SUPERVISORY CONTROL OF HYBRID SYSTEMS VIA l-COMPLETE APPROXIMATIONS

Thomas Moor[1] Jörg Raisch[2] Siu O'Young[3]

[1] Fachbereich Elektrotechnik, Universität der Bundeswehr Hamburg, D-22039 Hamburg, Fed. Rep. Germany, Tel.: +49 40 6541-2121, Email: thomas.moor@unibw-hamburg.de
[2] Max-Planck-Institut für Dynamik komplexer technischer Systeme, Leipziger Str. 44, D-39120 Magdeburg, Fed. Rep. Germany, Tel.: +49 391 6117-502, Email: raisch@mpi-magdeburg.mpg.de
[3] Faculty of Engineering and Applied Science, Memorial University of Newfoundland, St. John's, Newfoundland, Canada A1B 3X5, Tel. (709) 737 8345, Email:oyoung@engr.mun.ca

Keywords

Hybrid systems, supervisory control, behavioural approach, l-complete approximations.

Abstract

This contribution deals with the synthesis of supervisory control for hybrid systems Σ with discrete external signals. Such systems are in general neither l-complete nor representable by finite state machines. We find the strongest 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 the strongest k-complete abstraction Σ_k, $k > l$. Most of this paper is set within the framework of *Willems'* behavioural systems theory.

1 Introduction

The topic of this paper is supervisory control of time invariant hybrid systems with discrete external (input and output) signals. Roughly speaking, the external behaviour (the set of external signals) of such a system is unlikely to possess any properties apart from time invariance. For an example see [Lu94], where it is shown that the external behaviour of a certain class of particularly simple hybrid systems is Markovian if and only if a very restrictive condition holds. From a more general point of view, we observe that any kind of completeness property that the full (state) behaviour possesses will usually be lost when focus is on the external behaviour only. In general, the external (discrete) behaviour of a hybrid system cannot be represented by a finite state machine. In order to apply supervisory control synthesis techniques, we therefore introduce the strongest l-complete approximation as a discrete abstraction for the hybrid system and represent it by a finite state machine. Similar to the procedure described in [Wi89], 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.

Applying a slightly modified version of *Ramadge's* and *Wonham's* supervisory control theory [Ram87, Ram89], we check whether the control problem can be solved for the discrete abstraction: can we restrict the (l-complete) approximation behaviour to a set of "acceptable" trajectories? If this is the case, the least restrictive 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 organized as follows: in Section 2, we introduce l-complete approximations. In Section 3, we show how to determine the strongest l-complete approximation for a given hybrid system, and in Section 4, we apply supervisory control theory to find the maximally permissive feedback controller for this approximation. Finally, in Section 5, it is shown that this controller also solves the problem for the underlying hybrid system.

2 l-Complete approximations

We propose an approximation scheme that 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 [Wi91], 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*.*

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 [Wi91], Def. II.3) A dynamical system* $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$ *is said to be* time invariant *if* $\sigma\mathfrak{B} \subseteq \mathfrak{B}$*.*

© 1998 IEE, WODES98 – Cagliari, Italy
Proc. of the Fourth Workshop on Discrete Event Systems

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 [Wi91], 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: $\sigma^t w|_{[0,l]} = (\sigma^t w)|_{[0,l]} = w|_{[t,t+l]}$.

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 4 *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:*

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

(ii) $\mathfrak{B}'_l \supseteq \mathfrak{B}$*,* $\mathfrak{B}'_l$ *is l-complete* $\quad\Rightarrow\quad \mathfrak{B}'_l \supseteq \mathfrak{B}_l$.

The motivation for Definition 4 is the following: we want to synthesize supervisory control for Σ on the basis of the approximation Σ_l. Clearly, we need condition (i) to hold; otherwise, $\mathfrak{B}$ could contain unacceptable trajectories which could not be predicted by the approximation Σ_l and hence not be suppressed by a control strategy based on the approximate model. It is also obvious that we want condition (ii) 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 1 *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:*

$$\mathfrak{B}_l = \{w|\ w \in W^T,\, \sigma^t w\big|_{[0,l]} \in \mathfrak{B}\big|_{[0,l]}\ \forall\, t \in \mathbb{N}_0\}. \tag{2}$$

