Discrete Event Dynamic Systems: Theory and Applications, 14, 203–238, 2004

Compositional Abstractions of Hybrid Control Systems

PAULO TABUADA ptabuada@nd.edu
Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN 46556

GEORGE J. PAPPAS
Department of Electrical and Systems Engineering, University of Pennsylvania, Philadelphia, PA 19104

PEDRO LIMA
Institute for Systems and Robotics, Instituto Superior Técnico, Lisbon, Portugal

Abstract. Abstraction is a natural way to hierarchically decompose the analysis and design of hybrid systems. Given a hybrid control system and some desired properties, one extracts an abstracted system while preserving the properties of interest. Abstractions of purely discrete systems is a mature area, whereas abstractions of continuous systems is a recent activity. In this paper we present a framework for abstraction that applies to discrete, continuous, and hybrid systems. We introduce a composition operator that allows to build complex hybrid systems from simpler ones and show compatibility between abstractions and this compositional operator. Besides unifying the existing methodologies we also propose constructions to obtain abstractions of hybrid control systems.

Keywords: hybrid systems, compositionality, abstractions

1. Introduction

In the last decade, increasing attention has been paid to the modeling, analysis and control of large-scale, multi-agent, complex, hybrid systems. The impulse from the applications side has been tremendous and includes among others: automotive engines (Balluchi et al., 2000a,c), air-traffic management (Tomlin et al., 1998), chemical batch plants (Niebert and Yovine, 2000), manufacturing systems (Gokbayrak and Cassandras, 2000), TCP congestion control (Hespanha et al., 2001) and biomolecular networks (Alur et al., 2001).

One approach to deal with the inherent complexity of hybrid control systems is to organize them in a hierarchical framework where different layers of abstraction represent different aspects of the same system. Analysis tasks are performed on simpler, abstracted models that are equivalent with respect to the relevant properties. Synthesis tasks also benefit from this approach since the design starts at the top of the hierarchy on a simple model and is then successively refined by incorporating the modeling details of each layer of abstraction.

The notion of abstraction is quite mature in theoretical computer science, and, in particular, in the areas of concurrency theory (Milner, 1989; Winskel and Nielsen, 1994), and computer aided verification (Manna and Pnueli, 1995). This has resulted in formal and very meaningful notions of abstraction which are used to tackle exponential explosion of purely discrete systems. Given a discrete system, an abstraction is simply a quotient system

that preserves some properties of interest while ignoring detail. Language equivalence, simulation, and bisimulation are established notions of abstraction for discrete systems that preserve properties expressed in various temporal logics (Manna and Pnueli, 1992).

For purely continuous systems, the notions of abstraction, simulation, and bisimulation had no counterparts. Recently, similar notions were introduced in the collection of papers (Pappas et al., 2000; Pappas and Simic, 2002; Pappas, 2003; Tabuada and Pappas, 2002a,b). This research resulted in automatic constructions of abstractions for linear control systems (Pappas et al., 2000), while characterizing abstracting maps that preserve properties of interest such as controllability. Such notions were furthermore generalized for nonlinear control affine systems (Pappas and Simic, 2002) and fully nonlinear systems (Tabuada and Pappas, 2002b). Notions of bisimulation for purely continuous control systems were introduced in Pappas (2003) where linear control systems are embedded in the class of transition systems for which the notion of bisimulation was originally introduced in Park (1980) and also Milner (1989). It is shown in Pappas (2003) that different embeddings give rise to semantically different notions of bisimulation being characterized by different conditions. For nonlinear systems, a notion of bisimulation was introduced in Tabuada and Pappas (2002a) and it was shown that under certain conditions the abstractions described in Pappas and Simic (2002) are in fact bisimulations.

The notion of bisimulation has also proved useful in the context of control of discrete event systems. In Barret and Lafortune (1998) the relation between bisimulation, supervisory control of discrete event systems and model matching problems is clarified. Furthermore, it is shown how recasting supervisory control problems for discrete event systems as a bisimulation problem leads to more efficient algorithms. In Madhusudan and Thiagarajan (2002), bisimulation is fundamentally used at the level of the problem formulation by requiring the closed loop system to simulate or bisimulate the specification.

Based on these results, in Tabuada and Pappas (2001), we took the first steps towards constructing abstractions of hybrid systems while preserving timed languages. Even though only the continuous part of the system was abstracted, the important property that needed to be preserved in this abstraction was the detectability of the discrete switching conditions. Related but orthogonal work considers purely discrete abstractions of hybrid systems (Alur et al., 2000; Caines and Wei, 1998; Cury et al., 1998; Raisch and O'Young, 1998).

The similarities between notions of abstraction for discrete, continuous, and hybrid systems immediately raise the question of a more unified theory of abstraction. In this paper, we begin addressing this important issue. We start by first considering a more unified and abstract model for control systems. Our abstract control systems model is inspired by categorical definitions of systems that are as old as Arbib and Manes (1974), Ramadge and Wonham (1982) and as recent as Rutten (2000). Although categorically inspired, the paper is accessible to readers that are not familiar with category theory, except for some proofs that rely on simple category theory notions.

We show that purely discrete, continuous, and hybrid systems can be easily captured by our categorical model. Furthermore, using this model, one can show many useful properties regarding abstraction or composition that are independent of the discrete, continuous, or hybrid nature of the system.

As abstraction clearly depends on the property to be preserved, in this paper, we focus

on simulations and bisimulations as a convenient formalism leading to language equivalence and containment. In other words, given an original hybrid control system and an abstracting map, which performs state aggregation, we would like to extract another hybrid control system which simulates all trajectories of the original system. This is clearly useful for verification purposes since in order to determine if a system satisfies certain properties it is sufficient to check if its abstraction verifies the desired properties. However in many situations one needs lower complexity models that are both sufficient and necessary. This motivates the need for bisimulations which are symmetric simulation relations.

We also introduce an abstract operator that allows to built systems by interconnection of subsystems. This compositional operator, based on the categorical ideas in Winskel and Nielsen (1994), turns out to be compatible with simulations and even with bisimulations in certain cases. Compatibility means that instead of computing an abstraction of a complex large-scale system one can compute abstractions of the subsystems and is guaranteed that the interconnection of those abstractions is an abstraction of the original large-scale system. Our composition operator differs from the approaches described in Lynch et al. (2001), Alfaro and Henzinger (2001), in that we model synchronization by restricting the behavior of the systems without a priori defining inputs and outputs or internal and external variables and actions.

We specialize the developed results for hybrid systems, presenting a construction to obtain abstractions of hybrid control systems. Furthermore, we also provide sufficient conditions for the resulting abstraction to be a bisimulation of the original system. These results are then illustrated in a concrete application. We consider the hybrid model of a spark ignition engine described in Balluchi et al. (2000b) and show how our methods can be applied to obtain a smaller abstract model.

The structure of this paper is as follows:

In Section 2, an abstract notion of control systems which captures discrete, continuous, and hybrid control systems is introduced as well as a notion of abstraction and bisimulation. It is also shown how these notions can be used for verification of reachability based properties. Compositionality is discussed in Section 3 by introducing the notion of parallel composition with synchronization and showing how abstractions and bisimulations preserve this composition operator. In Section 4, we specialize these results to hybrid control systems, and present a construction to obtain abstractions of hybrid control systems that simulate the trajectories of the original system. The proposed methodology is illustrated with a spark ignition engine example in Section 5 and at Section 6 we list many interesting issues for future research. To keep the presentation of ideas fluid, we have collected some mathematical facts regarding partial maps and monoids in Appendix A, while in Appendix B we introduce the categorical notions of product and equalizer used in some of the proofs.

2. Abstract Control Systems

In this section, we seek to extract the essential features common to purely discrete and continuous systems that will allow to develop a fruitful theory of abstractions for hybrid

systems. This approach has the clear advantage of presenting in a unified way notions, results and algorithms common to discrete, continuous and hybrid control systems.

We start by recalling some known interpretations of continuous and discrete control systems to gain some motivation for the general definitions.

2.1. Discrete Control Systems

One of the usual models for discrete control systems are finite state automata (Cassandras and Lafortune, 1999; Kumar and Glerg, 1995), defined by a triple (Q, Σ, δ) where:

- Q is a finite set of states.
- Σ is a finite set of input symbols.
- $\delta : Q \times \Sigma \to Q$ is the next-state function.

We regard the partially defined map δ as defining the controlled dynamics, in the sense that for each $q \in Q$ there exists a set of choices (the elements $\sigma \in \Sigma$ such that $\delta(q, \sigma)$ is defined) that will influence the evolution of the state. This controlled evolution is usually modeled as a transition relation $\to \subseteq Q \times \Sigma \times Q$, but we will restrict our attention to deterministic[1] systems for which the relation $\to$ can be represented as a (partial) function δ.

We now look at finite state automata from a different but equivalent perspective. Let us denote by Σ^* the set of all finite strings obtained by concatenating elements in Σ. In particular, the empty string ε also belongs to Σ^*. Regarding concatenation of strings as a map from $\Sigma^* \times \Sigma^*$ to Σ^*, we can give Σ^* the structure of a monoid. Concatenation of strings is clearly an associative operation and the empty string ε can be taken as the monoid identity since it satisfies $s \cdot \varepsilon = \varepsilon \cdot s = s$ for any $s \in \Sigma^*$. We now recall from basic automata theory (Hopcroft and Ullman, 1979) that the transition function δ defines a unique partial map $\delta^* : Q \times \Sigma^* \to Q$ with the following properties:

$$\begin{aligned} \delta^*(q, \varepsilon) &= q \\ \delta^*(q, \sigma_1\sigma_2) &= \delta^*(\delta^*(q, \sigma_1), \sigma_2) \end{aligned}$$

These properties are in fact the definition of a monoid action, that is, δ^* is a (right) partially defined action of the monoid Σ^* on the set Q.

To clarify the similarities to the continuous case that we describe next, we elaborate a little on the structure of the monoid Σ^*. This monoid has been defined as the set of all finite sequences of elements in Σ. Alternatively, we can regard Σ^* as the disjoint union of all maps Σ^n, represented by:

$$\Sigma^* = \coprod_{n \in \mathbb{N}_0} \Sigma^n$$

Each set Σ^n, in the previous disjoint union, can be identified with the set of all maps from a set with n elements to Σ. In fact, choosing $\{1,2,3,\ldots,n\}$ as the set with n elements, we see that $(\sigma_1,\sigma_2,\sigma_3,\ldots,\sigma_n)\in\Sigma^n$ is simply the map $u\colon\{1,2,3,\ldots,n\}\to\Sigma$ defined by $u(i)=\sigma_i$ for $i=1,2,3,\ldots,n$. The empty string ε is identified with the (unique) map from the empty set to Σ. Concatenation of strings can now be seen as concatenation of maps defined as follows:

$$\begin{aligned}&\cdot : \Sigma^n\times\Sigma^m\to\Sigma^{n+m}\\ &(u(i),v(i))\mapsto(u\cdot v)(i)=\begin{cases}u(i) & \text{if } 1\le i\le n\\ v(i-n) & \text{if } n+1\le i\le n+m\end{cases}\end{aligned}\tag{1}$$

The above operation is well defined only if the number n is finite, otherwise we could not append the second map after the end of the first. Furthermore, as the concatenation $u\cdot v\in\Sigma^{n+m}$ must belong to Σ^* we need also to ensure that $n+m$ is finite which implies that m must also be finite. This shows that we are forced to work with finite length strings which will not be the case for continuous systems as we will see shortly.

2.2. *Continuous Control Systems*

For simplicity of presentation, we consider only time-invariant control systems, although the construction to be presented is generalizable to time varying systems. We assume also that the control systems satisfy the usual conditions for existence and uniqueness of solutions (Sontag, 1998). Consider a continuous control system, described by the triple (M,U,f), where:

- M is a smooth manifold modeling the state space.
- U is a smooth manifold modeling the input space.
- $f\colon M\times U\to TM$ is a smooth map assigning for each $u\in U$ the vector field $f(-,u)\colon M\to TM$.

