external behaviour of such a system can not be represented by a finite state machine. To be able to apply supervisory control synthesis techniques, we therefore introduce the strongest l-complete approximation as a discrete abstraction for the hybrid system. This l-complete approximation can be represented by a finite state machine. Similar to the procedure described in [19, Section 2.4.9], we choose a particularly simple state representation. Therefore, we can explicitly characterize the state evolution law of the approximation in terms of the underlying hybrid system.

In a second step, we apply a slightly modified version of *Ramadge*'s and *Wonham*'s supervisory control theory [16,17] and check whether the control problem can be solved for the discrete abstraction: we ask whether the (l-complete) approximation behaviour can be restricted to a set of "acceptable" trajectories or, in other words, be forced to "obey the specifications". If this is the case, the least restrictive suitable supervisor is determined. It is shown that this supervisor also restricts the external behaviour of the hybrid system in the desired fashion.

This paper is based on a previous workshop contribution by the authors [11]. In contrast to [11], however, not only the approximation step but also the supervisor synthesis method is treated within the framework of *Willems*' behavioural systems theory. In order to apply our method to practical problems, we also interpret the major steps on the realization level.

* Corresponding author.

0167-6911/99/$ - see front matter
PII: S0167-6911(99)00061-4

Control-related issues for hybrid systems have been treated in a number of publications. In the context of the present contribution, approximation-based approaches as discussed in [5,6,8–10,15] are most relevant. Control synthesis for linear hybrid systems, a class of systems that can be treated analytically, is described in [18]. An overview of the general area of hybrid systems is given by Grossman et al. [7], Antsaklis et al. [2–4], Alur et al. [1].

This paper is organized as follows: in Section 2, we recall basic definitions of *Willems*' behavioural approach and treat state machines within this framework. In Section 3, we introduce l-complete approximations and discuss how to realize them by finite past-induced state machines. In Section 4, we apply these results to a general class of hybrid systems. Synthesis of supervisors within the behavioural framework is treated in Section 5; supervisor synthesis based on approximations is discussed in Section 6.

2. Behaviours and state machines

The purpose of this section is to collect basic facts and definitions of *Willems*' behavioural approach and to investigate state machines within this framework.

Definition 1 (*See Willems* [20, *Definition* 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 $w \notin \mathfrak{B}$ can not occur. An overview of the behavioural framework is given in [20,19]. Within this paper, focus is on systems with discrete time axis $T = \mathbb{N}_0$.

Definition 2 (*See Willems* [20, *Definition* II.4])**.** A dynamical system $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$ is said to be *complete* if

$$w \in \mathfrak{B} \;\Leftrightarrow\; w|_{[t_1,t_2]} \in \mathfrak{B}|_{[t_1,t_2]} \quad \forall t_1, t_2 \in \mathbb{N}_0. \tag{1}$$

Here, $w|_{[t_1,t_2]}$, $t_1 \leqslant t_2$, is the restriction of the map $w : \mathbb{N}_0 \to W$ to the domain $[t_1, t_2] \cap \mathbb{N}_0$. To keep notation reasonably compact $w|_{[t_1,t_2]}$ is treated as a finite string of symbols without absolute time information, i.e. we do not distinguish between $w|_{[t_1,t_2]} \in W^{|[t_1,t_2]}$ and $(w(t_1), \ldots, w(t_2)) \in W^{t_2-t_1+1}$. Furthermore, $w|_\emptyset$ is defined to be the *empty string* w^*, i.e. $w^* = w|_\emptyset$ holds for every map w.

Whenever the signal space is clear from the context, a system is uniquely determined by its behaviour: we therefore refer to a *behaviour* as being complete, if it belongs to a complete *system*. This convention is also used with respect to all properties defined in the sequel.

Throughout this paper, systems are assumed to be complete and realizable by state machines:

Definition 3. Let the sets $W, X, X_0 \subseteq X$, $\delta \subseteq X \times W \times X$ denote the external *signal space*, the *state space*, *the set of initial conditions* and the *next state relation*, respectively. The tuple $P = (X, W, \delta, X_0)$ is called a *state machine*. If $|W| \in \mathbb{N}$ and $|X| \in \mathbb{N}$ (both sets are finite), P is said to be a *finite state machine*. The behaviour $\mathfrak{B}_s := \{(w,x) | (x(t), w(t), x(t+1)) \in \delta \forall t \in \mathbb{N}_0, x(0) \in X_0\}$ is referred to as the induced *full behaviour*, and $\Sigma_s := (\mathbb{N}_0, W \times X, \mathfrak{B}_s)$ as the induced state space system. The *external behaviour* $\mathfrak{B}_{ex}$ of Σ_s is defined to be the projection of $\mathfrak{B}_s$ onto $W^{\mathbb{N}_0}$, i.e. $\mathfrak{B}_{ex} := \mathscr{P}_W \mathfrak{B}_s := \{w | \exists x: (w,x) \in \mathfrak{B}_s\}$. Vice versa, a state machine P' with induced external behaviour $\mathfrak{B}'$ is said to be a *realization* of the system $\Sigma' = (\mathbb{N}_0, W, \mathfrak{B}')$. This is denoted by $\Sigma' \cong P'$.

We now introduce some basic terminology related to state machines.

Definition 4. Let $P_a = (A, W, \alpha, A_0)$ and $P_b = (B, W, \beta, B_0)$ be state machines. *Reachability*: A state $a_1 \in A$ is said to be *reachable*, if there exists a state $a_0 \in A_0$ and a sequence of transitions (elements in the next state relation) from α connecting a_0 with a_1. The state machine P_a is said to be *reachable*, if every state $a_1 \in A$ is reachable. *Do not care symbol* "–": We use "$(a, w, -) \in \alpha$" as an abbreviation for "$(a, w, a') \in \alpha$ for some $a' \in A$"; in analogy, "$(a, w, -) \notin \alpha$" means "$(a, w, a') \notin \alpha$ for all $a' \in A$". *Nonblocking property*: The state machine P_a is called *nonblocking*, if for every reachable state $a \in A$, there exists $w \in W$ such that $(a, w, -) \in \alpha$. *Union* $P_a \cup P_b := (A \cup B, W, \alpha \cup \beta, A_0 \cup B_0)$. *Parallel composition*: $P_a \parallel P_b := (A \times B, W, \lambda, A_0 \times B_0)$, where $((a,b), w, (a',b')) \in \lambda$ if and only if $(a, w, a') \in \alpha$ and $(b, w, b') \in \beta$.

If a state machine P realizing Σ is given, we can always construct a nonblocking state machine $P', \Sigma \cong P'$, by repeatedly removing blocking states and transitions that lead into blocking states. If the state space of

P is finite, the procedure is finite, and the state space of P' is also finite.

In the behavioural framework, connecting two systems $\Sigma_a = (\mathbb{N}_0, W, \mathfrak{B}_a)$ and $\Sigma_b = (\mathbb{N}_0, W, \mathfrak{B}_b)$ amounts to intersecting their behaviours, i.e. the system $\Sigma_\cap = (\mathbb{N}_0, W, \mathfrak{B}_a \cap \mathfrak{B}_b)$ represents the situation where trajectories need to be compatible with both the phenomena modelled by Σ_a and those modelled by Σ_b. On the realization level, this corresponds to parallel composition: it is a well-known fact that $\Sigma_a \cong P_a$, $\Sigma_b \cong P_b$ implies $\Sigma_\cap \cong P_a \| P_b$. In a supervisory control scenario, connecting plant and supervisor models the closed loop.

Definition 5 (*See Willems* [19, *Section* 2.2.1])**.** Let $\mathfrak{B}_s$ be the full behaviour induced by the state machine $P = (X, W, \delta, X_0)$. Then, P is said to be *past induced*, if $t \in \mathbb{N}_0$, $(w', x'), (w'', x'') \in \mathfrak{B}_s, w'|_{[0,t)} = w''|_{[0,t)}$ implies $x'(t) = x''(t)$.

A past-induced state machine is "instantaneously state observable": for every $t \in \mathbb{N}_0$, we can figure out $x(t)$ by only investigating the past $w|_{[0,t)}$ of the external signal. Thus, past inducedness is a crucial property for control related tasks. In fact, past-induced realizations of the plant model are the scenario where *Ramadge*'s and *Wonham*'s supervisory control theory is set.