Proof: Uniqueness follows immediately from the definition. To prove existence, take $\mathfrak{B}_l$ as defined by (2) and check conditions (i) and (ii). Σ is time invariant, hence $w \in \mathfrak{B} \Rightarrow \sigma^t w|_{[0,l]} \in \mathfrak{B}|_{[0,l]}$ for all $t \in \mathbb{N}_0$, and therefore $\mathfrak{B}_l \supseteq \mathfrak{B}$. l-completeness of $\mathfrak{B}_l$ is obvious, hence (i) 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 (2), 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 1 is an immediate consequence of equation (2):

Corollary 1 *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,*

(i) $\mathfrak{B}_l\big|_{[0,l]} = \mathfrak{B}\big|_{[0,l]}$,

(ii) $\mathfrak{B}_l \supseteq \mathfrak{B}_{l+1} \supseteq \mathfrak{B}$,

(iii) $\Sigma_l = \Sigma \quad\Leftrightarrow\quad \Sigma$ *is l-complete.*

The following definition provides a link between standard terminology from the field of DES (discrete event systems) and the behavioural approach.

Definition 5 *Let the sets $W,\ Z,\ Z_0 \subseteq Z,\ \delta \subseteq Z \times W \times Z$ denote the* external signal space*, the* state space*, the* set of initial conditions *and the* next state relation *respectively. The pair $P = (Z_0,\, \delta)$ is called a* state machine*. If $|W| \in \mathbb{N}$ and $|Z| \in \mathbb{N}$ (both sets are finite), P is said to be a* finite state machine*. The behaviour $\mathfrak{B}_s := \{(w, z)|\ (z(t),\, w(t),\, z(t+1)) \in \delta\ \forall\ t \in \mathbb{N}_0,\ z(0) \in Z_0\}$ is referred to as the induced (full) behaviour, and $\Sigma_s := (\mathbb{N}_0,\, W \times Z,\, \mathfrak{B}_s)$ 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 $W^{\mathbb{N}_0}$, that is $\mathfrak{B}_{ex} := \mathcal{P}_W\, \mathfrak{B}_s := \{w|\ \exists\, z :\ (w, z) \in \mathfrak{B}_s\}$. Vice versa P is said to be a realization of a system $\Sigma = (\mathbb{N}_0,\, W,\, \mathfrak{B})$ if $\mathfrak{B} = \mathfrak{B}_{ex}$. This is denoted by $\Sigma \cong P$.*

In order to construct a realization of Σ_l we set up a suitable state space Z and a next state relation δ_l. The procedure is based on memorizing the last l external signals $(w(t-l),\, \dots\ w(t-1))$ as state $z(t) \in Z$ at time $t \geq l$, similar to [Wi89], section 2.4.9. Since our time axis is $\mathbb{N}_0$ we need to take into account the effect of shorter strings for $t < l$.

$$Z := \{w^\star\} \bigcup_{1 \leq r \leq l} W^r, \quad Z_0 = \{w^\star\}\ , \tag{3}$$

where $w^\star \notin W$ is a new "dummy" symbol meaning "no external signal present so far". The next state relation is given by:

$$\delta_l := \bigcup_{0 \leq r \leq l} \delta_l^r \subseteq Z \times W \times Z\ , \tag{4}$$

where

$$\delta_l^0 := \{(w^\star,\, w_0,\, w_0)|\ w_0 \in \mathfrak{B}|_{[0,0]}\}\,, \tag{5}$$

$$\begin{aligned}\delta_l^r := \{((w_0, \ldots\ w_{r-1}),\, w_r,\, (w_0, \ldots\ w_r))|\\ (w_0, \ldots\ w_r) \in \mathfrak{B}|_{[0,r]}\}\ ,\ 1 \le r < l,\end{aligned} \tag{6}$$

$$\begin{aligned}\delta_l^l := \{((w_0, \ldots\ w_{l-1}),\, w_l,\, (w_1, \ldots\ w_l))|\\ (w_0, \ldots\ w_l) \in \mathfrak{B}|_{[0,l]}\}\ .\end{aligned} \tag{7}$$

Theorem 1 *Let Σ_l be the strongest l-complete approximation induced by the time invariant dynamical system $\Sigma = (\mathbb{N}_0,\, W,\, \mathfrak{B})$. Then Σ_l is realized by the finite state machine $P_l := (Z_0,\, \delta_l)$, defined by equations* (3) – (7)*.*

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

$$z(t) := \begin{cases} w^\star \text{ if } t = 0, \\ (w(0), \ldots, w(t-1)) \text{ if } 0 < t < l, \\ (w(t-l), \ldots, w(t-1)) \text{ if } t \ge l. \end{cases} \tag{8}$$