Similarly to the discrete case, continuous control systems can also be understood by means of a monoid action. To reveal this fact, we define the set U^t as the set of all maps[2] from the interval $[0,t]$ to the space of inputs U:

$$U^t=U^{[0,t]}\quad [0,t]\subseteq\mathbb{R}_0^+\tag{2}$$

An element of U^t is denoted by u^t, and represents a map from $[0,t]$ to U. Consider now the set U^* which is the disjoint union of all U^t for $t\in\mathbb{R}_0^+$:

$$U^* = \coprod_{t \in \mathbb{R}_0+} U^t \tag{3}$$

The set U^* can also be regarded as a monoid under the operation of concatenation, that is, if $u^{t_1} \in U^{t_1} \subset U^*$ and $v^{t_2} \in U^{t_2} \subset U^*$ then $u^{t_1} v^{t_2} = w^{t_1+t_2} \in U^{t_1+t_2} \subset U^*$ with concatenation given by:

$$u^{t_1} v^{t_2}(t) = \begin{cases} u^{t_1}(t) & \text{if} \quad 0 \leq t < t_1 \\ v^{t_2}(t - t_1) & \text{if} \quad t_1 \leq t < t_1 + t_2 \end{cases} \tag{4}$$

The identity element is given by the empty input, that is $\varepsilon = u^0$. This construction is analogous to the construction that obtains Σ^* from Σ, however the fact that t_1 and t_2 are (finite) real numbers does not imply that u^{t_1} is a finite concatenation of elements in U^*. We can have an infinite number of concatenations as long as the sum of the duration times converges. This should be contrasted with the finite case, where a finite number of concatenations is required.

Choosing an admissible input trajectory u^t (an element of U^*), $f(x, u^t)$ is a well defined vector field and, as such, it induces a flow which we denote by $\gamma_x \colon [0, t] \to M$, satisfying $\gamma_x(0) = x$. We can then regard any smooth control system as a monoid action by defining:

$$\begin{aligned} &\Phi \colon M \times U^* \to M \\ &(x, u^t) \mapsto \gamma_x(t) \end{aligned} \tag{5}$$

It is not difficult to see that Φ is in fact a well-defined monoid action since

$$\Phi(x, \varepsilon) = \gamma_x(0) = x$$

and

$$\Phi(x, u^{t_1} u^{t_2}) = \gamma_x(t_1 + t_2) = \gamma_{\gamma_x(t_1)}(t_2) = \Phi(\Phi(x, u^{t_1}), u^{t_2})$$

It is interesting to note that when U is a singleton (there are no choices to be made) the set U^t can be identified[3] with the number t so that U^* is given by $U^* = \coprod_{t \in \mathbb{R}_0+} t = \mathbb{R}_0^+$ and our control system Φ degenerates into an action of $\mathbb{R}_0^+$ on M, that is, the solution of a differential equation (a degenerate control system).

2.3. Abstract Control Systems

Motivated by the previous examples, we are lead to consider monoid actions as good candidates for an abstract model of control systems. This is quite classic in the discrete case and has also been explored in Sontag (1998) for the continuous case. Recently, similar ideas have been used to lift several results from regular expressions to timed expressions

(Asarin et al., 2002). The fact that the same characterization also captures the hybrid case, is perhaps surprising, but motivates the need to formalize the discussion so far.

DEFINITION 2.1 (abstract control system) *An abstract control system is a triple* $(S, \mathscr{M}, \Phi)$*, where* S *is a set,* $\mathscr{M}$ *is a monoid and* Φ *is a (possibly partially defined) action of the monoid* $\mathscr{M}$ *on the set* S*, that is, a map* $\Phi\colon S \times \mathscr{M} \to S$ *satisfying:*

1. *Identity:* $\Phi(s, \varepsilon) = s$.

2. *Semi-group:* $\Phi(s, m_1 m_2) = \Phi(\Phi(s, m_1), m_2)$.

We will usually denote an abstract control system simply by Φ or Φ_S if we wish to emphasize the set S. We also represent by $s \xrightarrow{m} s'$ the evolution from s to s' controlled by m and described by Φ, that is, $\Phi(s, m) = s'$. We are now ready to see how the present formalism can also describe hybrid control systems.

2.4. Hybrid Control Systems as Abstract Control Systems

Hybrid control systems also fit in the previous abstract framework. The state space of a hybrid control system is usually described as $Q \times X$, where Q is a finite set of states and X a smooth manifold. However, it will be convenient to relax this concept, and consider a set of smooth manifolds X_q parameterized by the discrete states, denoted by $X = \{X_q\}_{q \in Q}$ as the state space. This is natural, as different discrete states may be associated with different continuous control systems defined on different continuous state spaces. A point in X is represented by the pair (q, x), where $x \in X_q$.

As monoid we will use the set:

$$\mathscr{M} = \coprod_{n \in \mathbb{N}} (U^* \cup \Sigma^*)^n \tag{6}$$

assuming that $U^* \cap \Sigma^* = \{\varepsilon\}$ and regarding U^* and Σ^* simply as sets. Let us elaborate on the product operation on $\mathscr{M}$. This operation is defined as the usual concatenation and therefore it requires finite length strings. To accommodate this requirement and still be able to have an infinite number of concatenations of elements in U^* we proceed as follows. Suppose that we want to show that $\sigma_1 u^{t_1} u^{t_2} \ldots u^{t_n} \ldots \sigma_2$ belongs to $\mathscr{M}$, where t_n is a convergent sequence. Instead of regarding each element in the string as an element in $\mathscr{M}$, which would not allow us to define the last concatenation since it would happen after ∞, we regard σ_1 and σ_2 as elements of $\mathscr{M}$ and $u^{t_1} u^{t_2} \ldots u^{t_n} \ldots = u^{t'}$ as an element of U^* and consequently as an element of $\mathscr{M}$, where $t' = \sum_{n=1}^{\infty} t_n$. This string is then regarded as the map $u\colon \{1, 2, 3\} \to \mathscr{M}$ defined by $u(1) = \sigma_1$, $u(2) = u^{t'}$ and $u(3) = \sigma_3$. The product in $\mathscr{M}$ is then the usual concatenation on reduced strings, that is, strings where all consequent sequences of elements of U^* or Σ^* have been replaced by their product in U^* or Σ^*, respectively. The monoid $\mathscr{M}$ obtained by this construction is called the free product of U^* and Σ^* and is in fact the co-product[4] in the category of monoids (Howie, 1995).

Furthermore, we have the following characterization of $\mathscr{M}$ that will be useful in the next sections:

PROPOSITION 2.2 (Howie, 1995) *The monoid $\mathscr{M}$ is freely generated by the symbols $U^* \cup \Sigma^*$.*

We refer the reader to Appendix A, where the notion of freely generated monoid is described and proceed by casting hybrid control systems into the abstract control systems framework:

DEFINITION 2.3 (hybrid control systems) *A hybrid control system $H = (X, \mathscr{M}, \Phi)$ consists of:*

- *The state space $X = \{X_q\}_{q \in Q}$.*
- *A monoid $\mathscr{M} = \coprod_{n \in \mathbb{N}} (U^* \cup \Sigma^*)^n$.*
- *A partial action Φ of $\mathscr{M}$ on X.*

The semantics associated with the evolution from (q, x) governed by Φ and controlled by $m \in \mathscr{M}(q, x)$ is the standard transition semantics of hybrid systems (Henzinger, 1996). Suppose that $m = u^{t_1}\sigma_1\sigma_2 u^{t_2}$, then $(q, x) \xrightarrow{m} (q', x')$ means that the system starting at (q, x) evolves during t_1 units of time under continuous input u^{t_1}, jumps under discrete input σ_1 and them jumps again under σ_2. After the two consecutive jumps, the system evolves under the continuous control input u^{t_2} reaching (q', x'), t_2 units of time after the last jump. From the hybrid system construction, we can clearly extract the purely discrete case presented in Section 2.1 when X_q is a singleton and $U_q = \varnothing$ for each $q \in Q$. The purely continuous case presented in Section 2.2 is also recovered when Q is a singleton and $\Sigma = \varnothing$. This shows that the above model provides the right generalization from the discrete and continuous models.

2.5. Control System Abstractions

Having defined the structure of control systems and hybrid control systems in particular, we now consider relationships between abstract control systems that preserve their structure and can therefore be seen as abstract control systems homomorphisms. We shall call such maps, simulation maps, for reasons to be discussed shortly. Intuitively, given a system, we will transfer the study of its properties to the properties of a smaller system through the use of a simulation map between them.

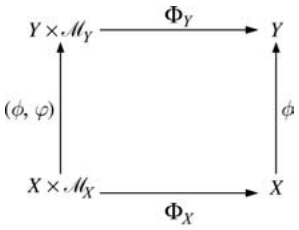
DEFINITION 2.4 (simulations of abstract control systems) *Let Φ_X and Φ_Y be two abstract control systems over X and Y with monoids $\mathscr{M}_X$ and $\mathscr{M}_Y$, respectively. A pair of maps (ϕ, φ) is said to be a simulation from Φ_X to Φ_Y when:*

- $\phi : X \to Y$ is a total map.
- $\varphi : X \times \mathscr{M}_X \to \mathscr{M}_Y$ is a partial map defined on $\Phi_X^{-1}(X)$ satisfying for every $x \in X$:

$$\varphi(x, \varepsilon) = \varepsilon \tag{7}$$

$$\varphi(x, m_1 m_2) = \varphi(x, m_1)\varphi(\Phi_X(x, m_1), m_2) \tag{8}$$

- the maps ϕ and φ satisfy $(\phi, \varphi)(X, \mathscr{M}_X) \subseteq \Phi_Y^{-1}(Y)$ and relate Φ_X to Φ_Y as expressed in the following commutative diagram.



(9)

or equivalently $\phi \circ \Phi_X(x, m) = \Phi_Y(\phi(x), \varphi(x, m))$.

When (ϕ, φ) is a simulation from Φ_X to Φ_Y we also say that Φ_Y is a simulation of Φ_X since for every evolution of Φ_X, the map ϕ transforms that evolution into an evolution of Φ_Y. It is in this sense, that Φ_Y simulates Φ_X. The map ϕ (when it is not injective) is to be understood as a state aggregation map, specifying which state information is propagated from the original system Φ_X to Φ_Y. Similarly, the map φ transforms the inputs of the original system Φ_X to the inputs of system Φ_Y.

This definition of simulation slightly generalizes the usual notions of morphisms between transition systems as described in Winskel and Nielsen (1994). Instead of considering maps $\phi : X \to Y$ and $\varphi : \mathscr{M}_X \to \mathscr{M}_Y$, we allow φ to depend also on X. This is necessary in order to correctly describe the relation between the input spaces of continuous control systems and its abstractions as discussed in Tabuada and Pappas (2002b). Nevertheless, abstract control systems and simulation maps still define a category, where composition of morphisms $(\phi_1(x_1), \varphi_1(x_1, m_1))$ and $(\phi_2(x_2), \varphi_2(x_2, m_2))$ is given by $(\phi_2 \circ \phi_1(x_1), \varphi_2(\phi_1(x_1), \varphi_1(x_1, m_1)))$ and identity morphisms are simply the identity maps.

The conditions expressed in Definition 2.4 may seem difficult to check in concrete examples. However, we shall take a constructive approach by introducing a construction that builds the map φ and the system Φ_Y from a given system Φ_X and map ϕ. Furthermore, φ and Φ_Y will satisfy all the conditions of Definition 2.4 by construction, thereby overcoming the necessity of determining if they are indeed satisfied.