A state machine P is past induced, if and only if there exists a map $\mathfrak{p} : \bigcup_{t\in\mathbb{N}_0} \mathfrak{B}|_{[0,t)} \to X$ such that

$$(w,x) \in \mathfrak{B}_s \Leftrightarrow w \in \mathfrak{B}, \quad x \in X^{\mathbb{N}_0}, \\ x(t) = \mathfrak{p}(w|_{[0,t)}) \quad \forall t \in \mathbb{N}_0. \tag{2}$$

$\mathfrak{p}$ is referred to as the *past-induced state map*. If the state machine P is past induced and nonblocking, X_0 contains at most one element. The parallel composition of two past-induced state machines is also past induced:

Proposition 6. *Let $P_a = (A, W, \alpha, A_0)$ and $P_b = (B, W, \beta, B_0)$ be past-induced realizations of $\Sigma_a = (\mathbb{N}_0, W, \mathfrak{B}_a)$ and $\Sigma_b = (\mathbb{N}_0, W, \mathfrak{B}_b)$, respectively. Then $P_a \| P_b$ is also past induced. Let $\mathfrak{p}_a, \mathfrak{p}_b$ and $\mathfrak{p}$ denote the past-induced state maps of P_a, P_b and $P_a \| P_b$, respectively. Then $\mathfrak{p}(w|_{[0,t)}) = (\mathfrak{p}_a(w|_{[0,t)}), \mathfrak{p}_b(w|_{[0,t)}))$ holds for all $w \in \mathfrak{B}_a \cap \mathfrak{B}_b$, $t \in \mathbb{N}_0$.*

In theory, any state machine P can be converted into a past-induced state machine without affecting its external behaviour. This, however, has to be paid for by "state explosion". Therefore, even for a finite P, this procedure is in general not feasible. The approximation scheme suggested in the following section addresses this problem.

3. *l*-complete approximations

In this section, we approximate a given system Σ with finite external signal space W, $|W| \in \mathbb{N}$, by an l-complete system Σ_l. The latter can then be realized by a past-induced finite state machine.

Definition 7 (*See Willems* [20, *Definition* II.3])**.** Let σ^t be 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 a dynamical system $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$ is said to be *time invariant*, if $\sigma\mathfrak{B} \subseteq \mathfrak{B}$.

Note that systems realized by state machines with restricted initial conditions are not necessarily time invariant. However, a system is time invariant, if it is realized by a state machine $P = (X, W, \delta, X)$ (i.e. if the set of initial conditions covers the entire state space).

Definition 8 (*See Willems* [20, *Definition* 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

$$w \in \mathfrak{B} \quad \Leftrightarrow \quad \sigma^t w|_{[0,l]} \in \mathfrak{B}|_{[0,l]} \quad \forall t \in \mathbb{N}_0. \tag{3}$$

Note that shifting is defined to be of higher priority than restricting: $\sigma^t w|_{[0,l]} = (\sigma^t w)|_{[0,l]}$.

An l-complete system can be represented by a difference equation with lag l. Not all systems are l-complete, however. For a system $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$ without this property, we now propose the notion of a "strongest l-complete approximation". Roughly speaking, this is a system evolving on the same time axis $\mathbb{N}_0$ and within the same signal space W as the original system, and with the smallest l-complete behaviour that covers the "original" behaviour $\mathfrak{B}$. Formally, this can be written as:

Definition 9. Let $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$ and $\Sigma_l = (\mathbb{N}_0, W, \mathfrak{B}_l)$ be time-invariant dynamical systems, with $l \in \mathbb{N}$. Σ_l is said to be a *strongest l-complete approximation* induced by Σ if the following conditions hold:

1. $\mathfrak{B}_l \supseteq \mathfrak{B}$, $\mathfrak{B}_l$ is l-complete.
2. $\mathfrak{B}'_l \supseteq \mathfrak{B}$, $\mathfrak{B}'_l$ is l-complete $\Rightarrow \mathfrak{B}'_l \supseteq \mathfrak{B}_l$.

The motivation for Definition 9 is the following: we want to synthesize supervisory control for Σ on

the basis of the approximation Σ_l. Clearly, we need condition (1) to hold; otherwise, $\mathfrak{B}$ could contain unacceptable trajectories which could not be predicted by Σ_l and hence not be suppressed by a control strategy based on the approximation. It is also obvious that we want condition (2) to hold: the smaller $\mathfrak{B}_l$, the more accurate the approximation Σ_l, and the better the chances for a suitable supervisor to exist.

Proposition 10. *Let $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$ be a time-invariant dynamical system. Choose an arbitrary $l \in \mathbb{N}$. Then, the strongest l-complete approximation induced by Σ, denoted by $\Sigma_l = (\mathbb{N}_0, W, \mathfrak{B}_l)$, exists uniquely, and $\mathfrak{B}_l$ is given by*

$$\mathfrak{B}_l = \{w \mid w \in W^{\mathbb{N}_0},\ \sigma^t w|_{[0,l]} \in \mathfrak{B}|_{[0,l]}\ \forall t \in \mathbb{N}_0\}. \quad (4)$$

Proof. Uniqueness follows immediately from Definition 9. To prove existence, take $\mathfrak{B}_l$ as defined by Eq. (4) and check conditions (1) and (2). Σ is time invariant, hence $w \in \mathfrak{B}$ implies $\sigma^t w|_{[0,l]} \in \mathfrak{B}|_{[0,l]}$ for all $t \in \mathbb{N}_0$, and therefore $\mathfrak{B}_l \supseteq \mathfrak{B}$. l-completeness of $\mathfrak{B}_l$ is obvious, hence condition (1) holds. Now, take any l-complete $\mathfrak{B}'_l$ that satisfies $\mathfrak{B}'_l \supseteq \mathfrak{B}$. Pick any $w \in \mathfrak{B}_l$; from Eq. (4), it follows immediately that $\sigma^t w|_{[0,l]} \in \mathfrak{B}|_{[0,l]} \subseteq \mathfrak{B}'_l|_{[0,l]}$ for all $t \in \mathbb{N}_0$. $\mathfrak{B}'_l$ being l-complete implies $w \in \mathfrak{B}'_l$. Hence, $\mathfrak{B}'_l \supseteq \mathfrak{B}_l$, and existence has been proven. □

Corollary 11 is an immediate consequence of Eq. (4):

Corollary 11. *Let $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$ be a time-invariant dynamical system and $\Sigma_l = (\mathbb{N}_0, W, \mathfrak{B}_l)$ the strongest l-complete approximation. Then,*

1. $\mathfrak{B}_l|_{[0,l]} = \mathfrak{B}|_{[0,l]}$,
2. $\mathfrak{B}_l \supseteq \mathfrak{B}_{l+1} \supseteq \mathfrak{B}$,
3. $\Sigma_l = \Sigma \Leftrightarrow \Sigma$ *is l-complete.*

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 external signals $(w(t-l), \ldots, w(t-1))$ as state $z(t) \in Z_l$ at time $t \geqslant l$, similar to Willems [19, Section 2.4.9]. Since our time axis is $\mathbb{N}_0$ we need to take into account the effect of shorter strings for $t < l$:

$$Z_l := \bigcup_{0 \leqslant r \leqslant l} W^r, \qquad W^0 := \{w^*\}, \quad (5)$$

where the empty string w^* is interpreted as "no external signal present so far". The next state relation is given by

$$\delta_l := \bigcup_{0 \leqslant r \leqslant l} \delta_l^r \subseteq Z_l \times W \times Z_l, \quad (6)$$

where

$$\delta_l^0 := \{(w^*, w_0, w_0) \mid w_0 \in \mathfrak{B}|_{[0,0]}\}, \quad (7)$$

$$\delta_l^r := \{((w_0, \ldots, w_{r-1}), w_r, (w_0, \ldots, w_r)) \mid (w_0, \ldots, w_r) \in \mathfrak{B}|_{[0,r]}\}, \quad 1 \leqslant r \leqslant l, \quad (8)$$

$$\delta_l^l := \{((w_0, \ldots, w_{l-1}), w_l, (w_1, \ldots, w_l)) \mid (w_0, \ldots, w_l) \in \mathfrak{B}|_{[0,l]}\}. \quad (9)$$

Theorem 12. *Let Σ_l be the strongest l-complete approximation induced by the time-invariant dynamical system $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$, $\mathfrak{B} \neq \emptyset$. Then, Σ_l is realized by the nonblocking past-induced finite state machine $P_l := (Z_l, W, \delta_l, Z_0)$, defined by Eqs. (5)–(9).*