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' such that $(w,\, z') \in \mathfrak{B}_{s,l}$. From the definition of δ_l it follows by induction that $z = z'$ and therefore $(z(t),\, w(t),\, z(t+1)) \in \delta_l$ for all $t \in \mathbb{N}_0$. Furthermore, the definition of δ_l implies $(z(t), w(t)) \in \mathfrak{B}|_{[0,l]}$ for all $t \ge l$. Observe that by Corollary 1, part (i), and by equation (8), $w|_{[t-l,t]} = (z(t), w(t)) \in \mathfrak{B}|_{[0,l]} = \mathfrak{B}_l|_{[0,l]}$ for all $t \ge l$. Since $\mathfrak{B}_l$ is l-complete, this implies $w \in \mathfrak{B}_l$. We now assume $w \in \mathfrak{B}_l$. It is obvious that $(z(t),\, w(t),\, z(t+1)) \in \delta_l$ for all $t \in \mathbb{N}_0$, and $z(0) = w^\star \in Z_0$. Hence $(w, z) \in \mathfrak{B}_{s,l}$ and therefore $w \in \mathfrak{B}_{ex,l}$. ■

3 Hybrid state space 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 discrete (i.e. W is finite), 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 6 *Let W, X and δ with $|W| \in \mathbb{N}$, $X = \mathbb{R}^n \times D$, $|D| \in \mathbb{N}$, and $\delta \subseteq X \times W \times X$ denote an external signal space, a state space and a next state relation respectively. Then the state machine $P = (X,\, \delta)$ is said to be a* hybrid state machine*. Let $\mathfrak{B}_s$ denote the the full behaviour induced by P. Then the system $\Sigma_s = (\mathbb{N}_0,\, W \times X,\, \mathfrak{B}_s)$ is called the* hybrid state space system *induced by P.*

Since the external behaviour $\mathfrak{B} = \mathcal{P}_W\, \mathfrak{B}_s$ induced by P is time invariant, we can approximate $\Sigma = (\mathbb{N}_0,\, W,\, \mathfrak{B})$ 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 complete by definition, we cannot expect $\mathfrak{B}$ to possess any completeness property. 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 hence amenable to standard methods from the field of DES theory.

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

Definition 7 *For a given hybrid state machine P in the notation of Definition 6 with induced external behaviour $\mathfrak{B}$, let $\mathcal{X}_l^t(\bar{w}|_{[0,l]}) \subseteq X$ denote the set of all states at time t ($t \le l$) that are compatible with $\bar{w}|_{[0,l]} \in W^{l+1}$:*

$$\mathcal{X}_l^t(\bar{w}|_{[0,l]}) := \\ \{\xi|\ \exists (w,\, x) \in \mathfrak{B}_s :\ x(t) = \xi,\ w|_{[0,l]} = \bar{w}|_{[0,l]}\}\,. \tag{9}$$

If the hybrid system is state trim ($\forall\ \xi \in X\ \exists (w,\, x) \in \mathfrak{B}_s,\ t \in \mathbb{N}_0 :\ x(t) = \xi$; see [Wi91], page 270), the sets of compatible states can be derived by a recursive formula, given in the following proposition. Note that in state machine terminology "state trimness of Σ_s" is equivalent to "P being temporally nonblocking", since the set of initial conditions in P happens to be the entire state space. See Definition 10.

Proposition 2 *For any given state trim hybrid system in the notation of Definition 6 and any trajectory $\bar{w} \in W^{\mathbb{N}_0}$, the following holds:*

$$\mathcal{X}_0^0(\bar{w}|_{[0,0]}) = \\ \{\xi|\ \exists \xi^+ \in X :\ (\xi,\, \bar{w}(0),\, \xi^+) \in \delta\}\ , \tag{10}$$

$$\mathcal{X}_{l+1}^{l+1}(\bar{w}|_{[0,l+1]}) = \\ \{\xi|\ \exists \xi^- \in \mathcal{X}_l^l(\bar{w}|_{[0,l]}) :\ (\xi^-,\, \bar{w}(l),\, \xi) \in \delta\} \\ \cap \mathcal{X}_0^0(\bar{w}(l+1))\ . \tag{11}$$

Proof: It is obvious that any ξ in one of the left hand side sets in (10) and (11) 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 equation (10). State trimness implies that there exist trajectories $(w^+,\, x^+) \in \mathfrak{B}_s$, $x^+(0) = \xi^+$ and $(w^-,\, x^-) \in \mathfrak{B}_s$, $x^-(0) = \xi$, $w^-(0) = \bar{w}(0)$. Let $x(t) := x^+(t-1)$, $w(t) := w^+(t-1)$ for all $t \ge 1$, and $x(0) := x^-(0)$, $w(0) := w^-(0)$. Then, $(x(t),\, w(t),\, x(t+1)) \in \delta$ for all $t \in \mathbb{N}_0$. Hence $(w,\, x) \in \mathfrak{B}_s$, and therefore $\xi = x(0) \in \mathcal{X}_0^0(\bar{w}|_{[0,0]})$, yielding equation (10).