It is within this category that we shall develop our study of abstractions, considering any simulation of a system as an abstraction of that system. We introduce also the celebrated notion of bisimulation (Park, 1980; Milner, 1989), a special simulation in the current setting. As the morphisms in this category are functions, we will only introduce bisimulations induced by maps. A different approach would consider defining morphisms

as relations, in which case a bisimulation would simply be a symmetric simulation relation, that is, a relation R such that both R and R^{-1} are simulations. We direct the reader to Tabuada et al. (2002) for an account of such an approach and proceed with the definition:

DEFINITION 2.5 (bisimulations of abstract control systems) *Let Φ_X and Φ_Y be abstract control systems over X and Y with monoids $\mathscr{M}_X$ and $\mathscr{M}_Y$, respectively. A simulation (ϕ, φ) from Φ_X to Φ_Y is a bisimulation when $(\phi(x), n) \in \Phi_Y^{-1}(Y)$ implies:*

$$\forall x' \in \phi^{-1}(\phi(x)) \quad \exists\, m \in \mathscr{M}_X(x') \quad \text{such that} \quad \varphi(x', m) = n \tag{10}$$

We note that in the special case where φ is in fact the identity map on $\mathscr{M}_X$, that is, $\varphi = id : \mathscr{M}_X \to \mathscr{M}_X = \mathscr{M}_Y$, we recover the notion of bisimulation introduced in Milner (1989) by regarding the graph Γ of ϕ:

$$\Gamma = \{(x, y) \in X \times Y \ : \ y = \phi(x)\}$$

as the bisimulation relation. In fact, if $(x, y) \in \Gamma$ and $x \xrightarrow{m} x'$, then by commutativity of diagram (9) we have that $\phi(x) = y \xrightarrow{m} y'$ and $(x', y') \in \Gamma$ by noting that $\varphi(x, m) = id(m) = m$ and $\phi(x') = y'$.

Several other approaches to bisimulation are reported in the literature and we point the reader to the comparative study in Roggenbach and Majster-Cederbaum (2000) and the references therein. However, we note that since abstract control systems are deterministic in the sense that given a pair (x, m) in the domain of Φ_X, $\Phi_X(x, m)$ is a uniquely determined point in X, simulation and bisimulation reduces to language inclusion and equivalence. Therefore, the importance of simulations lies on the possibility of transferring the study of properties over the trajectories of Φ_X to the study of the same properties over trajectories of Φ_Y. We now make this fact precise. Instead of trying to define trajectories of abstract control systems (which would be as difficult as defining trajectories of hybrid control systems, see the different approaches in Johansson (1999), Moor and Davoren (2001), Alur et al. (1995)) we will restrict our attention to the orbits of abstract control systems.

DEFINITION 2.6 *Let Φ_X be an abstract control system over X with monoid $\mathscr{M}_X$. The orbit of Φ_X through the point $x \in X$ is given by:*

$$\mathscr{O}_x = \{x' \in X : x' = \Phi_X(x, m) \text{ for any } m \text{ such that } (x, m) \in \Phi_X^{-1}(X)\} \tag{11}$$

Intuitively, the orbit $\mathscr{O}_x$ is the set of all the points that can be reached from x. We can now relate the orbits of abstract control systems to the orbits of the corresponding simulations:

PROPOSITION 2.7 (orbit propagation) *Let Φ_X and Φ_Y be abstract control systems over X and Y, respectively, and (ϕ, φ) a simulation from Φ_X to Φ_Y, then for every $x \in X$:*

$$\phi(\mathscr{O}_x) \subseteq \mathscr{O}_{\phi(x)} \tag{12}$$

Proof: Assume that Φ_Y is a simulation of Φ_X. If $x' \in \mathcal{O}_x$, then, by definition of orbit, there exists a $m \in \mathcal{M}_X$ such that $\Phi_X(x,m) = x'$. Applying ϕ on both sides we get:

$$\begin{aligned} & \phi \circ \Phi_X(x,m) = \phi(x') \\ \Leftrightarrow\ & \Phi_Y(\phi(x), \varphi(x,m)) = \phi(x') \end{aligned}$$

where the second equality holds by definition of simulation. This shows that $\phi(x') \in \mathcal{O}_{\phi(x)}$, and as x' was any point in $\mathcal{O}_x$, the desired inclusion is proved. ■

This result is important as it shows that any abstraction, in this context, can be used to verify reachability based properties of which safety (Manna and Pnueli, 1995) is an important example. This, we state formally in the next corollary:

COROLLARY 2.8 (reachability propagation) *Let Φ_X and Φ_Y be abstract control systems over X and Y, respectively, (ϕ, φ) a simulation from Φ_X to Φ_Y, $x \in X$ and $B \subseteq X$. Then, if the orbit of Φ_Y from $\phi(x)$ does not intersect $\phi(B)$, the orbit of Φ_X from x does not intersect B.*

Proof: Assume for the sake of contradiction that the orbit of Φ_Y from $\phi(x)$ does not intersects $\phi(B)$ and that the orbit of Φ_X from x intersects B. We then have $\mathcal{O}_x \cap B \neq \varnothing$ and it follows by Proposition 2.7 that for any $x' \in \mathcal{O}_x \cap B$:

$$\phi(x') \in \phi(\mathcal{O}_x) \cap \phi(B) \subseteq \mathcal{O}_{\phi(x)} \cap \phi(B)$$

which shows that $\mathcal{O}_{\phi(x)} \cap \phi(B) \neq \varnothing$ and leads to the desired contradiction. ■

This result provides only a sufficient condition, since if one shows that orbits of Φ_Y do intersect B, one cannot conclude anything about the original system. It is, therefore, desirable to determine abstractions which are not only sufficient but also necessary with respect to reachability based properties. This is the case for bisimulations as we now state:

PROPOSITION 2.9 (reachability equivalence) *Let Φ_X and Φ_Y be abstract control systems over X and Y, respectively, (ϕ, φ) a bisimulation from Φ_X to Φ_Y, $x \in X$ and $B \subseteq X$. Then, the orbit of Φ_Y from $\phi(x)$ does not intersect $\phi(B)$ iff the orbit of Φ_X from x does not intersect $\phi^{-1}(\phi(B))$.*

Proof: We only need to show that if the orbit of Φ_Y from $\phi(x)$ intersects $\phi(B)$ then the orbit of Φ_X from x intersects $\phi^{-1}(\phi(B))$. Assume that $y \in \mathcal{O}_{\phi(x)} \cap \phi(B)$, then by definition of orbit there exist a $n \in \mathcal{M}_Y$ such that $\Phi_Y(\phi(x), n) = y$. Using the fact that (ϕ, φ) is a bisimulation, we know that there exists a $m \in \mathcal{M}_X$ such that $\phi \circ \Phi_X(x,m) = y$ which shows that $\Phi_X(x,m) \in \phi^{-1}(y) \subseteq \phi^{-1}(\phi(B))$. ■

3. Compositional Abstractions

We have introduced the basic framework to discuss abstractions of hybrid control systems when regarded as a single component. However, in many situations, we also have knowledge about the internal interconnection structure of hybrid systems and we seek to take advantage of such knowledge. We thus need to model in the current framework, composition and synchronization of hybrid systems. We will follow the categorical description of transition systems in Winskel and Nielsen (1994), and introduce a notion of parallel composition with synchronization for abstract control systems. Furthermore, we will also determine when such notions are compatible with simulation and bisimulation. Compatibility will mean that in order to obtain an abstraction of a large system obtained by composing several modules, we can abstract each module individually and obtain the desired abstraction by composing the individual abstractions.

3.1. Parallel Composition with Synchronization

We model parallel composition with synchronization in two steps. In the first step, we perform what can be seen as an asynchronous product, where no interaction between systems is modeled and all possible evolutions of the two systems are allowed. Then we restrict this product by removing undesired evolutions thereby modeling synchronization. We start by introducing the product[5] of abstract control systems:

DEFINITION 3.1 (Product of abstract control systems) *Let* $\Phi_X : X \times \mathscr{M}_X \to X$ *and* $\Phi_Y : Y \times \mathscr{M}_Y \to Y$ *be two abstract control systems. The product of* Φ_X *and* Φ_Y *is the abstract control system* $\Phi_X \times \Phi_Y : (X \times Y) \times (\mathscr{M}_X \otimes \mathscr{M}_Y) \to X \times Y$ *defined by:*

$$\Phi_X \times \Phi_Y((x,y),(m,n)) = (\Phi_X(x,m), \Phi_Y(y,n))$$

We now present a simple example of a product of two systems.

Example 3.2: Consider the transition systems T_1 and T_2 inspired from Winskel and Nielsen (1994) and displayed on the left of Figure 1, where only the transitions labeled by the monoid generators are represented. The product of these transitions systems $T_1 \times T_2$ will consist of all possible evolutions of both systems as displayed on the right of Figure 1.

Example 3.3: For a purely continuous example, consider two control systems (M, U, f) and (N, V, g). On the product state space $M \times N$ and the product input space $U \times V$ we can define the product control system defined by $f \times g : M \times N \to T(M \times N)$ defined by $(f \times g)((x,u),(y,v)) = (f(x,u), g(y,v))$. Clearly, this control system captures all the possible trajectories of the individual control systems f and g.

As this notion of product captures all possible evolutions of both systems, we cannot model how the behavior of one of the systems influences the behavior of the other system.

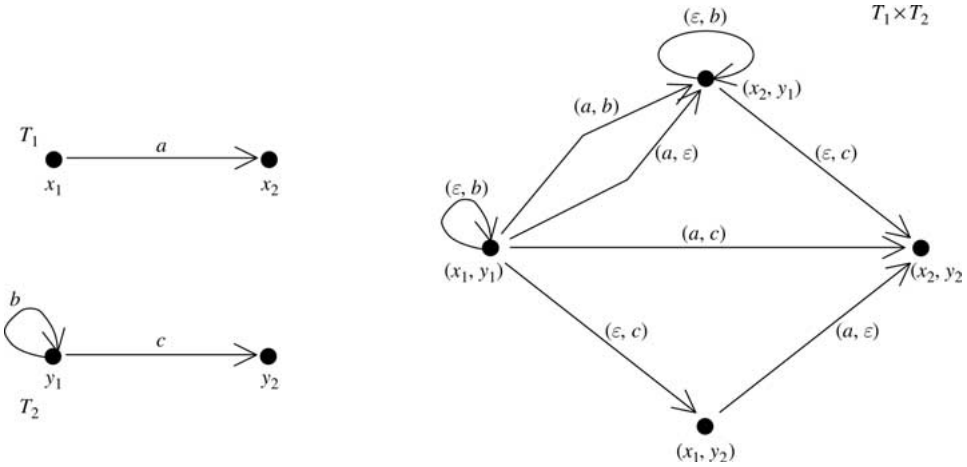


Figure 1. Transition systems T_1 and T_2 on the left and the corresponding product transition system $T_1 \times T_2$ on the right.

This will be achieved through the operation of restriction, which allows to remove undesired evolutions from the product system.

DEFINITION 3.4 (restriction of abstract control systems) *Let $\Phi_X : X \times \mathscr{M}_X \to X$ be an abstract control system and L a subset of $X \times \mathscr{M}_X$. The restriction of Φ_X to L is the abstract control system $\Phi_X|_L : L_X \times \mathscr{M}_X \to L_X$ defined by:*

$$\Phi_{X|L}(x,m) = \Phi_X(x,m) \quad \textit{iff} \quad (x,m) \in L \textit{ and for any prefix } m' \textit{ of } m,$$
$$\Phi_X(x,m') \in L_X \wedge (x,m') \in L$$

where L_X is the projection of L on X.