Proof. Let $\mathfrak{B}_{s,l}$ and $\mathfrak{B}_{\mathrm{ex},l} = \mathscr{P}_W \mathfrak{B}_{s,l}$ denote the full and the external behaviour induced by P_l. For $w \in W^{\mathbb{N}_0}$ and $t \in \mathbb{N}_0$ let

$$\mathfrak{p}(w|_{[0,t)}) := \begin{cases} w^* & \text{if } t = 0, \\ (w(0), \ldots, w(t-1)) & \text{if } 0 < t < l, \\ (w(t-l), \ldots, w(t-1)) & \text{if } t \geqslant l. \end{cases} \quad (10)$$

From the definition of δ_l it follows by induction that $(w,z) \in \mathfrak{B}_{s,l}$ if and only if $w \in \mathfrak{B}_{\mathrm{ex},l}$ and $z(t) = \mathfrak{p}(w|_{[0,t)})$ for all $t \in \mathbb{N}_0$. Hence, P_l is past induced, and $\mathfrak{p}$ serves as past-induced state map. In order to prove $\mathfrak{B}_l = \mathfrak{B}_{\mathrm{ex},l}$, we first assume $w \in \mathfrak{B}_{\mathrm{ex},l}$. Then $z(t) := \mathfrak{p}(w|_{[0,t)})$, $t \in \mathbb{N}_0$, defines a state trajectory $z \in Z_l^{\mathbb{N}_0}$ such that $(w,z) \in \mathfrak{B}_{s,l}$; hence, $(z(t), w(t)) \in \mathfrak{B}|_{[0,t]}$ for all $t \geqslant l$. From Corollary 11, part (1), and Eq. (10), it follows that $w|_{[t-l,t]} = (z(t), w(t)) \in \mathfrak{B}|_{[0,l]} = \mathfrak{B}_l|_{[0,l]}$ for all $t \geqslant l$. Since $\mathfrak{B}_l$ is l-complete, this implies $w \in \mathfrak{B}_l$. Vice versa, assume $w \in \mathfrak{B}_l$. It is obvious that $(\mathfrak{p}(w|_{[0,t)}), w(t), \mathfrak{p}(w|_{[0,t]})) \in \delta_l$ for all $t \in \mathbb{N}_0$. Hence, $z(t) := \mathfrak{p}(w|_{[0,t)})$, $t \in \mathbb{N}_0$, defines a state trajectory such that $(w,z) \in \mathfrak{B}_{s,l}$ and therefore $w \in \mathfrak{B}_{\mathrm{ex},l}$. To show that P_l is nonblocking, pick any reachable $\zeta \in Z_l$. As $\mathfrak{B}$ is nonempty, so is $\mathfrak{B}_l$. Hence, if $\zeta = w^*$, there exists a transition $(\zeta, -, -) \in \delta_l$. If $\zeta \neq w^*$, by the definition of δ_l there exists r, $0 \leqslant r < l$ such that $\zeta \in \mathfrak{B}|_{[0,r]}$. Hence, there exists a trajectory $w \in \mathfrak{B}$ such that $\zeta = w|_{[0,r]}$. This implies either $(\zeta, w(r+1), w|_{[0,r+1]}) \in \delta_l$ or $(\zeta, w(r+1), w|_{[1,r+1]}) \in \delta_l$. Thus, P_l is nonblocking. □

4. Hybrid systems

We now apply the results from above to a class of hybrid systems. It is characterized by the fact that the external signal is finite (i.e. $|W| \in \mathbb{N}$), while the state set X is a product of $\mathbb{R}^n$ and a finite set D. We still restrict systems to be time invariant and discrete time. However, from our point of view, it does not matter whether the time axis $\mathbb{N}_0$ is "clock time" (e.g. a regular sampling grid) or "logic time", enumerating the occurrence of events (where events could be defined as certain continuous variables crossing certain threshold values).

Definition 13. Let $W, |W| \in \mathbb{N}$, be an external signal space, $X = \mathbb{R}^n \times D$, $|D| \in \mathbb{N}$, a state space. Then, the state machine $P = (X, W, \delta, X_0)$ is said to be *hybrid*.

In the sequel, it will always be assumed that $X_0 = X$, i.e. the initial conditions are not restricted. This ensures time invariance of the external behaviour $\mathfrak{B}$ induced by P. Therefore, we can aim to approximate $\Sigma = (\mathbb{N}_0, W, \mathfrak{B}) \cong P$ by its strongest l-complete approximation $\Sigma_l = (\mathbb{N}_0, W, \mathfrak{B}_l)$.

Note that while the full behaviour $\mathfrak{B}_s$ is 1-complete by definition, we can not expect $\mathfrak{B}$ to be l-complete for any $l \in \mathbb{N}$. Hence, some degree of model accuracy will be lost when approximating $\mathfrak{B}$ by $\mathfrak{B}_l$. On the other hand, we know from the previous section that $\mathfrak{B}_l$ can be realized by the finite state machine P_l and is therefore amenable to methods from the field of DES theory.

We now discuss how to compute the next state relation δ_l for a given δ.

Definition 14. Let $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$ be a time-invariant system realized by the hybrid state machine $P = (X, W, \delta, X)$. Let $\mathfrak{B}_s$ be the full behaviour induced by P. Then, $\mathscr{X}(\bar{w}|_{[0,l]}) \subseteq X$ denotes the set of all states that are compatible with $\bar{w}|_{[0,l]} \in W^{l+1}$:

$$\mathscr{X}(\bar{w}|_{[0,l]}) := \{\xi \mid \exists (w,x) \in \mathfrak{B}_s\colon x(l) = \xi, \; w|_{[0,l]} = \bar{w}|_{[0,l]}\}. \tag{11}$$

If P is nonblocking, the sets of compatible states can be derived by the recursive formula given in the following proposition.

Proposition 15. *Let $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$ be a time-invariant system realized by a nonblocking state machine $P = (X, W, \delta, X)$. Then, in the notation of Definition 14, for any trajectory $\bar{w} \in W^{\mathbb{N}_0}$, the following holds*:

$$\mathscr{X}(\bar{w}|_{[0,0]}) = \{\xi \mid \exists \xi^+ \in X\colon (\xi, \bar{w}(0), \xi^+) \in \delta\}, \tag{12}$$

$$\mathscr{X}(\bar{w}|_{[0,l+1]}) = \{\xi \mid \exists \xi^- \in \mathscr{X}(\bar{w}|_{[0,l]})\colon (\xi^-, \bar{w}(l), \xi) \in \delta\} \cap \mathscr{X}(\bar{w}(l+1)). \tag{13}$$

Proof. It is obvious that any ξ in one of the left-hand-side sets in (12) or (13) satisfies the conditions stated on the respective right-hand-side. Hence the left-hand-side sets are contained in the right-hand-side sets. To show the converse, pick any ξ from the right-hand-side set of Eq. (12). Let $\mathfrak{B}_s$ denote the full behaviour induced by P. As P is nonblocking, there exists a trajectory $(w,x) \in \mathfrak{B}_s$, $x(0) = \xi$ and $w(0) = \bar{w}(0)$; hence, $\xi = x(0) \in \mathscr{X}(\bar{w}|_{[0,0]})$, yielding Eq. (12). Now, pick any ξ from the right-hand-side set in Eq. (13). As $\xi^- \in \mathscr{X}(\bar{w}|_{[0,l]})$, we know a trajectory $(w^-, x^-) \in \mathfrak{B}_s$ to exist such that $w^-|_{[0,l]} = \bar{w}|_{[0,l]}$ and $x^-(l) = \xi^-$. As $\xi \in \mathscr{X}(\bar{w}(l+1))$, there exists a trajectory $(w^+, x^+) \in \mathfrak{B}_s$ such that $x^+(0) = \xi$ and $w^+(0) = \bar{w}(l+1)$. We construct a trajectory $(w,x) \in \mathfrak{B}_s$ by concatenating $(w^-, x^-)|_{[0,l]}$ and (w^+, x^+): Let $x(t) := x^-(t)$, $w(t) := w^-(t)$ for all $t \leqslant l$, and $x(t) := x^+(t-l-1)$, $w(t) := w^+(t-l-1)$ for all $t > l$. This yields $x(l+1) = \xi$ and $w|_{[0,l+1]} = \bar{w}|_{[0,l+1]}$, implying $\xi \in \mathscr{X}(\bar{w}|_{[0,l+1]})$. Hence, it has been shown that Eq. (13) holds. □

From Eq. (13), it can be seen that $\mathscr{X}(\bar{w}|_{[0,l+1]})$ is the intersection of the set of all states which are reachable from $\mathscr{X}(\bar{w}|_{[0,l]})$ within one time step and the set of states compatible with the single external symbol $\bar{w}(l+1)$. If we can perform these operations repeatedly, we can compute all sets $\mathscr{X}(\cdot) \subseteq X$ compatible to strings up to length l. As we assume the external signal space W to be a finite set, $\mathfrak{B}|_{[0,l]}$ is also finite. Furthermore, $\bar{w}|_{[0,l]} \in \mathfrak{B}|_{[0,l]}$ is equivalent to $\mathscr{X}(\bar{w}|_{[0,l]}) \neq \emptyset$. The next state relation δ_l is defined in terms of $\mathfrak{B}|_{[0,l]}$. This is obvious from Eqs. (5)–(9). Thus, computing the sets of compatible states for all strings of external signals up to length l leads to an explicit representation of δ_l.