Now, pick any ξ from the right hand side set in equation (11). As $\xi^- \in \mathcal{X}_l^l(\bar{w}|_{[0,l]})$, 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 $\xi \in \mathcal{X}_0^0(\bar{w}(l+1))$, there exists a trajectory $(w^+, x^+) \in \mathfrak{B}_s$ such that $x^+(0) = \xi$ and $w^+(0) = \bar{w}(l+1)$. Completely analogous to the previous case, we construct a trajectory $(w, x) \in \mathfrak{B}_s$ by concatenating $(w^-, x^-)|_{[0,l]}$ and (w^+, x^+). This yields $\xi \in \mathcal{X}_{l+1}^{l+1}(\bar{w}|_{[0,l+1]})$. Hence, it has been shown that Equation (11) holds. ■

We still need to show how sets of compatible (hybrid) states are linked to the (discrete) next state relation δ_l:

Theorem 2 *Let $\Sigma_s = (\mathbb{N}_0, W \times X, \mathfrak{B}_s)$ be a hybrid state space system in the notation of Definition 6 with external behaviour $\mathfrak{B} = \mathcal{P}_W \mathfrak{B}_s$. Let δ_l be defined by equations* (4) – (7)*. Then, for every triple $(z, w_0, z^+) \in Z \times W \times Z$, $z = (z_0, \dots z_{r-1})$, the following holds: $(z, w_0, z^+) \in \delta_l$ if and only if conditions (i) and (ii) are satisfied:*

(i) If $z = w^\star$ then $z^+ = w_0$.
If $z \neq w^\star$, $r < l$ then $z^+ = (z_0, \dots z_{r-1}, w_0)$.
If $r = l$ then $z^+ = (z_1, \dots z_{l-1}, w_0)$.

(ii) If $z = w^\star$ then $\mathcal{X}_0^0(w_0) \neq \emptyset$.
If $z \neq w^\star$ then $\mathcal{X}_r^r((z_0, \dots z_{r-1}, w_0)) \neq \emptyset$.

Proof: First assume $(z, w_0, z^+) \in \delta_l$. Condition (i) then obviously holds. Furthermore, there exists $w \in \mathfrak{B}$ such that $w|_{[0,r]} = (z_0, \dots z_{r-1}, w_0)$. Since $\mathfrak{B}$ is the external behaviour of $\mathfrak{B}_s$, there exists an $x \in X^T$ such that $(w, x) \in \mathfrak{B}_s$. Therefore $\mathcal{X}_r^r((z_0, \dots z_{r-1}, w_0))$ cannot be empty, hence condition (ii) holds. Vice versa assume conditions (i) and (ii) to hold for a fixed $(z, w_0, z^+) \in Z \times W \times Z$. Now (ii) implies existence of a trajectory $(w, x) \in \mathfrak{B}_s$ such that $w|_{[0,r]} = (z_0, \dots z_{r-1}, w_0)$. Observing $w \in \mathcal{P}_W \mathfrak{B}_s = \mathfrak{B}$ together with condition (i) yields $(z, w_0, z^+) \in \delta_l$. ■

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

$$W = U \times Y \ , \quad |U| \in \mathbb{N} \ , |Y| \in \mathbb{N} \ , \tag{12}$$

$$f \colon X \times U \to X \ , \quad g \colon X \to Y \ , \tag{13}$$

$$\delta := \{(\xi, (\nu, \mu), \xi^+) |\ \xi^+ = f(\xi, \nu),\ \mu = g(\xi)\} \, . \tag{14}$$