This restriction operation captures synchronization notions for continuous and discrete control systems as we now describe in the following examples:

Example 3.5: As an example of continuous synchronization we consider two robots in the plane as displayed in Figure 2. The state space for each robot is $\mathbb{R}^4$ consisting of (x_1, x_2, x_3, x_4), where (x_1, x_2) represent the robot position and (x_3, x_4) the robot velocity. The coordinates for the second robot are (y_1, y_2, y_3, y_4) and have similar interpretation. We now assume that the robots are cooperatively transporting a rigid bar. The synchronization of the two robots can be modeled as the subset $L_{\mathbb{R}^4 \times \mathbb{R}^4} \subseteq \mathbb{R}^4 \times \mathbb{R}^4$ defined by:

$$L_{\mathbb{R}^4 \times \mathbb{R}^4} = \{((x_1, x_2, x_3, x_4), (y_1, y_2, y_3, y_4)) \in \mathbb{R}^4 \times \mathbb{R}^4 : x_1 = y_1 + k_1 \wedge x_2 = y_2 + k_2\}$$

where k_1 and k_2 are positive constants related with the dimensions of the transported object. The final synchronizing set is obtained by appending to $L_{\mathbb{R}^4 \times \mathbb{R}^4}$ the monoids to obtain $L = L_{\mathbb{R}^4 \times \mathbb{R}^4} \times \mathscr{M}_X \times \mathscr{M}_Y$.

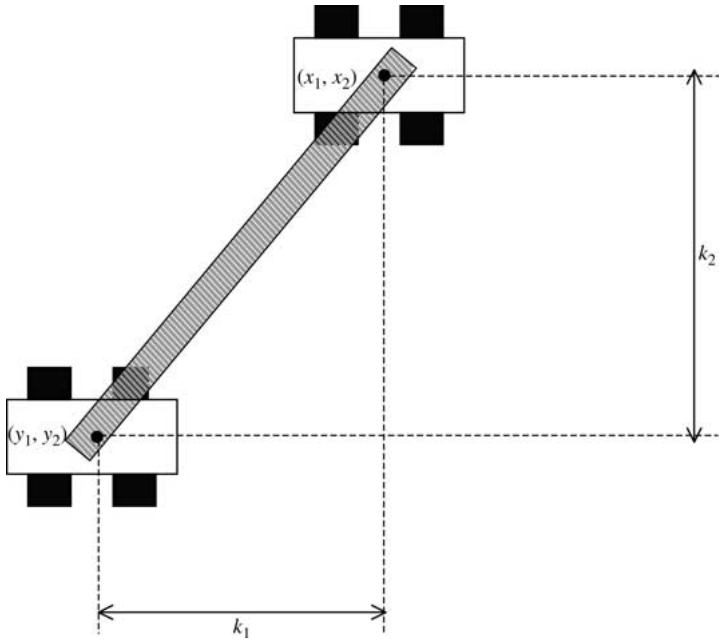


Figure 2. Robots cooperatively transporting a rigid bar.

The previous example modeled restriction at the level of the states, however, for purely discrete systems one of the most popular notions of synchronization consists of synchronizing state machines or transition systems on common events. This is captured in this framework by properly choosing the set L as shown in the next example:

Example 3.6: Consider the transition system displayed on the left of Figure 1. By specifying the set L as the product and prefix closure of:

$$\{x_1, x_2\} \times \{y_1, y_2\} \times \{(\varepsilon, c), (a, b)\}$$

it is possible to synchronize the event a with the event b on the parallel composition of these systems. The resulting transition system is displayed in Figure 3.

With the notions of product and restriction at hand, we can now define a general operation of parallel composition with synchronization.

DEFINITION 3.7 (parallel composition with synchronization) *Let* $\Phi_X : X \times \mathscr{M}_X \to X$ *and* $\Phi_Y : Y \times \mathscr{M}_Y \to Y$ *be two abstract control systems and consider the set* $L \subseteq (X \times Y) \times (\mathscr{M}_X \otimes \mathscr{M}_Y)$. *The parallel composition of* Φ_X *and* Φ_Y *with synchronization over* L *is the abstract control system denoted by* $\Phi_X \parallel_L \Phi_Y$ *and defined as:*

$$\Phi_X \parallel_L \Phi_Y = (\Phi_X \times \Phi_Y)|_L \tag{13}$$

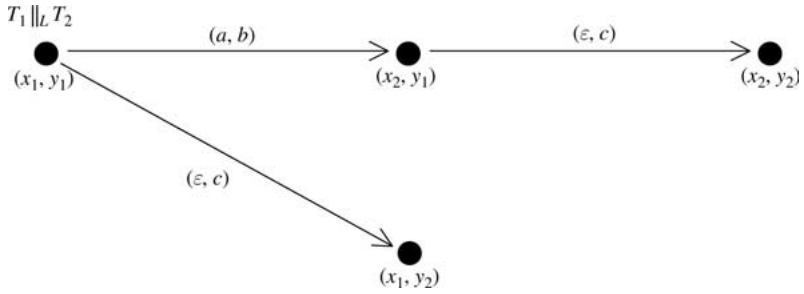


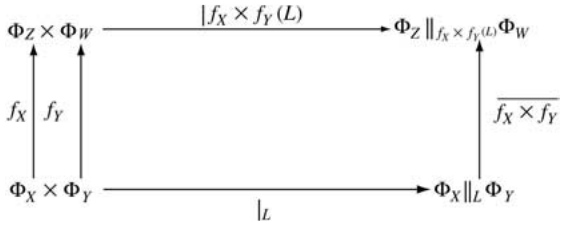
Figure 3. Parallel composition with synchronization of the transition systems T_1 and T_2 displayed on the left of Figure 1.

3.2. Compositionality of Simulations

We now determine if composition of subsystems is compatible with simulation. This compatibility allows to break the computation of abstractions by computing abstractions of each subsystem individually. The resulting abstractions are then composed and synchronized to obtain an abstraction of the original system. The next result shows that this is always possible for simulations and describes how the process of computing abstractions can be rendered more efficient by exploiting the interconnection structure of hybrid systems.

THEOREM 3.8 (compositionality of simulations): *Let Φ_X, Φ_Y, Φ_Z, Φ_W be abstract control systems and let $f_X = (\phi_X, \varphi_X)$ and $f_Y = (\phi_Y, \varphi_Y)$ be simulations from Φ_X to Φ_Z and from Φ_Y to Φ_W, respectively. Consider a set $L \subseteq (X \times Y) \times (\mathscr{M}_X \otimes \mathscr{M}_Y)$ and its projection $L_{X\times Y}$ on $X \times Y$. The parallel composition of Φ_Z and Φ_W with synchronization over $(f_X \times f_Y)(L)$ is a simulation of the parallel composition of Φ_X and Φ_Y with synchronization over L, where the simulation from $\Phi_X \|_L \Phi_Y$ to $\Phi_Z \|_{(f_X\times f_Y)(L)} \Phi_W$ is $\overline{f_X \times f_Y} = f_X \times f_Y|_{(\Phi_X\|_L\Phi_Y)^{-1}(L_{X\times Y})}$.*

The contents of the previous theorem can equivalently be expressed in the following commutative diagram:

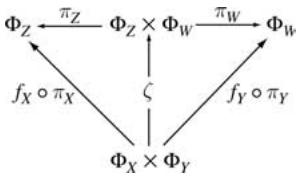


(14)

which emphasizes its importance. We can see that, in general, it is much easier to abstract each individual subsystem Φ_X and Φ_Y and by parallel composition with synchronization on $f_X \times f_Y(L)$ obtain $\Phi_Z \|_{f_X\times f_Y(L)} \Phi_W$, than is to abstract directly $\Phi_X \|_L \Phi_Y$. The above

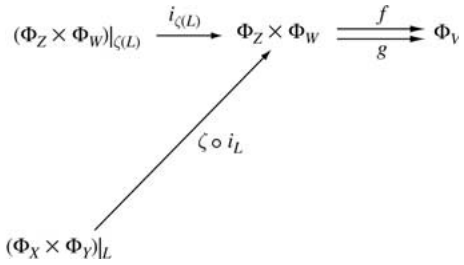
result was stated for parallel composition of two abstract control systems but it can be easily extended to any finite number of abstract control systems.

Proof: We shall make use of the categorical notions of product and equalizer reviewed in Appendix B. Consider the product system $(\Phi_Z \times \Phi_W, \pi_Z, \pi_W)$ and the triple $(\Phi_X \times \Phi_Y, f_X \circ \pi_X, f_Y \circ \pi_Y)$. By definition of product we know that there is one and only one morphism ζ such that:



(15)

commutes and this morphism is given by $\zeta = \langle f_X, f_Y \rangle = f_X \times f_Y$, meaning that $f_X \times f_Y$ is a simulation from $\Phi_X \times \Phi_Y$ to $\Phi_Z \times \Phi_W$. We now make use of the fact that the operation of restriction can be categorically defined by an equalizer. With this in mind we consider the following diagram:



(16)

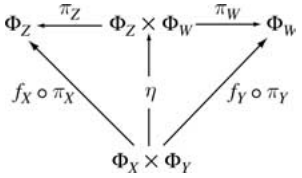
where $(\Phi_Z \times \Phi_W|_{\zeta(L)}, i_{\zeta(L)})$ is the equalizer of f and g, which agree on $\zeta(L)$. We now show that $f \circ \zeta \circ i_L = g \circ \zeta \circ i_L$, for i_L the inclusion morphism from $\Phi_X \times \Phi_Y|_L$ to $\Phi_X \times \Phi_Y$. This follows from $(\Phi_X \parallel_L \Phi_Y)^{-1}(L_{X\times Y}) \subseteq L$, which implies $\zeta \circ i_L((\Phi_X \parallel_L \Phi_Y)^{-1}(L_{X\times Y}))$ $= \zeta((\Phi_X \parallel_L \Phi_Y)^{-1}(L_{X\times Y})) \subseteq \zeta(L)$ since $f = g$ on $\zeta(L)$, we have $f \circ \zeta \circ i_L = g \circ \zeta \circ i_L$. Therefore, by definition of equalizer, there exists one and only one simulation η from $\Phi_X \parallel_L \Phi_Y$ to $\Phi_Z \parallel_{\zeta(L)} \Phi_W$ which is given by $\eta = \zeta \circ i_L = f_X \times f_Y|_{(\Phi_X \parallel_L \Phi_Y)^{-1}(L)}$. ■

3.3. Compositionality of Bisimulations

We now extend the previous compatibility results from simulations to bisimulations. We start with a very simple lemma stating that product respects bisimulations:

LEMMA 3.9. *Given abstract control systems Φ_X, Φ_Y, Φ_Z, Φ_W and bisimulations f_X and f_Y from Φ_X to Φ_Z and from Φ_Y to Φ_W, respectively, the product system $\Phi_Z \times \Phi_W$ is a bisimulation of $\Phi_X \times \Phi_Y$, where the bisimulation from $\Phi_X \times \Phi_Y$ to $\Phi_Z \times \Phi_W$ is $f_X \times f_Y$.*

Proof: Consider the following commutative diagram:



(17)

By definition of product there exists one and only one morphism η such that the above diagram commutes. In fact, η is the morphism $\eta = (f_X \circ \pi_X, f_Y \circ \pi_Y) = f_X \times f_Y$ meaning that $\Phi_Z \times \Phi_W$ is a simulation of $\Phi_X \times \Phi_Y$ with simulation $f_X \times f_Y$ from $\Phi_X \times \Phi_Y$ to $\Phi_Z \times \Phi_W$. We now show that $f_X \times f_Y$ is also a bisimulation. Let $((z,w),(o,p)) \in (Z \times W) \times (\mathscr{M}_Z \otimes \mathscr{M}_Z)$. Since Φ_Z is a bisimulation of Φ_X, there is a $(x,m) \in X \times \mathscr{M}_X$ such that $f_X(x,m) = (z,o)$ and similarly there exists a $(y,n) \in Y \times \mathscr{M}_Y$ such that $f_Y(y,n) = (w,p)$. We now see that $f_X \times f_Y((x,y),(m,n)) = ((z,w),(o,p))$ which shows that $f_X \times f_Y$ is also a bisimulation. ■