As an example, consider a hybrid system in strictly nonanticipating input/state/output form:

$$W = U \times Y, \quad |U| \in \mathbb{N}, \; |Y| \in \mathbb{N}, \tag{14}$$

$$f : X \times U \to X, \qquad g : X \to Y, \tag{15}$$

$$\delta := \{(\xi, (v, \mu), \xi') \mid \xi' = f(\xi, v), \; \mu = g(\xi)\}. \tag{16}$$

Note that P is nonblocking, but, in general, not past induced. Essentially, these are the same assumptions as in [14]. Indeed, the strongest l-complete approximation Σ_l induced by this hybrid system turns out to be equivalent — up to minor difference in the definition of z — to the "discrete abstraction A_{l+1}" defined in [14], or the "abstraction A_l" in [13]. Furthermore, Σ_l is similar to the "condensed model of order l" as proposed in [9], where the (more restrictive) class of switched-integrator systems is discussed. In our framework, Proposition 15 yields for any $u \in U^{\mathbb{N}_0}$, $y \in Y^{\mathbb{N}_0}$:

$$\mathscr{X}((u,y)|_{[0,0]}) = g^{-1}(y(0)), \tag{17}$$

$$\mathscr{X}((u,y)|_{[0,l+1]}) = f(\mathscr{X}((u,y)|_{[0,l]}), u(l)) \cap g^{-1}(y(l+1)). \tag{18}$$

Whenever one is able to repeatedly compute images under $f(\cdot, v)$ for fixed $v \in U$, inverse images under g, and intersections of those, the above equations can be used to compute the sets of compatible states and, hence, the next state relation for the approximation.

However, f and g are often given in implicit form only. This, for example, is the case when the discrete time axis is determined by continuous variables crossing certain threshold values. In this situation, it is common to apply an additional approximation step based on partitioning the continuous part of the state space. Typically, this leads to a realization P_{ca} with a large finite state space. Unfortunately, it is hardly ever past induced. Hence, in a second step, we compute the strongest l-complete approximation $\Sigma_l = (\mathbb{N}_0, W, \mathfrak{B}_l) \cong P_l$ for P_{ca}. If P_{ca} realizes a conservative approximation $\Sigma_{\mathrm{ca}} = (\mathbb{N}_0, W, \mathfrak{B}_{\mathrm{ca}})$ of the hybrid system Σ, then $\mathfrak{B} \subseteq \mathfrak{B}_{\mathrm{ca}} \subseteq \mathfrak{B}_l$ holds. In this case, Σ_l is still an l-complete approximation of Σ, but not necessarily the strongest one.

Before using l-complete approximations Σ_l for the purposes of supervisory control synthesis, we summarize the proposed abstraction procedure: our starting point is a hybrid state machine $P = (X, W, \delta, X)$. This induces the (full) behaviour $\mathfrak{B}_{\mathrm{s}}$ and the (discrete) external behaviour $\mathfrak{B} = \mathscr{P}_W \mathfrak{B}_{\mathrm{s}}$. First, choose an $l \in \mathbb{N}$ and compute (or conservatively estimate) the sets of compatible states $\mathscr{X}(\vec{w}|_{[0,r]})$ for all strings $\vec{w}|_{[0,r]}$, $r \leqslant l$. This can be done by the recursive formula stated in Proposition 15. Then, the (purely discrete) next state relation δ_l is set up according to Theorem 12. Hence, $P_l = (Z_l, W, \delta_l, Z_0)$ is a realization of an l-complete approximation Σ_l for $\Sigma = (\mathbb{N}, W, \mathfrak{B})$.

5. Supervisory control

A supervisor is a dynamical system $\Sigma_{\mathrm{sup}} = (\mathbb{N}_0, W, \mathfrak{B}_{\mathrm{sup}})$. Roughly speaking, its task is to prevent the system $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$ from evolving on trajectories which are deemed to be unacceptable — the supervisor is meant to suitably restrict the behaviour $\mathfrak{B}$. When the supervisor Σ_{sup} and the system Σ are connected, the closed-loop is modelled by $\Sigma_{\mathrm{cl}} = (\mathbb{N}_0, W, \mathfrak{B}_{\mathrm{cl}})$, where $\mathfrak{B}_{\mathrm{cl}} := \mathfrak{B} \cap \mathfrak{B}_{\mathrm{sup}}$. Characterizing the acceptable behaviour by a system $\Sigma_{\mathrm{spec}} = (\mathbb{N}_0, W, \mathfrak{B}_{\mathrm{spec}})$, we ask for a supervisor such that $\mathfrak{B}_{\mathrm{cl}} \subseteq \mathfrak{B}_{\mathrm{spec}}$.

The mechanism of interaction is to stop $w(t)$ from taking certain values in W. However, in general, it will not be possible to disable all elements in W independently. Throughout this paper, a unique product decomposition $W = U \times Y$ is considered, where U denotes the set of *input signals*, and Y the set of *output signals* — by $(u, y) = w \in W^{\mathbb{N}_0}$ we always refer to this decomposition; i.e. we implicitly assume $u = \mathscr{P}_U w \in U^{\mathbb{N}_0}$, $y = \mathscr{P}_Y w \in Y^{\mathbb{N}_0}$, where $\mathscr{P}_U$ and $\mathscr{P}_Y$ denote the canonical projections from $U \times Y$ onto U and Y, respectively. While the trajectory evolves, the supervisor is only allowed to "disable" input signals in an explicit manner. In turn, this may prevent certain output signals from occurring, but the latter cannot be disabled individually: when preventing the signal value $(\mu, v) \in U \times Y$, this can only be done by preventing all external signal values $\{(\mu, \tilde{v}) \mid \tilde{v} \in Y\}$ simultaneously. Definition 16 formalizes the desired mechanism of interaction.

Definition 16. The system $\Sigma_{\mathrm{sup}} = (\mathbb{N}_0, W, \mathfrak{B}_{\mathrm{sup}})$ is said to be an *admissible supervisor* w.r.t. the system $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$ if $w, \tilde{w} \in \mathfrak{B}$, $t \in \mathbb{N}_0$, $w|_{[0,t]} \in \mathfrak{B}_{\mathrm{sup}}|_{[0,t]}, \tilde{w}|_{[0,t)} = w|_{[0,t)}$ and $\mathscr{P}_U \tilde{w}(t) = \mathscr{P}_U w(t)$, implies that $w|_{[0,t]}, \tilde{w}|_{[0,t]} \in (\mathfrak{B} \cap \mathfrak{B}_{\mathrm{sup}})|_{[0,t]}$.

In other words: If w is a trajectory of $\mathfrak{B}$ such that the string $w|_{[0,t]}$ is not prevented by the supervisor Σ_{sup}, then $w|_{[0,t]}$ can be continued to a closed-loop trajectory. Then, any string $\tilde{w}|_{[0,t]} \in \mathfrak{B}|_{[0,t]}$ which equals $w|_{[0,t]}$ up to the last output symbol must also be allowed by Σ_{sup}.

Note that, according to Definition 16, the trivial system $\Sigma_\emptyset := (\mathbb{N}_0, W, \emptyset)$ is an admissible supervisor w.r.t. any system $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$. This, however, leads to an empty closed-loop behaviour. Obviously, this is not desirable. On the contrary, we want to maximize the closed-loop behaviour while still meeting the

specifications, i.e. we want the supervisor to be maximally permissive. If every admissible supervisor leads to an empty closed-loop behaviour, this can be interpreted as follows: "the only way to avoid violating the specifications is not to run the system".

To formalize this discussion, let $\mathfrak{C}(\Sigma, \Sigma_{\text{spec}})$ denote the set of all closed-loop behaviours $\mathfrak{B}_{\text{cl}} := \mathfrak{B} \cap \mathfrak{B}_{\text{sup}}$, such that $\Sigma_{\text{sup}} = (\mathbb{N}_0, W, \mathfrak{B}_{\text{sup}})$ is an admissible supervisor w.r.t. Σ and $\mathfrak{B} \cap \mathfrak{B}_{\text{sup}} \subseteq \mathfrak{B}_{\text{spec}}$ holds.