Since the time axis is $\mathbb{N}_0$, state trimness is guaranteed. Essentially, these are the same assumptions as in [Rai97]. Indeed, the strongest l-complete approximation Σ_l induced by this hybrid system turns out to be equivalent – up to a minor difference in the definition of z – to the "discrete abstraction A_{l+1}" defined in [Rai97], or the "abstraction A_l" in [Rai98a]. Furthermore, Σ_l is similar to the "condensed model of order l" as proposed in [Mo98], where the (more restrictive) class of switched-integrator-systems is discussed. In our framework, Proposition 2 yields for any $u \in U^{\mathbb{N}_0}$, $y \in Y^{\mathbb{N}_0}$:

$$\mathcal{X}_0^0((u, y)\big|_{[0,0]}) = g^{-1}(y(0)) \ , \tag{15}$$

$$\mathcal{X}_{l+1}^{l+1}((u, y)\big|_{[0,l+1]}) = f(\mathcal{X}_l^l((u, y)\big|_{[0,l]}), u(l)) \cap g^{-1}(y(l+1)) \ . \tag{16}$$

Whenever one is able to repeatedly compute images under $f(\,\cdot\,, \nu)$ for fixed $\nu \in U$, 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.

Before using the strongest l-complete approximation Σ_l for the purposes of supervisory control synthesis, we summarize the proposed abstraction procedure: our starting point is a hybrid state machine $P = (X, \delta)$. This induces the (full) behaviour $\mathfrak{B}_s$ and the (discrete) external behaviour $\mathfrak{B} = \mathcal{P}_W \mathfrak{B}_s$. First, choose an $l \in \mathbb{N}$ and compute the sets of compatible states $\mathcal{X}_r^r(\hat{w}|_{[0,r]})$ for all strings $\hat{w}|_{[0,r]}$, $r \leq l$. This can be done by a recursive formula as stated in Proposition 2. Then, the (purely discrete) next state relation δ_l is set up according to Theorem 2. From Theorem 1, we know that $P_l = (Z_0, \delta_l)$ is a realization of the strongest l-complete approximation Σ_l induced by $\Sigma = (\mathbb{N}_0, W, \mathfrak{B})$, hence $\mathfrak{B}_l \supseteq \mathfrak{B}$. Recall that the latter is a necessary condition if controller synthesis for Σ is to be based on Σ_l.

4 Supervisory Control

Roughly speaking, a supervisor's task is to prevent the (hybrid) system $\Sigma = (T, W, \mathfrak{B})$ from evolving on trajectories which are deemed to be unacceptable – the supervisor is meant to suitably restrict the behaviour $\mathfrak{B}$. The mechanism of interaction is to stop $w(t)$ from taking certain values in W. However, only a subset W_c of elements in W can be "disabled", or controlled, by the supervisor, whereas elements in $W_{uc} := W \setminus W_c$ cannot be prevented from happening. Moreover, we need to take into account that, in general, it will not be possible to disable all elements in W_c independently: the set W_c is partitioned into disjoint subsets W_c^i, $i = 1, \dots, p$,

$$W_c = \bigcup_{i=1}^{p} W_c^i, \ W_c^i \cap W_c^j = \emptyset \text{ for } i \neq j, \tag{17}$$

where either all elements in W_c^i are disabled simultaneously, or all of them are allowed to occur.

Our solution procedure is as follows: we first synthesize a supervisor for an l-complete approximation $\Sigma_l = (\mathbb{N}_0, W, \mathfrak{B}_l)$ of Σ by employing a modified version of *Ramadge*'s and *Wonham*'s theory; a version similar to the one presented here has been described in [Rai98b]. Then, we show that the supervisor obtained for Σ_l does indeed solve the problem for the underlying hybrid system Σ.

In this section, the time axis $\mathbb{N}_0$ is interpreted to be "clock time". To keep notation as simple as possible, we assume that the acceptable behaviour is defined on the same signal space W as $\mathfrak{B}$ and $\mathfrak{B}_l$. Hence, the acceptable behaviour is characterized by a system $\Sigma_{spec} = (\mathbb{N}_0, W, \mathfrak{B}_{spec})$, which we assume to be realized by a finite state machine P_{spec}, $\Sigma_{spec} \cong P_{spec}$, with state set X_{spec}, next state relation δ_{spec}, and initial state set $X_{spec_0} \subseteq X_{spec}$.