Although the product respects bisimulations the same does not happen with the operation of restriction. Consider the example displayed in Figure 4 where the abstract control system on top is bisimilar to the system below with respect to the maps defined by:

$$\begin{aligned}\phi(x_1) = x_1, \phi(x_2) = x_3, \phi(x_3) = x_3, \phi(x_4) = x_4 \\ \varphi(x_1,\varepsilon) = \varepsilon, \varphi(x_1,m_1) = m_1, \varphi(x_2,\varepsilon) = \varepsilon, \varphi(x_2,m_2) \\ = \varepsilon, \varphi(x_3,\varepsilon) = \varepsilon, \varphi(x_3,m_3) = m_3, \varphi(x_4,\varepsilon) = \varepsilon\end{aligned}$$

If we now restrict the system below to the product and prefix closure of:

$$L = \{(x_1,\varepsilon),(x_1,m_1),(x_2,\varepsilon),(x_3,\varepsilon),(x_3,m_3),(x_4,\varepsilon)\} \tag{18}$$

and restrict the system on top to $(\phi,\varphi)(L)$ the systems will cease to be bisimilar since the system on top can move from x_3 to x_4 by m_3 but the restricted system can not simulate that evolution when on $x_2 \in \phi^{-1}(x_3)$. This difficulty can be overcomed by additional assumptions as stated in the next proposition:

PROPOSITION 3.10 *Let Φ_X and Φ_Y be abstract control systems, f a bisimulation from Φ_X to Φ_Y, L a subset of $X \times \mathscr{M}_X$ satisfying $f^{-1}(f(L)) = L$. The restriction $\Phi_X|_L$ is a bisimulation of $\Phi_Y|_{f(L)}$ where $f|_{\Phi_X|_L^{-1}(L_X)}$ is the bisimulation from $\Phi_X|_L$ to $\Phi_Y|_{f(L)}$.*

Proof: Let $f = (\phi,\varphi)$ and $(y,n) \in \Phi_Y|_{f(L)}^{-1}(\phi(L_X))$. Since $(y,n) \in \Phi_Y^{-1}(Y)$ and Φ_Y is bisimilar to Φ_X we know that for every $x \in \phi^{-1}(y)$ there exists a m such that $\varphi(x,m) = n$. We now show that such (x,m) also belongs to $\Phi_X|_L^{-1}(L_X)$. Let $x' = \Phi_X(x,m)$ and note that $\phi(x') = \Phi_Y(y,n)$ since f is a simulation from Φ_X to Φ_Y. From the assumption $f^{-1}(f(L)) = L$, it follows that $x' \in L_X$ and $(x,m) \in L$ so that by definition of restriction $(x,m) \in \Phi_X|_L^{-1}(L_X)$ as desired. ■

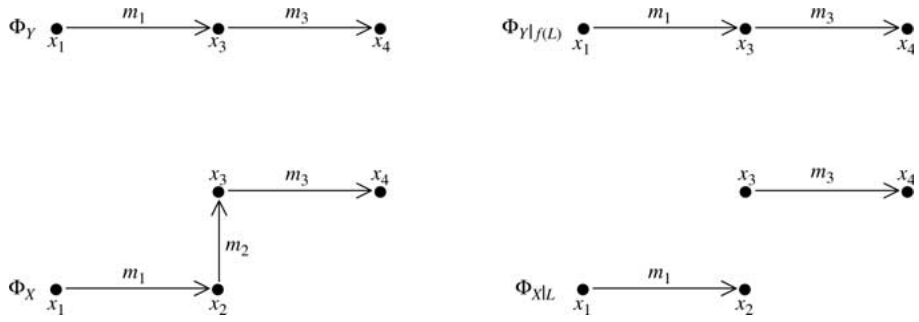


Figure 4. Bisimilar abstract control systems that cease to be bisimilar after the operation of restriction.

The above propositions lead to the following result concerning the compositionality of bisimulations:

THEOREM 3.11 (compositionality of bisimulations) *Let Φ_X, Φ_Y, Φ_Z, Φ_W be abstract control systems, $f_X = (\phi_X, \varphi_X)$ and $f_Y = (\phi_Y, \varphi_Y)$ bisimulations from Φ_X to Φ_Z and from Φ_Y to Φ_W, respectively, L a subset of $\subseteq (X \times Y) \times (\mathscr{M}_X \otimes \mathscr{M}_Y)$ satisfying $(f_X \times f_Y)^{-1}(f_X \times f_Y(L)) = L$ and denote by $L_{X\times Y}$ the projection of L on $X \times Y$. The parallel composition of the simulations Φ_Z and Φ_W with synchronization over $(f_X \times f_Y)(L)$ is a bisimulation of the parallel composition of Φ_X and Φ_Y with synchronization over L, where the simulation from $\Phi_X \parallel_L \Phi_Y$ to $\Phi_Z \parallel_{(f_X \times f_Y)(L)} \Phi_W$ is $f_X \times f_Y|_{(\Phi_X \parallel_L \Phi_Y)^{-1}(L_{X\times Y})}$.*

From the previous result we conclude that if we have a means of computing bisimulations and choose the synchronization set L carefully, we can compute bisimulations by exploring interconnection of large-scale systems. In the next section, we provide a construction to effectively compute abstractions and in certain situations bisimulations of hybrid control systems.

4. Hybrid Control Systems

Having developed the general theory at a fairly abstract level, allowing to show the desired results with relatively ease, we turn to the application of such results to hybrid control systems. The results presented in this section can be seen as a translation to the language of hybrid systems of the introduced results for abstract control systems. Inevitably, the statement of such results will become extremely complicated by making explicit all the relevant conditions at the level of invariants, guards, etc. The reader is urged to contrast the simplicity of the abstract control systems formulation with the tedious version for hybrid systems.

We start by reviewing the hybrid automaton model to set the notation for the remaining section.

DEFINITION 4.1 (hybrid automata) *hybrid automaton is a tuple*

$H_X = (X, X_0, \Sigma_X, U_X, f_X, \mathrm{Inv}_X, \mathrm{Guard}_X, \mathrm{Reset}_X)$ *consisting of:*

- *The state space* $X = \{X_q\}_{q\in Q}$*, a collection of smooth manifolds* X_q *parameterized by a finite set of discrete states* Q*.*
- *A set of initial states* $X_0 \subseteq X$*.*
- *A finite set of labels* Σ_X*, parameterizing the discrete transitions between discrete states.*
- *The continuous input space* $U_X = \{U_X^q\}_{q\in Q}$*, a collection of inputs spaces parameterized by the discrete states.*
- *A collection of control systems* $f_X = \{f_X^q\}_{q\in Q}$, $f_X^q : \mathrm{Inv}_X^q \times U_X^q \to T\mathrm{Inv}_X^q$*, parameterized by the discrete locations.*
- *The invariant* $\mathrm{Inv}_X = \{\mathrm{Inv}_X^q\}_{q\in Q}$, $\mathrm{Inv}_X^q \subseteq X_q$*, a collection of subsets of X parameterized by the discrete locations.*
- *The guards* $\mathrm{Guard}_X = \{\mathrm{Guard}_X^{(q,\sigma,q')}\}_{(q,\sigma,q')\in\Pi}$, $\mathrm{Guard}_X^{(q,\sigma,q')} \subseteq \mathrm{Inv}_X^q$*, a collection of subsets of the invariant, parameterized by* Π*, the subset of all the triples* $(q,\sigma,q') \in Q \times \Sigma_X \times Q$ *such that there exists a discrete transition from* q *to* q' *labeled by* σ*.*
- *The reset maps,* $\mathrm{Reset}_X = \{\mathrm{Reset}_X^{(q,\sigma,q')}\}_{(q,\sigma,q')\in\Pi}$, $\mathrm{Reset}_X^{(q,\sigma,q')} : \mathrm{Guard}_X^{(q,\sigma,q')} \to 2^{\mathrm{Inv}q'}$*, a collection of set valued maps defining the possible locations of the continuous state after the discrete transition.*

We now translate the theory developed for abstract control systems to the language of hybrid automata. The principal link between the two formulations will be given by the notion of simulation that we now characterize in terms of hybrid automata:

PROPOSITION 4.2 *Let*

$$H_X = (X, X_0, \Sigma_X, U_X, f_X, \mathrm{Inv}_X, \mathrm{Guard}_X, \mathrm{Reset}_X)$$
$$H_Y = (Y, Y_0, \Sigma_Y, U_Y, f_Y, \mathrm{Inv}_Y, \mathrm{Guard}_Y, \mathrm{Reset}_Y)$$

be hybrid control systems and $\mathscr{D}_X = \{\mathscr{D}_X^q\}_{q\in Q}$ *and* $\mathscr{D}_Y = \{\mathscr{D}_Y^p\}_{p\in P}$ *the collection of vector fields pointwise defined by*:

$$\mathscr{D}_X^q(x) = \bigcup_{u\in U_X^q} f_X^q(x,u)$$
$$\mathscr{D}_Y^p(y) = \bigcup_{v\in U_Y^p} f_Y^p(y,v)$$

A pair of maps $\phi = (\phi_D, \phi_C) : X \to Y$ *consisting of*:

- *Discrete state aggregation map:* $\phi_D : Q \to P$,
- *Continuous state aggregation map:* $\phi_C = \{\phi_C^q\}_{q \in Q}$, $\phi_C^q : \mathrm{Inv}_X^q \to \mathrm{Inv}_Y^{\phi_D(p)}$

satisfying:

- *Preservation of initial conditions:* $f(X_0) \subseteq Y_0$.
- *Continuous abstraction:* $T_x \phi_C^q(\mathscr{D}_X^q(x)) \subseteq \mathscr{D}_Y^{\phi_D(q)} \circ \phi_X^q(x)$,

and a map $\varphi_D : Q \times \Sigma_X \to \Sigma_Y$ *satisfying*:

- *Preservation of transition enabling:* $\phi_C^q(\mathrm{Guard}_X^{(q,\sigma,q')}) \subseteq \mathrm{Guard}_Y^{(\phi_D(q),\varphi_D(q,\sigma),\phi_D(q'))}$,
- *Preservation of resets:* $\phi_C^q(\mathrm{Reset}_X^{(q,\sigma,q')}(x)) \subseteq \mathrm{Reset}_Y^{(\phi_D(q),\varphi_D(q,\sigma),\phi_D(q'))} \circ \phi_C^q(x)$.

defines a simulation from H_X *to* H_Y.

Proof: We will show that the given data defines a simulation (ϕ, φ) from H_X to H_Y. For the state aggregation map ϕ we simply take $\phi = (\phi_D, \phi_C)$. The definition of φ takes more work and will make use of the freeness properties of the monoid $\mathscr{M}_X$ associated with the hybrid system H_X. Recall that by Proposition 2.2 the monoid $\mathscr{M}_X = \coprod_{n \in \mathbb{N}_0} (\Sigma_X^* \cup U_X^*)^n$ is freely generated by the set $\Sigma_X^* \cup U_X^*$ and that Σ_X^* is freely generated by the set Σ_X, therefore we only need to define φ for elements in $\Sigma_X \cup U_X^*$. We treat the discrete case first: As we considered only deterministic systems in the abstract framework we start by enlarging the set Σ_X to $\overline{\Sigma_X}$ so as to parameterize the nondeterminism. We replace every $\sigma \in \Sigma_X$ with (σ, x') for every $x' \in \mathrm{Reset}_X^{(q,\sigma,q')}$ and similarly for Σ_Y. This ensures that the abstract control systems Φ_X and Φ_Y associated with H_X and H_Y are now deterministic, since different elements in $\mathrm{Reset}_X^{(q,\sigma,q')}$ are parameterized by different symbols in $\overline{\Sigma_X}$. We also extend φ_D to $\overline{\varphi_D} : Q \times \overline{\Sigma_X} \to \overline{\Sigma_Y}$ by $\overline{\varphi_D}(q, (\sigma, x')) = (\sigma', x'')$, where $\sigma' = \varphi_D(q, \sigma)$ and x'' satisfies:

$$\begin{aligned} \Phi_Y((\phi_D(q), \phi_C^q(x)), \overline{\varphi_D}(q, (\sigma, x'))) &= \phi(q', x'') \\ &= \phi \circ \Phi_X((q, x), (\sigma, x')) \end{aligned} \tag{19}$$

which is always possible given the preservation of transition enabling and resets assumptions on the map φ_D. This allows to define φ by $\overline{\varphi_D}$ for elements in $\overline{\Sigma_X}$. Freeness of Σ_X^* and (19) now ensures the existence of an extension of $\overline{\varphi_D}$ satisfying conditions (7), (8) and (9) of Definition 2.4.