Proposition 17. *Let A be some index set and $\Sigma_\alpha = (\mathbb{N}_0, W, \mathfrak{B}_\alpha)$ be admissible supervisors w.r.t $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$ for all $\alpha \in A$. Then, $\Sigma_{\text{sup}} := (\mathbb{N}_0, W, \bigcup_{\alpha\in A} \mathfrak{B}_\alpha)$ is also an admissible supervisor w.r.t. Σ.*

Proof. Pick any $w, \tilde{w} \in \mathfrak{B}$, $t \in \mathbb{N}_0$ such that $w|_{[0,t]} \in (\bigcup_{\alpha\in A} \mathfrak{B}_\alpha)|_{[0,t]}, \tilde{w}|_{[0,t)} = w|_{[0,t)}$ and $\mathscr{P}_U \tilde{w}(t) = \mathscr{P}_U w(t)$. We need to show that $w|_{[0,t]}, \tilde{w}|_{[0,t]} \in (\mathfrak{B} \cap (\bigcup_{\alpha\in A} \mathfrak{B}_\alpha))|_{[0,t]}$. Observe that $(\bigcup_{\alpha\in A} \mathfrak{B}_\alpha)|_{[0,t]} = \bigcup_{\alpha\in A}(\mathfrak{B}_\alpha|_{[0,t]})$; hence, $w|_{[0,t]} \in \mathfrak{B}_\alpha|_{[0,t]}$ for some $\alpha \in A$. This implies $w|_{[0,t]}, \tilde{w}|_{[0,t]} \in (\mathfrak{B} \cap \mathfrak{B}_\alpha)|_{[0,t]}$. Therefore $w|_{[0,t]}, \tilde{w}|_{[0,t]} \in (\mathfrak{B} \cap (\bigcup_{\alpha\in A} \mathfrak{B}_\alpha))|_{[0,t]}$. □

As $\mathfrak{B} \cap \mathfrak{B}_{\text{sup}} = \mathfrak{B} \cap \mathfrak{B}_{\text{cl}}$ and $\mathfrak{B}_{\text{cl}} \subseteq \mathfrak{B}_{\text{sup}}$, an immediate consequence from Definition 16 is that any closed-loop behaviour $\mathfrak{B}_{\text{cl}} \in \mathfrak{C}(\Sigma, \Sigma_{\text{spec}})$ constitutes an admissible supervisor $\Sigma_{\text{sup}} = (\mathbb{N}_0, W, \mathfrak{B}_{\text{cl}})$ w.r.t. Σ. Then, by the above proposition, the union $\mathfrak{B}^+_{\text{cl}}$ of all closed-loop behaviours in $\mathfrak{C}(\Sigma, \Sigma_{\text{spec}})$ is also an admissible supervisor $\Sigma^+_{\text{sup}} = (\mathbb{N}_0, W, \mathfrak{B}^+_{\text{cl}})$ w.r.t Σ. Obviously, $\mathfrak{B}^+_{\text{cl}} \subseteq \mathfrak{B} \cap \mathfrak{B}_{\text{spec}}$; hence $\mathfrak{B}^+_{\text{cl}} \in \mathfrak{C}(\Sigma, \Sigma_{\text{spec}})$ is the supremal element of $\mathfrak{C}(\Sigma, \Sigma_{\text{spec}})$ (w.r.t. the partial order induced by "$\subseteq$"). Therefore, $\mathfrak{B}^+_{\text{cl}}$ can be seen as the least-restrictive closed-loop behaviour which can be achieved by an admissible supervisor and which meets the specification. Obviously, an admissible supervisor giving rise to the least-restrictive closed-loop behaviour $\mathfrak{B}^+_{\text{cl}}$ is given by Σ^+_{sup}.

We now investigate the problem on the realization level.

Definition 18. Let $P = (X, W, \delta, X_0)$ and $P_{\text{spec}} = (X_{\text{spec}}, W, \delta_{\text{spec}}, X_{\text{spec}_0})$ be state machines. Let $P_{\|} := (Q, W, \lambda, Q_0) := P \parallel P_{\text{spec}}$. The transitions $(\xi, \omega, \xi') \in \delta$ and $(\tilde{\xi}, \tilde{\omega}, \tilde{\xi}') \in \delta$ are called *partners*, if $\xi = \tilde{\xi}$ and $\mathscr{P}_U \omega = \mathscr{P}_U \tilde{\omega}$. Let $\tilde{P}_{\|} = (Q, W, \tilde{\lambda}, \tilde{Q}_0)$ be a state machine such that (i) $\tilde{\lambda} \subseteq \lambda$, $\tilde{Q}_0 \subseteq Q_0$, and (ii) a transition $((\xi, \xi_{\text{spec}}), \omega, (\xi', \xi'_{\text{spec}})) \in \lambda$ can only be an element in λ, if for every partner $(\xi, \tilde{\omega}, \tilde{\xi}')$ of (ξ, ω, ξ') there exists a transition $((\xi, \xi_{\text{spec}}), \tilde{\omega}, (\tilde{\xi}', -))$ in $\tilde{\lambda}$. Then, $\tilde{P}_{\|}$ is called a *substructure* of $P \parallel P_{\text{spec}}$ w.r.t. P.

Indeed, a system Σ_{sup} realized by a nonblocking substructure of $P \parallel P_{\text{spec}}$ w.r.t. P is an admissible supervisor w.r.t. $\Sigma \cong P$ enforcing the specifications:

Proposition 19. *Let $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$ and $\Sigma_{\text{spec}} = (\mathbb{N}_0, W, \mathfrak{B}_{\text{spec}})$ be realized by past-induced state machines $P = (X, W, \delta, X_0)$ and $P_{\text{spec}} = (X_{\text{spec}}, W, \delta_{\text{spec}}, X_{\text{spec}_0})$, respectively. Let $P_{\text{sup}} = (Q, W, \delta_{\text{sup}}, Q_{\text{sup}_0})$ be a nonblocking substructure of $P \parallel P_{\text{spec}}$ w.r.t. P. Then, $\Sigma_{\text{sup}} = (\mathbb{N}_0, W, \mathfrak{B}_{\text{sup}}) \cong P_{\text{sup}}$ is an admissible supervisor w.r.t. Σ. The closed-loop behaviour meets the specifications: $\mathfrak{B}_{\text{cl}} := \mathfrak{B} \cap \mathfrak{B}_{\text{sup}} \subseteq \mathfrak{B}_{\text{spec}}$.*

Proof. Observe that $\mathfrak{B}_{\text{sup}} \cap \mathfrak{B} \subseteq \mathfrak{B}_{\text{spec}}$, hence $\mathfrak{B}_{\text{cl}} = \mathfrak{B}_{\text{sup}} \subseteq \mathfrak{B}_{\text{spec}}$. Let $\mathfrak{p}_{\text{x}}$ and $\mathfrak{p}_{\text{spec}}$ denote the past-induced state maps of P and P_{spec}, respectively. Note that as $P \parallel P_{\text{spec}}$ is past induced, so is P_{sup}: the map $(\mathfrak{p}_{\text{x}}, \mathfrak{p}_{\text{spec}})$ restricted to the domain $\bigcup_{t\in\mathbb{N}_0} \mathfrak{B}_{\text{sup}}|_{[0,t)}$ serves as past-induced state map of P_{sup}. Now pick any $w, \tilde{w} \in \mathfrak{B}$, $t \in \mathbb{N}_0$ such that $w|_{[0,t]} \in \mathfrak{B}_{\text{sup}}|_{[0,t]}, \tilde{w}|_{[0,t)} = w|_{[0,t)}$ and $\mathscr{P}_U \tilde{w}(t) = \mathscr{P}_U w(t)$. As $\mathfrak{B}_{\text{cl}} = \mathfrak{B}_{\text{sup}}$, we have $w|_{[0,t]} \in (\mathfrak{B} \cap \mathfrak{B}_{\text{sup}})|_{[0,t]}$. Let $\xi = \mathfrak{p}_{\text{x}}(w|_{[0,t)})$, $\xi' = \mathfrak{p}_{\text{x}}(w|_{[0,t]})$, $\xi_{\text{spec}} = \mathfrak{p}_{\text{spec}}(w|_{[0,t)})$ and $\xi'_{\text{spec}} = \mathfrak{p}_{\text{spec}}(w|_{[0,t]})$. Hence, $((\xi, \xi_{\text{spec}}), w(t), (\xi', \xi'_{\text{spec}})) \in \delta_{\text{sup}}$. Let $\tilde{\xi}' = \mathfrak{p}_{\text{x}}(\tilde{w}|_{[0,t]})$ and observe the transitions $(\xi, w(t), \xi') \in \delta$ and $(\xi, \tilde{w}(t), \tilde{\xi}') \in \delta$ to be partners. As P_{sup} is a substructure w.r.t. P, there exists a $\tilde{\xi}'_{\text{spec}}$ such that $((\xi, \xi_{\text{spec}}), \tilde{w}(t), (\tilde{\xi}', \tilde{\xi}'_{\text{spec}})) \in \delta_{\text{sup}}$. As P_{sup} is nonblocking, there exists a trajectory $\hat{w} \in \mathfrak{B}_{\text{sup}}$ such that $\hat{w}|_{[0,t]} = \tilde{w}|_{[0,t]}$; hence, $\tilde{w}|_{[0,t]} \in (\mathfrak{B} \cap \mathfrak{B}_{\text{sup}})|_{[0,t]}$. Thus, Σ_{sup} is an admissible supervisor w.r.t. Σ. □