Recall that Σ_l is realized by a finite state machine, denoted by $P_l = (Z_0, \delta_l)$, $\Sigma_l \cong P_l$. First, we formally remove all unacceptable trajectories by intersecting $\mathfrak{B}_l$ and $\mathfrak{B}_{spec}$. It is a well known fact that a realization for the intersection of two behaviours can be obtained by forming the parallel composition of the realizations of the two behaviours:

Fact 1 *Let P_l and P_{spec} be realizations of $\Sigma_l = (\mathbb{N}_0, W, \mathfrak{B}_l)$ and $\Sigma_{spec} = (\mathbb{N}_0, W, \mathfrak{B}_{spec})$. Then,*

$$(\mathbb{N}_0, W, \mathfrak{B}_l \cap \mathfrak{B}_{spec}) \cong P_l \parallel P_{spec}, \qquad (18)$$

where the parallel composition of P_l and P_{spec} is defined by $P_l \parallel P_{spec} := (Q_0, \lambda)$, and the set Q_0 of initial states is given by

$$Q_0 := Z_0 \times X_{spec_0} \subseteq Z \times X_{spec} := Q\,,$$

and the next state relation $\lambda \subseteq Z \times X_{spec} \times W \times Z \times X_{spec}$ is defined by

$$\begin{aligned} &((z, x_{spec}), w, (z', x'_{spec})) \in \lambda \\ &\Leftrightarrow (z, w, z') \in \delta_l \text{ and } (x_{spec}, w, x'_{spec}) \in \delta_{spec}\,. \end{aligned} \qquad (19)$$

Forming the parallel composition $P_l \parallel P_{spec}$ formally removes all transitions (elements in the next state relation) which violate the specifications – but this is done without caring for "implementability": we need to take into account that a transition (q, w, q') can only be eliminated if $w \in W_c$, that a symbol $w \in W_c^i$ can only be disabled if all other symbols in W_c^i are disabled simultaneously, and that a transition cannot be removed if that creates a deadlock situation – stopping time is impossible. The optimal supervisor's job can then be thought of as enforcing the "least restrictive" but implementable substructure of $P_l \parallel P_{spec}$. This is formalized in the following paragraph:

Definition 8 *Let $\lambda^1 = (q_1, w_1, q_1') \in \lambda$ and $\lambda^2 = (q_2, w_2, q_2') \in \lambda$. The transitions λ^1 and λ^2 are called* partners*, if $q_1 = q_2$ and $w_1, w_2 \in W_c^i$ for some W_c^i. $\tilde{P} = (\tilde{Q}_0, \tilde{\lambda})$ is called a* substructure *of $P_l \parallel P_{spec}$ (denoted by $\tilde{P} \subseteq P_l \parallel P_{spec}$), if $\tilde{\lambda} \subseteq \lambda$, $\tilde{Q}_0 \subseteq Q_0$, and a transition $\lambda^i \in \lambda$ can only be an element in $\tilde{\lambda}$, if all its partners are also contained in $\tilde{\lambda}$.*

A state $q_2 \in \tilde{Q}$ is *reachable from a state* $q_1 \in \tilde{Q}$, if there is a sequence of transitions from $\tilde{\lambda}$ connecting q_1 with q_2. q_2 is *reachable* if it is reachable from an initial state $q_1 \in \tilde{Q}_0$. $\tilde{P}$ is called *reachable* if all states $q_2 \in \tilde{Q}$ are reachable.

Definition 9 *Let $W_c \subseteq W$ be the set of transition labels of P_l (and hence $P_l \parallel P_{spec}$) which can be disabled by a control agent. Let $\tilde{P} = (\tilde{Q}_0, \tilde{\lambda})$ be a reachable substructure of $P_l \parallel P_{spec}$ with state set $\tilde{Q}$ and with $\tilde{Q}_0 = Q_0$. Then $\tilde{P}$ is said to be* controllable w.r.t. to P_l, *if $(z, w, z') \in \delta_l$ (the next state relation of P_l), $(z, x_{spec}) \in \tilde{Q}$, and $((z, x_{spec}), w, -) \notin \tilde{\lambda}$ implies that $w \in W_c$ ($-$ means "don't care").*

Clearly, a substructure $\tilde{P}$ of $P_l \parallel P_{spec}$ can only be implemented by a supervisor if it is controllable w.r.t. P_l. Another condition for implementability is that the progress of time can never be stopped:

Definition 10 *A substructure $\tilde{P}$ of $P_l \parallel P_{spec}$ with state set $\tilde{Q}$ and next state relation $\tilde{\lambda}$ is called* temporally nonblocking, *if for every reachable state $q \in \tilde{Q}$ there exists $w \in W$, $q' \in \tilde{Q}$ such that $(q, w, q') \in \tilde{\lambda}$.*