For elements in U_X^* we consider an arbitrary but fixed $q \in Q$ and make use of the fact (shown in Tabuada and Pappas, 2002b that a map $\phi_C^q : \mathrm{Inv}_X^q \to \mathrm{Inv}_Y^{\phi_D(p)}$ satisfying $T_x \phi_C^q(\mathscr{D}_X^q(x)) \subseteq \mathscr{D}_Y^{\phi_D(q)} \circ \phi_C^q(x)$ defines a unique map $\varphi_C^q : \mathrm{Inv}_X^q \times U_X^q \to U_Y^{\phi_D(p)}$ such that

for any pair $(x(t), u(t))$ of state and input trajectories of f_X^q, $(\phi_C^q, \varphi_C^q)(x(t), u(t))$ is a state and input trajectory of $f_Y^{\phi_D(q)}$. We now see that for any $u^{t'} \in U_X^*$ with codomain U_X^q we have:

$$\begin{aligned}\phi \circ \Phi_X(x, u^{t'}) &= (\phi_D(q), \phi_C^q \circ \gamma_x(t')) \\ &= \Phi_Y((\phi_D(q), \phi_C^q(x)), \varphi_C^q(x, u^{t'})) \end{aligned} \tag{20}$$

where γ_x is the integral curve of $f_q^X(x, u^{t'})$. Furthermore, by definition of ϕ_C^q we have $\phi_C^q(\mathrm{Inv}_X^q) \subseteq \mathrm{Inv}_Y^{\phi_D(q)}$ so that $\Phi_X(x, u^t) \in \mathrm{Inv}_X^q$ for every prefix u^t of $u^{t'}$ implies that $\Phi_Y(\phi_C^q(x), \varphi_C^q(x, u^t)) \in \mathrm{Inv}_Y^{\phi_D(q)}$ for every prefix $\varphi_C^q(x, u^t)$ of $\varphi_C^q(x, u^{t'})$. It then follows from (20) that we can define φ by $\{\varphi_C^q\}_{q \in Q}$ for elements in U^* as it satisfies conditions (7), (8) and (9) of Definition 2.4.

Having defined φ for elements in Σ_X and U^*, it follows that φ extends uniquely to $\mathscr{M}_X$ thereby defining a simulation (ϕ, φ) from H_X to H_Y. ■

The previous proposition can also be used in a more constructive way if used as a construction for hybrid abstractions. Before presenting the construction, we review some notions of invariance. Given a smooth map $f : M \to N$ we denote by Tf the tangent map or derivative of f. We will also use the notation $\ker(Tf)$ to denote the distribution consisting of all vector fields X such that $Tf(X) = 0$. Given a set A, we say that A is invariant under a vector field X if every trajectory of X starting in A will remain in A for all time. This notion is extended to invariance under a distribution by considering that A is invariant under every vector field belonging to a distribution. These concepts are now used in the following construction, which given H_X and ϕ, constructs H_Y simulating H_X.

CONSTRUCTION 4.3 (construction of abstractions) *Let* $H_X = (X, X_0, \Sigma_X, U_X, f_X, \mathrm{Inv}_X, \mathrm{Guard}_X, \mathrm{Reset}_X)$ *be a hybrid system,* $\phi = (\phi_D, \{\phi_C^q\}_{q \in Q}) : X \to Y$ *a pair of maps, with* $\phi_D : Q \to P$ *and* $\phi_C^q : \mathrm{Inv}_X^q \to \mathrm{Inv}_Y^{\phi_D(q)}$. *Hybrid system* $H_Y = (Y, Y_0, \Sigma_Y, U_Y, f_Y, \mathrm{Inv}_Y, \mathrm{Guard}_Y, \mathrm{Reset}_Y)$ *is obtained from* H_X *and* ϕ *by the following steps:*

1. $Y := f(X)$,
2. $Y_0 := f(X_0)$,
3. $\Sigma_Y := \Sigma_X$,
4. $U_Y := \{U_Y^p\}_{p \in P}, U_Y^{\phi_D(q)} = \cup_{q' \in \phi_D^{-1} \circ \phi_D(q)} \varphi_C^{q'}(U_X^{q'})$,
5. $f_Y^{\phi_D(q)} :=$ *the continuous abstraction*[6] *of every* $f_X^{q'}$ *such that* $q' \in \phi_D^{-1} \circ \phi_D(q)$,
6. $\mathrm{Inv}_Y^{\phi_D(q)} := \cup_{q' \in \phi_D^{-1} \circ \phi_D(q)} \phi_C^{q'}(\mathrm{Inv}_X^{q'})$,
7. $\mathrm{Guard}_Y^{(\phi_D(q), \sigma, \phi_D(q'))} := \cup_{q'' \in \phi_D^{-1} \circ \phi_D(q)} \phi_C^{q''}(\mathrm{Guard}_X^{(q'', \sigma, q')})$,
8. $\mathrm{Reset}_Y^{(\phi_D(q), \sigma, \phi_D(q'))} \circ \phi_C^q(x) := \cup_{q'' \in \phi_D^{-1} \circ \phi_D(q)} \phi_C^{q''}(\mathrm{Reset}_X^{(q'', \sigma, q')}(x))$.

The steps of the previous construction were designed so as to provide the conditions described in Proposition 4.2. The first step defines the new state space as the image of X by f. Since the invariants, guards and resets can be seen as subsets of the state space, they are also defined as the image of H_X invariants, guards and resets by f as described in steps 6, 7 and 8. Similarly, the space of continuous inputs U_Y is obtained as the image of U_X by the map φ_C, uniquely determined by ϕ as described in Tabuada and Pappas (2002b). Note, that in concrete applications the explicit computation of U_Y and φ is not necessary as the construction of continuous abstractions described in Pappas and Simic (2002) and required by step 5 provides the equations for the abstracted control system. The second step ensures that ''preservation of initial conditions'' is met while the third step defines the discrete labels in H_Y as the discrete labels in H_X.

This construction determines an abstraction of a given hybrid control system H_X based on the state aggregation map ϕ as asserted in the next result where the relevant assumptions on the input data are provided:

THEOREM 4.4 (computation of hybrid abstractions) *Given a hybrid control system H_X where the control systems f_X^q are control affine and a map $\phi = (\phi_D, \phi_C)$ where $\phi_D : Q \to P$ and $\phi_C = \{\phi_C^q\}_{q \in Q}$, $\phi_C^q : \mathrm{Inv}_X^q \to \mathrm{Inv}_Y^{\phi_D(q)}$ is a submersion, Construction 4.3 defines a hybrid control system H_Y which is a simulation of H_X.*

Proof: The result follows by Proposition 4.2 by considering:

- The map $\varphi_D : Q \times \Sigma_X \to \Sigma_Y$ defined by $\varphi_D(q, \sigma) = \sigma$ for every (q, σ) such that there exists a $x \in \mathrm{Inv}_X^q$ satisfying $((q, x), \sigma) \in \Phi_X^{-1}(X)$, where Φ_X is the abstract control system associated with hybrid control system H_X.

- The fact that $\mathscr{D}_Y^{\phi_D(q)}$ satisfies $T_x\phi_C^{q'}(\mathscr{D}_X^{q'}(x)) \subseteq \mathscr{D}_Y^{\phi_D(q)} \circ \phi_C^q(x)$ for every $x \in \mathrm{Inv}_X^{q'}$ and every $q' \in \phi_D^{-1} \circ \phi_D(q)$. ■

As was already discussed for abstract control systems, bisimulations provide sufficient as well as necessary conditions regarding reachability equivalence. It is therefore important to determine when the abstraction determined by Construction 4.3 is in fact a bisimulation. Sufficient conditions are presented in the following result:

THEOREM 4.5 (bisimilar hybrid systems): *Let $H_X = (X, X_0, \Sigma_X, U_X, f_X, \mathrm{Inv}_X, \mathrm{Guard}_X, \mathrm{Reset}_X)$ be a hybrid control system, $\phi = (\phi_D, \phi_C)$ a state aggregation map satisfying the conditions of Theorem 4.4 and $H_Y = (Y, Y_0, \Sigma_Y, U_Y, f_Y, \mathrm{Inv}_Y, \mathrm{Guard}_Y, \mathrm{Reset}_Y)$ the hybrid control system defined by Construction 4.3. If the following conditions are met:*

- *Continuous invariance—for every $q \in Q$:*
  - *$ker(T\phi_X^q)$ is controlled invariant for f_X^q.*
  - *Inv_X^q is invariant for $ker(T\phi_X^q)$.*

- *Every guard on discrete state q is invariant for $\ker(T\phi_X^q)$.*
- *The image by the reset maps (of discrete state q) of every point in its domain is invariant for $\ker(T\phi_X^q)$.*

- *Discrete invariance—$\phi_D(q) = \phi_D(q')$ implies:*
  - $T_x\phi_C^q(\mathscr{D}_X^q(x)) = T_x\phi_C^{q'}(\mathscr{D}_X^{q'}(x))$.
  - $\phi_C^q(\text{Guard}_X^{(q,\sigma,q'')}) = \phi_C^{q'}(\text{Guard}_X^{(q',\sigma,q''')})$, *for all* $q''' \in \phi_D^{-1} \circ \phi(q'')$.
  - $\phi_C^q(x) = \phi_C^{q'}(x) \Rightarrow \phi_C^q(\text{Reset}_X^{(q,\sigma,q'')}(x)) = \phi_C^{q'}(\text{Reset}_X^{(q',\sigma,q''')}(x))$, *for all* $q''' \in \phi_D^{-1} \circ \phi(q'')$.

then H_Y is a bisimulation of H_X.

Proof: As in the proof of Proposition 4.2 we consider that Σ_X, Σ_Y and φ_D have been extended so that (ϕ, φ) is a simulation from Φ_X to Φ_Y. We will show that (10) holds for elements in $\Sigma_X \cup U_X^*$ since the freeness properties of $\mathscr{M}_X$ will then imply that (10) holds for every element in $\mathscr{M}_X$.

We treat the continuous case first.

From the results reported in Tabuado and Pappas (2002a) we know that if $\ker(T\phi_C^q)$ is controlled invariant for a control system f_X^q, then its abstraction under the map ϕ_C^q is a bisimulation. If several discrete states are aggregated to the same continuous case, the resulting continuous abstraction is still a bisimulation since $\phi_D(q) = \phi_D(q')$ implies that the abstractions of f_X^q and $f_X^{q'}$ are the same. Furthermore, from invariance of Inv_X^q under $\ker(T\phi_X^q)$ we conclude that any continuous trajectory $x(t)$ leaves the invariant iff the abstracted trajectory $\phi_c^q(x(t))$ leaves the invariant, which means that continuous trajectories are well defined on the original system iff they are well defined in the abstraction. This shows that for any $(\phi(x), n) \in \Phi_Y^{-1}(Y)$, there exists a $(x, m) \in \mathscr{M}_X$ such that $\varphi(x, m) = n$, where Φ_X and Φ_Y are the abstract control systems associated with H_X and H_Y, respectively.