This raises the question, whether every admissible supervisor Σ_{sup} meeting the specifications can be realized by a nonblocking substructure. This is not the case. But we can always find an admissible supervisor Σ'_{sup} which is realized by a nonblocking substructure and which is at least as permissive as Σ_{sup}.

Proposition 20. *Let $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$ and $\Sigma_{\text{spec}} = (\mathbb{N}_0, W, \mathfrak{B}_{\text{spec}})$ be realized by nonblocking past-induced state machines $P = (X, W, \delta, X_0)$ and $P_{\text{spec}} = (X_{\text{spec}}, W, \delta_{\text{spec}}, X_{\text{spec}_0})$, respectively. Let $\Sigma_{\text{sup}} = (\mathbb{N}_0, W, \mathfrak{B}_{\text{sup}})$ be an admissible supervisor w.r.t. Σ such that $\mathfrak{B}_{\text{cl}} := \mathfrak{B} \cap \mathfrak{B}_{\text{sup}} \subseteq \mathfrak{B}_{\text{spec}}$. Then, there exists a nonblocking past-induced substructure of*

$P \parallel P_{\text{spec}}$ w.r.t. P, denoted by P'_{sup}, such that $\mathfrak{B}_{\text{cl}} \subseteq \mathfrak{B}'_{\text{cl}} := \mathfrak{B} \cap \mathfrak{B}'_{\text{sup}} \subseteq \mathfrak{B}_{\text{spec}}$, where $\mathfrak{B}'_{\text{sup}}$ denotes the external behaviour induced by P'_{sup}.

Proof. *If* $\mathfrak{B}_{\text{cl}} = \emptyset$, we choose the empty set as initial condition: $P'_{\text{sup}} = (X \times X_{\text{spec}}, W, \emptyset, \emptyset)$ is a nonblocking past-induced substructure of $P \parallel P_{\text{sup}}$. We now construct a suitable P'_{sup} for the case $\mathfrak{B}_{\text{cl}} \neq \emptyset$. Let $P_{\parallel} := (Q, W, \lambda, Q_0) := P \parallel P_{\text{spec}}$, where $Q = X \times X_{\text{spec}}$ and $Q_0 = X_0 \times X_{\text{spec}_0}$. As P and P_{spec} are past induced, so is $P_{\parallel}$; hence, $|Q_0| \leqslant 1$. As $\mathfrak{B}_{\text{cl}} \subseteq \mathfrak{B} \cap \mathfrak{B}_{\text{spec}}$ is nonempty, $Q_0 = \{\rho_0\}$. Let $\mathfrak{p}$ denote the past-induced state map of $P_{\parallel}$. Define the next state relation $\delta'_{\text{sup}} \subseteq Q \times W \times Q$ by

$$\delta'_{\text{sup}} := \{(\mathfrak{p}(w|_{[0,t)}), w(t), \mathfrak{p}(w|_{[0,t+1)})) \mid w \in \mathfrak{B}_{\text{cl}}, \; t \in \mathbb{N}_0\} \tag{19}$$

and check $P'_{\text{sup}} := (Q, W, \delta'_{\text{sup}}, Q_0)$ to be a nonblocking past-induced substructure of $P \parallel P_{\text{spec}}$ w.r.t. P. As $\mathfrak{B}_{\text{cl}} \subseteq \mathfrak{B} \cap \mathfrak{B}_{\text{spec}}$ and $P_{\parallel}$ is past induced, we have $\delta'_{\text{sup}} \subseteq \lambda$; hence, $\mathfrak{B}'_{\text{sup}} \subseteq \mathfrak{B} \cap \mathfrak{B}_{\text{spec}}$. On the other hand, it is obvious that $\mathfrak{B}_{\text{cl}} \subseteq \mathfrak{B}'_{\text{sup}}$. Hence, $\mathfrak{B}_{\text{cl}} \subseteq \mathfrak{B}'_{\text{sup}} = \mathfrak{B}'_{\text{cl}} \subseteq \mathfrak{B}_{\text{spec}}$. As $\delta'_{\text{sup}} \subseteq \lambda$, P'_{sup} is past induced. To show that P'_{sup} is nonblocking, pick any reachable $\rho \in Q$. As $\mathfrak{B}_{\text{cl}}$ is nonempty, so is $\mathfrak{B}'_{\text{sup}}$. Hence, if $\rho = \rho_0$, there must exist a transition $(\rho, -, -) \in \delta'_{\text{sup}}$. If $\rho \neq \rho_0$, it follows from (19) that there exists $w \in \mathfrak{B}_{\text{cl}}$ and $t \in \mathbb{N}_0$ such that $\rho = \mathfrak{p}(w|_{[0,t+1)})$; hence, $(\rho, w(t+1), \mathfrak{p}(w|_{[0,t+2)})) \in \delta'_{\text{sup}}$. Thus, P'_{sup} is nonblocking. Finally, we check that P'_{sup} is a substructure of $P \parallel P_{\text{spec}}$ w.r.t. P: pick any transition $((\xi, \xi_{\text{spec}}), \omega, (\xi', \xi'_{\text{spec}})) \in \delta'_{\text{sup}}$ and any partner $(\xi, \tilde{\omega}, \tilde{\xi}') \in \delta$ of $(\xi, \omega, \xi') \in \delta$. By (19), there exists a $w \in \mathfrak{B}_{\text{cl}}$ and a $t \in \mathbb{N}_0$ such that $\mathfrak{p}(w|_{[0,t)}) = (\xi, \xi_{\text{spec}})$ and $w(t) = \omega$. Let $\mathfrak{p}_x$ denote the past-induced state map of P; hence, $\xi = \mathfrak{p}_x(w|_{[0,t)})$. As P is nonblocking, there exists a $\tilde{w} \in \mathfrak{B}$ such that $\tilde{w}|_{[0,t)} = w|_{[0,t)}, \tilde{w}(t) = \tilde{\omega}$ and $\mathfrak{p}_x(\tilde{w}|_{[0,t]}) = \tilde{\xi}'$. Clearly, $w \in \mathfrak{B}, w|_{[0,t]} \in \mathfrak{B}_{\text{sup}}|_{[0,t]}$ and $\mathscr{P}_U \tilde{w}(t) = \mathscr{P}_U w(t)$. Then, as Σ_{sup} is an admissible supervisor w.r.t. $\Sigma, \tilde{w}|_{[0,t]} \in \mathfrak{B}_{\text{cl}}|_{[0,t]}$. This implies $((\xi, \xi_{\text{spec}}), \tilde{\omega}, (\tilde{\xi}', -)) \in \delta'_{\text{sup}}$. □

It follows directly from the above propositions that only substructures of $P \parallel P_{\text{spec}}$ w.r.t. P need to be considered when the least restrictive closed-loop behaviour is to be synthesized:

Theorem 21. *Let $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$ and $\Sigma_{\text{spec}} = (\mathbb{N}_0, W, \mathfrak{B}_{\text{spec}})$ be realized by nonblocking past-induced state machines $P = (X, W, \delta, X_0)$ and $P_{\text{spec}} = (X_{\text{spec}}, W, \delta_{\text{spec}}, X_{\text{spec}_0})$, respectively. Denote the supremal element of $\mathfrak{C}(\Sigma, \Sigma_{\text{spec}})$ by $\mathfrak{B}^+_{\text{cl}}$. Then $\Sigma^+_{\text{sup}} = (\mathbb{N}_0, W, \mathfrak{B}^+_{\text{cl}})$ is an admissible supervisor w.r.t. Σ, and Σ^+_{sup} can be realized by a nonblocking past-induced substructure of $P \parallel P_{\text{spec}}$ w.r.t. P, denoted by P^+_{sup}. If both P and P_{spec} are finite, so is P^+_{sup}.*

The theorem is immediately inferred from Propositions 19 and 20. If P and P_{spec} are finite, P^+_{sup} can be synthesized by a fixed-point algorithm. An implementation coded in C++ has been reported in [12].