Let $\tilde{P}_1 = (\tilde{Q}_{1_0}, \tilde{\lambda}_1)$ and $\tilde{P}_2 = (\tilde{Q}_{2_0}, \tilde{\lambda}_2)$ be two substructures of $P_l \parallel P_{spec}$. Then the *union* of $\tilde{P}_1$ and $\tilde{P}_2$ is defined as

$$\tilde{P}_1 \cup \tilde{P}_2 := (\tilde{Q}_{1_0} \cup \tilde{Q}_{2_0}, \tilde{\lambda}_1 \cup \tilde{\lambda}_2). \qquad (20)$$

It is immediately clear that $\tilde{P}_1 \cup \tilde{P}_2$ is another substructure of $P_l \parallel P_{spec}$. The relation $\subseteq$ induces a partial ordering on the set of all substructures of $P_l \parallel P_{spec}$.

Lemma 1 *Let $\{\tilde{P}_{CN}\}$ be the set of all substructures of $P_l \parallel P_{spec}$ which are controllable w.r.t P_l and temporally nonblocking. $\{\tilde{P}_{CN}\}$ is closed under union.*

Proof: Let $\tilde{P}_1$ and $\tilde{P}_2$ be two substructures of $P_l \parallel P_{spec}$ with state sets $\tilde{Q}_1$, $\tilde{Q}_2$, and next state relations $\tilde{\lambda}_1$ and $\tilde{\lambda}_2$, respectively. Let both $\tilde{P}_1$ and $\tilde{P}_2$ be controllable w.r.t. P_l. Assume (z, x_{spec}) is in the state set of $\tilde{P}_1 \cup \tilde{P}_2$, $(z, w, z') \in \delta_l$, but $((z, x_{spec}), w, -) \notin \tilde{\lambda}_1 \cup \tilde{\lambda}_2$. Then either $(z, x_{spec}) \in \tilde{Q}_1$ and $((z, x_{spec}), w, -) \notin \tilde{\lambda}_1$, or $(z, x_{spec}) \in \tilde{Q}_2$ and $((z, x_{spec}), w, -) \notin \tilde{\lambda}_2$. In both cases, $w \in W_c$, as both $\tilde{P}_1$ and $\tilde{P}_2$ are controllable w.r.t. P_l. Hence, $\tilde{P}_1 \cup \tilde{P}_2$ is controllable w.r.t. P_l. Now, assume that both $\tilde{P}_1$ and $\tilde{P}_2$ are temporally nonblocking. Let q be any element in the state set of $\tilde{P}_1 \cup \tilde{P}_2$. Then either $q \in \tilde{Q}_1$, hence $\exists\, w \in W$ and $q' \in \tilde{Q}_1$ such that $(q, w, q') \in \tilde{\lambda}_1$ or $q \in \tilde{Q}_2$, hence $\exists\, w \in W$ and $q' \in \tilde{Q}_2$ such that $(q, w, q') \in \tilde{\lambda}_2$. Existence of a $(q, w, q') \in \tilde{\lambda}_1 \cup \tilde{\lambda}_2$ is therefore guaranteed, and $\tilde{P}_1 \cup \tilde{P}_2$ is temporally nonblocking. ■

Hence, if non-empty, $\{\tilde{P}_{CN}\}$ forms an upper-semilattice (with the join operation being $\cup$). Clearly, $\{\tilde{P}_{CN}\}$ is finite. Therefore, the following holds:

Corollary 2 *If $\{\tilde{P}_{CN}\}$ is non-empty, there exists a (unique) greatest substructure of $P_l \parallel P_{spec}$ (w.r.t. the ordering via $\subseteq$) which is controllable w.r.t. P_l and temporally nonblocking.*

If $\{\tilde{P}_{CN}\}$ is non-empty, denote its supremal element by $P_{sup} = (Q_{sup_0}, \lambda_{sup})$. It can be interpreted as the transition structure of $P_l \parallel P_{spec}$ that survives under the least restrictive implementable supervisory control policy which guarantees the specifications to be met. It can also be interpreted as a realization of the supervisor, which, at every state $q \in Q_{sup}$, disables certain symbols from $W_c \subseteq W$. Denote the dynamical system induced by P_{sup} by $\Sigma_{sup} = (\mathbb{N}_0, W, \mathfrak{B}_{sup})$, $\Sigma_{sup} \cong P_{sup}$. By construction,

$$\emptyset \subset \mathfrak{B}_{sup} \subseteq \mathfrak{B}_l \cap \mathfrak{B}_{spec}. \tag{21}$$

P_{sup} can be formally synthesized via a fixed-point algorithm in a computer-aided design environment. This procedure has been coded in C++ with an object oriented architecture [O'Y98].