We now consider the discrete case. Assume that we have $\Phi_Y((p, y), \sigma) = (p', y')$ for the abstract control system Φ_Y associated with H_Y. This means that $(p, y) \in \text{Guard}_Y^{(p,\sigma,p')}$ and as the guards on H_X are invariant for $\ker(T\phi_C^q)$ and $\phi_D(q) = \phi_D(q')$ implies $\phi_C^q(\text{Guard}_X^{(q,\sigma,q'')}) = \phi_C^{q'}(\text{Guard}_X^{(q',\sigma,q'')})$ we have that every point $x \in (\phi_C^q)^{-1}(y)$ for $q \in \phi_D^{-1}(p)$ belongs to the guard associated with the transitions (q, σ, q'') where $q'' \in \phi_D^{-1} \circ \phi_D(p')$. It now follows from $\phi_C^q(\text{Reset}_X^{(q,\sigma,q'')}(x)) = \phi_C^{q'}(\text{Reset}_X^{(q',\sigma,q''')}(x))$ that for every $(q, x) \in \phi^{-1}(p, y)$ there exists a σ such that such that $\varphi_D((q, x), \sigma) = \sigma$ as required by (10). The result now follows from the freeness properties of $\mathscr{M}_X$. ■

The results regarding the computation of simulations and bisimulation are illustrated in the next section where a spark ignition example is discussed in detail. Furthermore, the proposed construction combined with Theorem 3.8 can be applied to complex hybrid systems to exploit interconnection. In that case the synchronizing set L depends on the specific composition operator used.

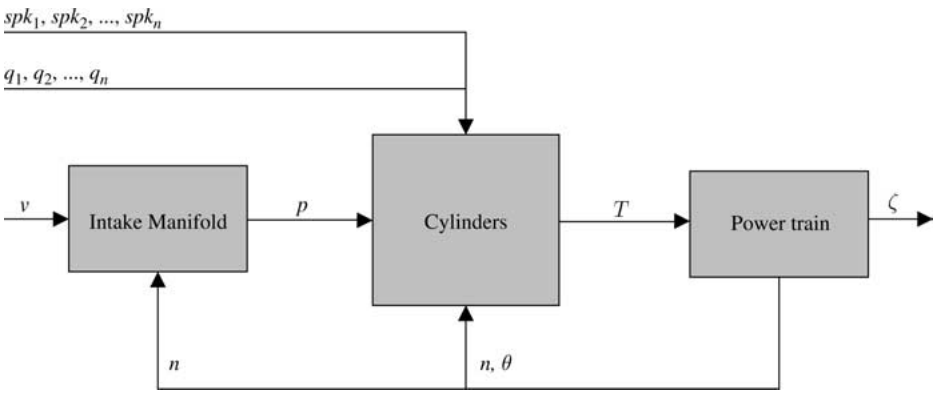


Figure 5. Block diagram representation of the spark ignition engine model.

5. A Spark Ignition Engine Example

We now illustrate the use of Construction 4.3 with a spark ignition engine model taken from Balluchi et al. (2000). Consider the block diagram representation displayed in Figure 5.

The intake manifold block models the throttle dynamics which can be controlled by applying a voltage v to regulate the throttle angle. This angle, regulates the pressure p from which the air inflow rate into the combustion chamber can be determined. The discrete operation of the n cylinders is modeled by the cylinders block which admits as inputs the injected fuel described by $q_1, q_2, \ldots, q_n$ and discrete inputs $spk_1, \ldots, spk_n$ controlling the spark advance with respect to the top most position of the pistons. Finally, the torque T produced by the cylinders is used in the power train block to determine the crack shaft angle θ, angular velocity n as well as other variables contained in the vector ζ. We defer the reader to Balluchi et al. (2000b) for a more detailed explanation of the model.

5.1. *Modeling the Cylinders*

The hybrid nature of the system comes from the interaction of the continuous dynamics describing the intake manifold and the power train, with the discrete nature of the cylinders evolution. Considering an engine with four cylinders, each cylinder is modeled by a state machine with six states, as displayed in Figure 6.

In the notation of Balluchi et al. (2000b), the state *I* models the intake phase where the combustion chamber is filled with the air-fuel mixture until reaching its top most position. The states *BS* and *PA* model the compression phase where the piston compresses the air–fuel mixture. The state *BS* models the before spark phase where no spark has yet occurred while the state *PA* models the positive advance phase, where a spark occurs before the piston reaches its top most position. The states *AS* and *NA* model the expansion phase. In the state *AS*, after spark, torque is being produced by the explosion of the mixture ignited by a spark. However, if no spark occurs before the piston reaches the top most position, the

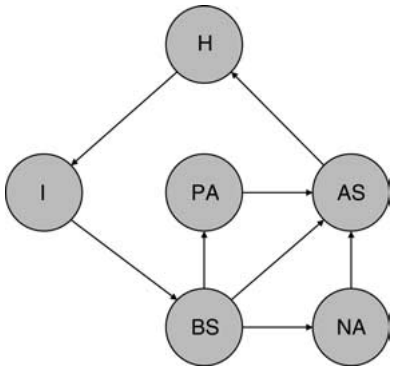


Figure 6. State machine modeling the discrete operation of each cylinders.

expansion phase initiates and no torque is produced, this is modeled by the state *NA*, negative advance. Finally the state *H* models the exhaust phase, where the gases produced in the combustion process are expelled from the combustion chamber. While the transitions $H \to I$, $I \to BS$, $BS \to NA$, $AS \to H$ depend only on the cylinder position, the remaining transitions depend on the discrete input *SPK* modeling the occurrence of a spark. Since several transitions depend on the position of the cylinder which is given by the continuous dynamics governing the power train, it is natural to combine the power train model with the state machine describing the cylinders in the hybrid automaton presented in Figure 7.

The continuous dynamics is also displayed in Figure 7, where the continuous states z_1, z_2 and z_3 are used to record the mass of air and fuel injected at the intake phase as well as the spark advance which will be used to determine the torque produced at the state *AS* as described in Balluchi et al. (2000b). Recording these values is in fact the justification for the several reset maps appearing on the hybrid automaton. The continuous dynamics is equal in every discrete state, except for the state *AS* where the produced torque *T* is added to the external torque T_e produced by the other pistons. The production of the torque T_e generated by the other pistons is not captured in this modeled so that T_e is treated as an input. The invariants of each mode are defined by bounds on the piston position measured by the crank shaft angle while the guards involve conditions on the crank shaft angle as well as the external input *SPK* modeling the occurrence of a spark. The remaining undefined constants and functions are irrelevant for our analysis and can be obtained from Balluchi et al. (2000b).

5.2. Abstracting the Hybrid Model

As in an engine several pistons run in parallel to generate torque, the model of the several pistons can be obtained by performing the parallel composition with synchronization of the hybrid automaton describing each piston. We consider an engine with four pistons, where each piston is described by the hybrid automaton displayed in Figure 7 having state

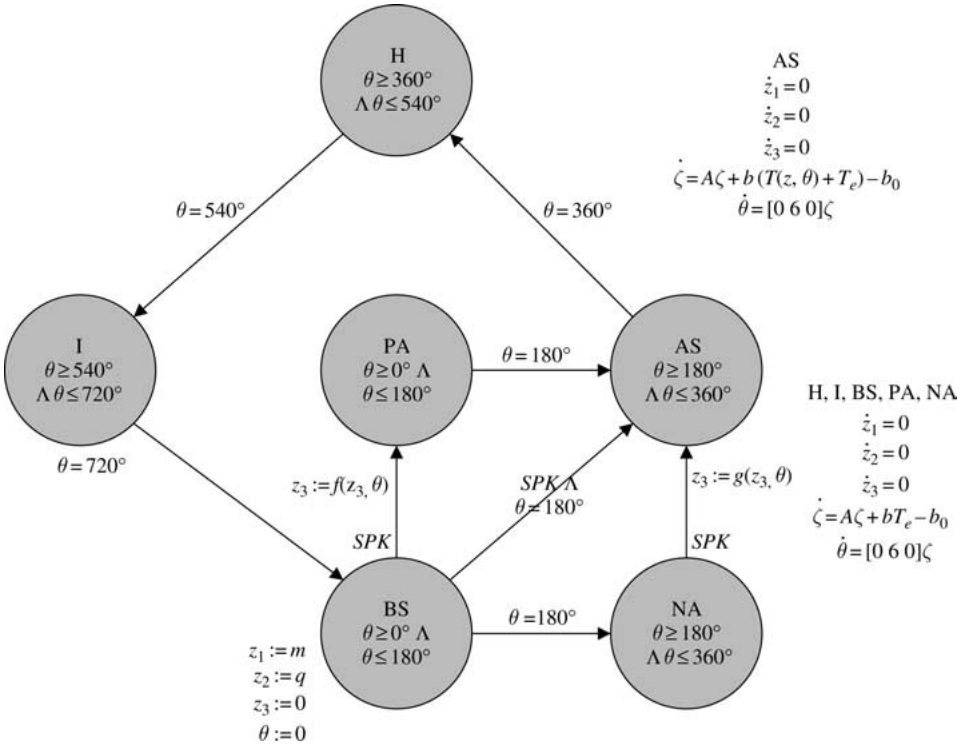


Figure 7. Hybrid automaton modeling each cylinder.

space $Q \times \mathbb{R}^6$ and input space $\mathbb{R}$. The synchronization between the pistons is then defined by the set $L \subseteq (Q \times \mathbb{R}^6 \times \mathbb{R})^4$:

$$L = \{(q, x, u) \in (Q \times \mathbb{R}^6 \times \mathbb{R})^4 : \theta_1 = \theta_2 + 180^\circ = \theta_3 + 360^\circ = \theta_4 + 540^\circ \wedge T_{ei} = \sum_{j \neq i} T_j \, i, j \in \{1, 2, 3, 4\}\} \tag{21}$$

We have, therefore, two approaches to compute an abstraction of the engine model. Either we abstract the model of each piston individually and then we compose the abstractions, or we abstract the model of the engine as a whole. Theorem 3.8 ensures that both approaches produce the same results which lead us to abstract each piston individually so as the reduce the complexity of the involved computations.

By inspecting Figure 7 we see that the states *PA*, *BS* and *NA* represent different phases leading the torque production phase. This suggests that they can be aggregated into a single before torque state, denoted by *BT*. This is accomplished by defining the discrete aggregation map $\phi_D : Q \to P$ to be:

$$\phi_D(PA) = \phi_D(BS) = \phi_D(NA) = BT, \quad \phi_D(AS) = AS, \quad \phi_D(H) = H, \quad \phi_D(I) = I$$

For the continuous state aggregation map we take the identity, that is:

$$\phi_C^q(x) = x, \quad \forall q \in \{I, PA, BS, AS, NA, H\}$$

Following the steps of Construction 4.3 we obtain:

1. $Y = \{BT, AS, H, I\} \times \mathbb{R}^7 = P \times \mathbb{R}^7 = f(X)$.

2. $Y_0 = Y = f(X)$ since the $X_0 = X$.

3. $\Sigma_X = \Sigma_Y$.

4. $U_Y^p = \mathbb{R}$ since we are not aggregating the continuous dynamics.

5. $f_Y^{\phi_D(q)} = f_X^q$ since we are not aggregating the continuous dynamics and the aggregated discrete states have the same continuous dynamics.

6. The invariants remain the same for the states AS, H and I, while the invariant of RT is given by $\text{Inv}_Y^{RT} = \phi_C^{PA}(\text{Inv}_X^{PA}) \cup \phi_C^{BS}(\text{Inv}_X^{BS}) \cup \phi_C^{NA}(\text{Inv}_X^{NA}) = \text{Inv}_X^{PA} \cup \text{Inv}_X^{BS} \cup \text{Inv}_X^{NA}$ and is given by the condition $0^\circ \leq \theta \leq 360^\circ$.