6. Supervisory control based on conservative approximations

Recall that the above algorithm for supervisory control can only be used if the plant model $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$ is realized by a nonblocking finite past-induced state machine $P = (X, W, \delta, X_0)$.

If the plant is time invariant, but fails to be either finite or nonblocking, we suggest the following procedure: we first apply the approximation scheme from Section 3 and realize an l-complete approximation of Σ by a nonblocking finite past-induced state machine $P_{\text{ca}}, \Sigma_{\text{ca}} = (\mathbb{N}_0, W, \mathfrak{B}_{\text{ca}}) \cong P_{\text{ca}}$. In a second step, we apply the results of Section 5 and synthesize a realization P^+_{sup} of the least-restrictive closed-loop behaviour $\mathfrak{B}^+_{\text{cl}} \in \mathfrak{C}(\Sigma_{\text{ca}}, \Sigma_{\text{spec}})$ meeting the specifications. For this, we assume Σ_{spec} to be realized by a nonblocking finite past-induced state machine P_{spec}. The system $\Sigma^+_{\text{sup}} = (\mathbb{N}_0, W, \mathfrak{B}^+_{\text{cl}}) \cong P^+_{\text{sup}}$ is an admissible supervisor w.r.t. Σ_{ca}, and $\mathfrak{B}_{\text{ca}} \cap \mathfrak{B}^+_{\text{cl}} = \mathfrak{B}^+_{\text{cl}} \subseteq \mathfrak{B}_{\text{spec}}$.

Now, we need to show two properties: (i) Σ^+_{sup} is an admissible supervisor w.r.t. the plant Σ; (ii) when connecting Σ^+_{sup} to the plant Σ, the closed loop will not exhibit any unacceptable behaviour. (ii) is obvious, because $\mathfrak{B}_{\text{cl}} := \mathfrak{B} \cap \mathfrak{B}^+_{\text{cl}} \subseteq \mathfrak{B} \cap \mathfrak{B}_{\text{spec}} \subseteq \mathfrak{B}_{\text{spec}}$. We claim that (i) is also true, if Σ exhibits the input–output structure stated below.

Definition 22 (*see Willems* [20, *Definition* VIII.1 *and* VIII.4]). The system $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$, $W = U \times Y$, is said to be an I/– system if:

1. the input is free, i.e. $\mathscr{P}_U \mathfrak{B} = U^{\mathbb{N}_0}$;
2. the output does not anticipate the input, i.e. for all $t \in \mathbb{N}_0, (\tilde{u}, \tilde{y}), (\hat{u}, \hat{y}) \in \mathfrak{B}$ the following implication holds:

$$\tilde{u}|_{[0,t]} = \hat{u}|_{[0,t]} \;\Rightarrow\; \exists y \in Y^{\mathbb{N}_0}\colon\ y|_{[0,t]} = \tilde{y}|_{[0,t]}, \; (\hat{u}, y) \in \mathfrak{B}. \tag{20}$$

Note that, unlike *Willems*' I/O systems [20, Definition VIII.3], an I/– system does not require the output to process the input, i.e. we do not demand that the future of the output signal is uniquely determined by the input and the past of the output [20, Definition VIII.2]. The hybrid systems introduced in Section 4 are I/– systems but, in general, not I/O systems in *Willems*' sense.

Definition 23. A state machine $P = (X, W, \delta, X_0)$ is said to be an I/S/– *machine*, if for every reachable $\xi \in X$, $\mu \in U$, there exists a $v \in Y$ such that $(\xi, (\mu, v), -) \in \delta$.

Note that I/S/– machines are nonblocking. The link between I/– systems and I/S/– machines is provided by the following proposition.

Proposition 24. *If P is an I/S/– machine, the induced system Σ is an I/– system. Vice versa, Σ being an I/– system and P being a nonblocking past-induced realization implies that P is an I/S/– machine.*

Proof. Let $\mathfrak{B}_s$ and $\mathfrak{B}$ denote the full and external behaviour induced by $P = (X, W, \delta, X_0)$. First, assume P to be an I/S/– machine. Obviously, the input is free. To show that the output does not anticipate the input, focus on $t \in \mathbb{N}_0$, $(\tilde{u}, \tilde{y}), (\hat{u}, \hat{y}) \in \mathfrak{B}$ such that $\tilde{u}|_{[0,t]} = \hat{u}|_{[0,t]}$. Pick $\tilde{x}$, $\hat{x} \in X^{\mathbb{N}_0}$ such that $(\tilde{u}, \tilde{y}, \tilde{x}), (\hat{u}, \hat{y}, \hat{x}) \in \mathfrak{B}_s$. Clearly, $\tilde{x}(t+1) =: \xi_{t+1}$ is reachable. Then, because of the I/S/– property, we can successively pick $\xi_{\tau+1} \in X$, $v_\tau \in Y$, $\tau > t$, such that $(\xi_\tau, (\hat{u}(\tau), v_\tau), \xi_{\tau+1}) \in \delta$. Let $y(\tau) := \tilde{y}(\tau)$, $x(\tau) := \tilde{x}(\tau)$ for all $\tau \leqslant t$ and $y(\tau) := v_\tau$, $x(\tau) := \xi_\tau$ for all $\tau > t$. Observe that $(\hat{u}, y, x) \in \mathfrak{B}_s$, hence $(\hat{u}, y) \in \mathfrak{B}$. Thus, Σ is an I/– system. Secondly, assume Σ to be an I/– system and P to be a nonblocking past induced realization. Pick any reachable $\xi \in X$ and any $\mu \in U$. As P is nonblocking, there exists $t \in \mathbb{N}_0$ and $(\tilde{u}, \tilde{y}, \tilde{x}) \in \mathfrak{B}_s$ such that $\tilde{x}(t) = \xi$. Since the input is free, there exists $(\hat{u}, \hat{y}) \in \mathfrak{B}$ such that $\hat{u}|_{[0,t)} = \tilde{u}|_{[0,t)}$ and $\hat{u}(t) = \mu$. Pick $\hat{x}$ such that $(\hat{u}, \hat{y}, \hat{x}) \in \mathfrak{B}_s$. In the case $t = 0$, ξ is the only element in X_0 (this follows from P being past induced). Hence, $(\xi, (\mu, \hat{y}(0)), -) \in \delta$. We now consider the case $t > 0$. As the output is not anticipated by the input, there exists a $y \in Y^{\mathbb{N}_0}$ such that $y|_{[0,t)} = \tilde{y}|_{[0,t)}$, $(\hat{u}, y) \in \mathfrak{B}$. Pick x such that $(\hat{u}, y, x) \in \mathfrak{B}_s$. Since P is past induced, $x(t) = \xi$ holds; hence, $(\xi, (\mu, y(t)), x(t+1)) \in \delta$. Therefore, P is an I/S/– machine. □

We can now prove the claim related to property (i):

Theorem 25. *Let $\Sigma_{ca} = (\mathbb{N}_0, W, \mathfrak{B}_{ca})$ be a conservative approximation of $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$, i.e. $\mathfrak{B} \subset \mathfrak{B}_{ca}$; let $\Sigma_{sup} = (\mathbb{N}_0, W, \mathfrak{B}_{sup})$ be a complete admissible supervisor w.r.t. Σ_{ca}. If Σ is a complete I/– system, then Σ_{sup} is an admissible supervisor w.r.t. Σ. If the closed-loop behaviour $\mathfrak{B}_{ca} \cap \mathfrak{B}_{sup}$ is nonempty, so is $\mathfrak{B} \cap \mathfrak{B}_{sup}$.*

Proof. We first prove the following claim:

$$w \in \mathfrak{B},\ w|_{[0,t]} \in (\mathfrak{B}_{ca} \cap \mathfrak{B}_{sup})|_{[0,t]} \Rightarrow w|_{[0,t]} \in (\mathfrak{B} \cap \mathfrak{B}_{sup})|_{[0,t]}. \tag{21}$$