If $\{\tilde{P}_{CN}\}$ is empty, the supervisory control problem has no solution. This implies that either the strongest l-complete approximation Σ_l is too coarse, or the specifications are too strict (they cannot be met no matter how accurate our approximation is) and need to be relaxed. In the former case, we need to provide a finer approximation: we can try the strongest k-complete approximation Σ_k, $k > l$, which, by Corollary 1, is guaranteed to be at least as accurate as Σ_l.

5 Applying supervisory control to Σ

We still need to answer the following question: what is going to happen when we "connect" the supervisory controller $\Sigma_{sup} = (\mathbb{N}_0, W, \mathfrak{B}_{sup}) \cong P_{sup}$ to the underlying (hybrid) system $\Sigma = (\mathbb{N}_0, W, \mathfrak{B}) \cong P$? In the behavioural framework, connecting two systems amounts to intersecting their behaviours. The closed loop behaviour $\mathfrak{B}_{cl}$ is therefore $\mathfrak{B}_{cl} = \mathfrak{B} \cap \mathfrak{B}_{sup}$. Hence, the parallel composition $P_{sup} \parallel P$ is a realization of the closed loop system $\Sigma_{cl} = (\mathbb{N}_0, W, \mathfrak{B}_{cl})$. As $\mathfrak{B} \subseteq \mathfrak{B}_l$ (Corollary 1) and $\mathfrak{B}_{sup} \subseteq \mathfrak{B}_{spec}$ (equation (21)), this implies that the system Σ under supervision P_{sup} will not exhibit any unacceptable behaviour:

$$\mathfrak{B}_{cl} \subseteq \mathfrak{B}_{spec}. \tag{22}$$

Since the supervisor is still not able to stop time, we need to ensure that the parallel composition $P_{sup} \parallel P$ is temporally nonblocking. To do this, we need to impose additional structure on Σ: we could, for example, restrict ourselves to the class of strictly nonanticipating hybrid systems defined in (12) - (14). Then, $W_c = W = \{(u_i, y_j),\ i = 1, \dots |U|,\ j = 1, \dots |Y|\}$ and $W_c^i = \{(u_i, y_j),\ j = 1, \dots |Y|\}$, i.e. the supervisor can disable all "control symbols" $u_i \in U$ independently. Since the supervisor is temporally nonblocking by construction, for every state (z, x_{spec}) reachable from an initial state, at least one partition W_c^i of external symbols is allowed to occur. Now observe from equations (12) - (14) that for every hybrid state $\xi \in X$ there exists $w \in W_c^i$ and $\xi^+ \in X$ such that $(\xi, w, \xi^+) \in \delta$. Hence, the parallel composition $P_{sup} \parallel P$ indeed is temporally nonblocking.

6 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 find the strongest l-complete approximation for the hybrid system; this approximation can be represented by a finite state machine; hence slightly modified tools from DES theory can be applied 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.

References

[Lu94] Lunze, J.: Qualitative modelling of linear dynamical systems with quantized state measurements, *Automatica*, Vol. 30, pp. 417–431, 1994.

[Mo98] Moor, T.: Event driven control of switched-integrator-systems, *Proc. ADPM98*, pp. 271-277, Reims, March 1998.

[O'Y98] O'Young, S. D.: Hybrid RTSS, *Internal Report, Faculty of Engineering, Memorial University of Newfoundland*, 1998.

[Rai97] 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, Vol. 1273, pp. 342-360, 1997.

[Rai98a] Raisch, J.: A hierarchy of discrete abstractions for a given hybrid plant, *Proc. ADPM98*, pp. 55-62, Reims, March 1998.

[Rai98b] Raisch, J., O'Young, S. D.: Discrete approximation and supervisory control of continuous systems, *IEEE Transactions on Automatic Control, Special issue on hybrid systems*, Vol. 43, April 1998.

[Ram87] Ramadge, P. J., Wonham, W. M.: Supervisory control of a class of discrete event systems, *SIAM J. Control and Optimization*, Vol. 25, pp. 206–230, 1987.

[Ram89] Ramadge, P. J., Wonham, W. M.: The control of discrete event systems, *Proceedings of the IEEE*, Vol. 77, pp. 81–98, 1989.

[Wi89] Willems, J. C.: Models for dynamics, *Dynamics Reported*, Vol. 2, pp. 172-269, 1989.

[Wi91] 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.