Pick any $w \in \mathfrak{B}$, $t \in \mathbb{N}_0$ such that the left-hand side in (21) holds. We now successively construct trajectories $w_k \in \mathfrak{B}$, $k \in \mathbb{N}_0$, $k \geqslant t$, starting with $w_t := w$, such that

$$w_k|_{[0,k]} \in (\mathfrak{B}_{ca} \cap \mathfrak{B}_{sup})|_{[0,k]},$$

$$w_k|_{[0,k-1]} = w_{k-1}|_{[0,k-1]} \tag{22}$$

holds for all $k > t$. Focus on an arbitrary $k > t$ and assume (22) to hold for some $w_k \in \mathfrak{B}$. Then we can pick a $\tilde{w}_k \in \mathfrak{B}_{ca} \cap \mathfrak{B}_{sup}$ such that $\tilde{w}_k|_{[0,k]} = w_k|_{[0,k]}$. As $\mathfrak{B}$ is an I/– system, there exists $\hat{w}_k \in \mathfrak{B} \subseteq \mathfrak{B}_{ca}$ such that $\hat{w}_k|_{[0,k]} = \tilde{w}_k|_{[0,k]}$ and $\mathscr{P}_U \hat{w}_k = \mathscr{P}_U \tilde{w}_k$. Observe that: $\tilde{w}_k \in \mathfrak{B}_{ca}$, $\tilde{w}_k|_{[0,k+1]} \in (\mathfrak{B}_{ca} \cap \mathfrak{B}_{sup})|_{[0,k+1]}$, $\hat{w}_k \in \mathfrak{B}_{ca}$ and $\mathscr{P}_U \hat{w}_k(k+1) = \mathscr{P}_U \tilde{w}_k(k+1)$. As Σ_{sup} is an admissible supervisor w.r.t Σ_{ca}, the above properties imply $\hat{w}_k|_{[0,k+1]} \in (\mathfrak{B}_{ca} \cap \mathfrak{B}_{sup})|_{[0,k+1]}$; hence, $w_{k+1} := \hat{w}_k$ satisfies Eq. (22). This completes the construction of the series of trajectories $(w_k)_{k \geqslant t}$, $w_k \in \mathfrak{B}$. By the second part of (22), $w_l(k) = w_k(k)$ for all $k, l \geqslant k$; hence, $(w_k)_{k \geqslant t}$ converges pointwise. Let $w_\infty(t) := \lim_{k \to \infty} w_k(t)$ for all $t \in \mathbb{N}_0$. Observe that $w_\infty|_{[0,k]} = w_k|_{[0,k]}$ for all $k \geqslant t$. Thus (22) implies $w_\infty|_{[0,k]} \in \mathfrak{B}|_{[0,k]}$ and $w_\infty|_{[0,k]} \in \mathfrak{B}_{sup}|_{[0,k]}$ for all $k \geqslant t$; hence, as Σ and Σ_{sup} are complete, $w_\infty \in \mathfrak{B} \cap \mathfrak{B}_{sup}$. Thus $w|_{[0,t]} = w_\infty|_{[0,t]}$ can be continued within $\mathfrak{B} \cap \mathfrak{B}_{sup}$; hence, the claim (21) has been proven. In order to prove the theorem, pick any $w, \tilde{w} \in \mathfrak{B}$, $t \in \mathbb{N}_0$ such that $w|_{[0,t]} \in \mathfrak{B}_{sup}|_{[0,t]}$, $\tilde{w}|_{[0,t)} = w|_{[0,t)}$ and $\mathscr{P}_U \tilde{w}(t) = \mathscr{P}_U w(t)$. Then Σ_{sup} being an admissible supervisor w.r.t Σ_{ca} and $\mathfrak{B} \subseteq \mathfrak{B}_{ca}$ implies $w|_{[0,t]}$, $\tilde{w}|_{[0,t)} \in (\mathfrak{B}_{ca} \cap \mathfrak{B}_{sup})|_{[0,t]}$. Hence, by (21) $w|_{[0,t]}$, $\tilde{w}|_{[0,t]} \in (\mathfrak{B} \cap \mathfrak{B}_{sup})|_{[0,t]}$. Thus Σ_{sup} is an admissible supervisor w.r.t. Σ. Now, assume $\mathfrak{B}_{ca} \cap \mathfrak{B}_{sup}$ to be nonempty. Again by (21), this implies $\mathfrak{B} \cap \mathfrak{B}_{sup}$ to be nonempty too. □

7. Conclusions

In this contribution, we use the framework provided by *Willems*' behavioural systems theory to suggest an approach for synthesizing supervisory control for hybrid systems. We first determine an l-complete approximation Σ_l of the hybrid system under consideration; this approximation can be represented by a finite state machine. Hence, in a second step, tools from the theory of discrete event systems (DES) can be used to solve the supervisory control problem on the approximation level. It is then shown that the desired closed-loop properties are retained if the supervisor is connected to the underlying hybrid system. If no solution exists for Σ_l, approximation accuracy can be increased by computing a k-complete approximation Σ_k, $k > l$.

References

[1] R. Alur, T.A. Henzinger, E.D. Sontag (Eds.), Hybrid Systems III, Lecture Notes in Computer Science, vol. 1066, Springer, Berlin, 1996.

[2] P.J. Antsaklis, W. Kohn, A. Nerode, S. Sastry (Eds.), Hybrid Systems II, Lecture Notes in Computer Science, vol. 999, Springer, Berlin, 1995.

[3] P.J. Antsaklis, W. Kohn, A. Nerode, S. Sastry (Eds.), Hybrid Systems IV, Lecture Notes in Computer Science, vol. 1273, Springer, Berlin, 1997.

[4] P.J. Antsaklis, A. Nerode (Eds.), IEEE Transactions on Automatic Control, Special Issue on Hybrid Systems, vol. 43, 1998.

[5] P.J. Antsaklis, J.A. Stiver, M. Lemmon, Hybrid system modelling and autonomous control systems, in: R.L. Grossman, A. Nerode, A.P. Ravn, H. Rischel (Eds.), Hybrid Systems, Lecture Notes in Computer Science, vol. 736, Springer, Berlin, 1993, pp. 366–392.

[6] J.E.R. Cury, B.A. Krogh, T. Niinomi, Synthesis of supervisory controllers for hybrid systems based on approximating automata, IEEE Trans. Automat. Control, Special Issue on Hybrid Systems 43 (1998) 564–568.

[7] R.L. Grossman, A. Nerode, A.P. Ravn, H. Rischel (Eds.), Hybrid Systems, Lecture Notes in Computer Science, vol. 736, Springer, Berlin, 1993.

[8] J. Lunze, Stabilization of nonlinear systems by qualitative feedback controllers, Int. J. Control 62 (1995) 109–128.

[9] T. Moor, Event driven control of switched-integrator-systems, Proceedings of the ADPM98, Reims, 1998, pp. 271–277.

[10] T. Moor, J. Raisch, Discrete control of switched linear systems, in: Proceedings of the European Control Conference, Karlsruhe, 1999, pp. I1014–1015.

[11] T. Moor, J. Raisch, S.D. O'Young, Supervisory control of hybrid systems via l-complete approximations, Proceedings of the WODES98, IEE, 1998, pp. 426–431.

[12] S.D. O'Young, Hybrid RTSS, Internal Report, Faculty of Engineering, Memorial University of Newfoundland, 1998.

[13] J. Raisch, A hierarchy of discrete abstractions for a given hybrid plant, Proceedings of the ADPM98, Reims, 1998, pp. 55–62.

[14] J. Raisch, S.D. O'Young, A totally ordered set of discrete abstractions for a given hybrid or continuous system, in: P.J. Antsaklis, W. Kohn, A. Nerode, S. Sastry (Eds.), Hybrid Systems IV, Lecture Notes in Computer Science, vol. 1273, Springer, Berlin, 1997, pp. 342–360.

[15] J. Raisch, S.D. O'Young, Discrete approximation and supervisory control of continuous systems, IEEE Trans. Automat. Control, Special Issue on Hybrid Systems 43 (1998) 569–573.

[16] P.J. Ramadge, W.M. Wonham, Supervisory control of a class of discrete event systems, SIAM J. Control Optim. 25 (1987) 206–230.

[17] P.J. Ramadge, W.M. Wonham, The control of discrete event systems, Proc. IEEE 77 (1989) 81–98.

[18] M. Tittus, B. Egardt, Control-law synthesis for linear hybrid systems, Proceedings of the 33rd IEEE Conference on Decision and Control, 1994, pp. 961–966.

[19] J.C. Willems, Models for dynamics, Dyn. Rep. 2 (1989) 172–269.

[20] J.C. Willems, Paradigms and puzzles in the theory of dynamic systems, IEEE Trans. Automat. Control 36 (3) (1991) 258–294.