7. The guard $\text{Guard}_X^{(BS,BS \to PA,PA)}$ associated with the transition $BS \to PA$ remains unchanged as there is no continuous state aggregation. It is therefore expressed as $SPK \wedge \theta \leq 180^\circ$ since the guard is contained in the invariant. Similarly $\text{Guard}_X^{(PA,PA \to AS,AS)}$ is transformed to $\theta = 90^\circ$, $\text{Guard}_X^{(BS,BS \to AS,AS)}$ transformed to $SPK \wedge \theta = 90^\circ$, $\text{Guard}_X^{(BS,BS \to NA,NA)}$ transformed to $\theta = 180^\circ$ and finally $\text{Guard}_X^{(NA,NA \to AS,AS)}$ is transformed to $SPK \wedge 180^\circ \leq \theta$.

8. The reset $\text{Reset}_X^{(BS,BS \to PA,PA)}$ is now a reset from BT to BT, while the functional form f of the reset map does not change as there is no continuous state aggregation. Similarly $\text{Reset}_X^{(PA,PA \to AS,AS)}$, $\text{Reset}_X^{(BS,BS \to AS,AS)}$ and $\text{Reset}_X^{(BS,BS \to NA,NA)}$ remain the identity maps and $\text{Reset}_X^{(NA,NA \to AS,AS)}$ is now a reset from BT to AS with the same functional form given by the map g.

The resulting hybrid automaton is displayed in Figure 8.

We note that this abstraction fails to be a bisimulation since $\phi_C(\text{Inv}_X^{NA}) = \text{Inv}_X^{NA} \subseteq \text{Inv}_X^{BT} \neq \text{Inv}_X^{PA} = \phi_C(\text{Inv}_X^{PA})$ and this implies that for a continuous evolution starting at $\theta = 200^\circ$ on discrete state BT, there is no possible evolution of $PA \in \phi_D^{-1}(BT)$ that can be mapped to the evolution on state BT as evolutions in PA have to conform to the invariant.

This model can be further simplified by identifying the transition $BT \to BT$ guarded by $\theta = 180^\circ$ with the ε transition which is defined for every point in the invariant. Similarly, the transitions from BT to AS with guards $\theta = 180^\circ$ and $\theta = 180^\circ \wedge SPK$ can also be identified as they have equal reset maps. This can be formally done by considering a

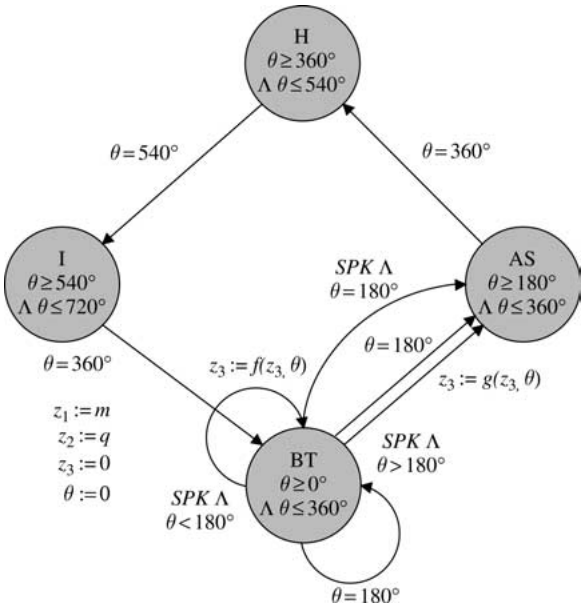


Figure 8. Abstraction of the hybrid automaton displayed in Figure 7.

simulation map which does not aggregate the states, but aggregates these transitions. Further aggregation is possible by identifying the states H, I and T which results in the hybrid automaton displayed in Figure 9.

This abstraction can now be composed with similar models of the remaining pistons to obtain the complete hybrid automaton describing the engine. For an engine with four pistons this is achieved by determining the product of four copies of the hybrid system displayed in Figure 9 followed by the operation of restriction. Following Theorem 3.8, the synchronization set is defined by $f_1 \times f_2 \times f_3 \times f_4(L)$ for the set L defined in (21) and maps $f_1 = f_2 = f_3 = f_4$ defining the state aggregation. Since the sequence of abstractions leading

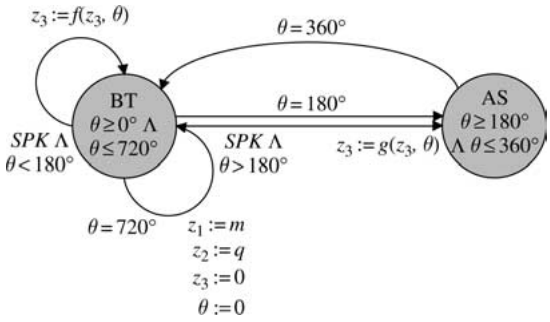


Figure 9. Abstraction of the hybrid automaton displayed in Figure 8.

to the hybrid model in Figure 9 was based on identity maps for continuous aggregation, it follows that:

$$f_1 \times f_2 \times f_3 \times f_4(L) = L$$

Restricting the product hybrid system to the set L leads to the following possible discrete configurations:

$$q_1 = (BT, BT, BT, AS)$$
$$q_2 = (BT, BT, AS, BT)$$
$$q_3 = (BT, AS, BT, BT)$$
$$q_4 = (AS, BT, BT, BT)$$
$$q_5 = (BT, BT, BT, BT)$$

However, the first four discrete states can also be abstracted into a single discrete state *TP* describing torque production, which leads to a hybrid system with only two discrete states *TP* and *NTP*, where *NTP* corresponds to state q_5, where no piston is producing torque. We note that a similar abstraction has been used in Balluchi et al. (2000c) to determine the maximal safe set for idle speed control of automotive engines, although it has not been obtained in any formal framework. The model used in Balluchi et al. (2000c) has three discrete states S, S_+ and S_-. State S_- corresponds to state *NTP* while both states S and S_+ correspond to our state *TP*. Two states are used in Balluchi et al. (2000c) to model the torque production phase to be able to distinguish between the before spark and after spark phases in the compression mode. In our model no such distinction is visible at the level of discrete states, but the continuous reset maps allow to update the variables z_1, z_2 and z_3 required to determine the correct value of the produced torque. We have thus been able to abstract the initial model, where each piston was modeled by a six states hybrid automaton to a hybrid system with only two discrete states modeling the synchronized operation of the four pistons. Furthermore, by exploiting compositionality we only performed the product of four hybrid systems with two discrete states each, resulting in a hybrid system with $2^4 = 16$ discrete states. If one would have abstracted the engine model as a whole, the required product hybrid system would have $2^4 = 1296$ discrete states. These numbers clearly illustrate the computational advantages of exploiting compositionality provided by Theorem 3.8. The resulting abstraction can now be used for analysis as is done, for example in Balluchi et al. (2000c), or synthesis.

6. Conclusions

In this paper we have addressed the problem of computing abstractions for hybrid control systems. A notion of abstraction was proposed based on the notions of simulation and bisimulation. These notions were presented in a general setting comprising discrete, continuous and hybrid control systems. Several important properties were proved in this

general setting which are directly applicable to hybrid systems. We also introduced a composition operator that allows to construct large-scale, complex hybrid systems by interconnecting smaller hybrid systems. We showed that this composition operator is compatible with abstractions and under certain conditions also with bisimulation. These results were then instantiated to hybrid control systems where a construction was proposed to compute abstractions based on state aggregation maps.

Several interesting directions for future research remain. It is important to understand how the proposed notions of bisimulation and abstraction can be compared with several other discussed in the literature, specially in the case when inputs and outputs are explicitly defined. Also important is to render the proposed results more computational by looking at special classes of hybrid control systems for which the abstraction process can be completely automated. The main difficulty that needs to be addressed is the automated computation of abstractions for purely continuous systems. While one does not hope to find computational approaches for all continuous systems, special classes such as linear systems are amenable to algorithmic approaches.

Appendix A. Functions, Partial Functions and Monoids

Functions and Partial Functions

We start by reviewing some facts regarding functions to set notation. Let $f: A \to B$ be a map, if S is a subset of A we denote by $f(S)$ the subset of B defined by:

$$f(S) = \cup_{s \in S} f(s) \tag{22}$$

We also use the set notation $f^{-1}(b)$ to refer to all points $a \in A$ such that $f(a) = b$ and if S is a subset of B we denote by $f^{-1}(S)$ the set:

$$f^{-1}(S) = \cup_{s \in S} f^{-1}(s) \tag{23}$$

Given maps $f: A \to B$ and $g: C \to D$, we represent by $f \times g: A \times C \to B \times D$ the map defined by $(a, c) \mapsto (f(a), g(c))$ for every $(a, c) \in A \times C$.

We now introduce some ideas regarding partially defined maps. Given a partially defined map $f: A \to B$, we denote the subset of A for which f is defined by $f^{-1}(B)$. Furthermore, given another partially defined map $g: A \to B$, we shall consider the two maps equal iff $g^{-1}(B) = f^{-1}(B)$ and $g|_{g^{-1}(B)} = f|_{f^{-1}(B)}$. Intuitively, two partially defined maps are equal when they are defined on the same subset of A and when restricted to that set, they are equal as ordinary maps. Composition is defined for partially defined maps $f: A \to B$ and $g: B \to C$ providing $g \circ f: A \to C$ defined on $(g \circ f)^{-1}(C) = f^{-1}(g^{-1}(C))$. We note that composition of partially defined maps is still an associative operation. We also extend the notion of restriction of a function to this context. For a given (partially defined or not) function $f: A \to B$ and a set $C \subseteq f^{-1}(B)$, we denote that by $f|_C: A \to B$ the partial function defined by:

$$\begin{cases} f|_C(a) = f(a) & \text{for every } a \in C \\ \text{undefined} & \text{otherwise} \end{cases} \tag{24}$$

Monoids

A monoid is a triple $(\mathscr{M}, \cdot, \varepsilon)$ where $\mathscr{M}$ is a set closed under the associative operation $\cdot : \mathscr{M} \times \mathscr{M} \to \mathscr{M}$ and ε is a special element of $\mathscr{M}$ called identity. This element satisfies $\varepsilon \cdot m = m \cdot \varepsilon = m$ for any $m \in \mathscr{M}$. We will usually denote $m_1 \cdot m_2$ simply by $m_1 m_2$ and refer to the monoid simply as $\mathscr{M}$. Given two elements m_1 and m_2 from $\mathscr{M}$ we say that m_1 is a prefix of m_2 iff there exists another $m \in \mathscr{M}$ such that $m_1 m = m_2$. Given two monoids $(\mathscr{M}_X, \cdot, \varepsilon_X)$ and $(\mathscr{M}_Y, \cdot, \varepsilon_Y)$ we denote by $\mathscr{M}_X \otimes \mathscr{M}_Y$ the direct product of $\mathscr{M}_X$ and $\mathscr{M}_Y$. The direct product, which is still a monoid, is defined by the set $\mathscr{M}_X \times \mathscr{M}_Y$ equipped with pairwise multiplication defined by:

$$(m, n)(m', n') = (mm', nn') \in \mathscr{M}_X \times \mathscr{M}_Y$$

for $(m, n), (m', n') \in \mathscr{M}_X \times \mathscr{M}_Y$ and where mm' denotes multiplication in $\mathscr{M}_X$ and nn' denotes multiplication in $\mathscr{M}_Y$. Finally, the unit in $\mathscr{M}_X \otimes \mathscr{M}_Y$ is naturally given by $(\varepsilon_X, \varepsilon_Y)$. A map $h : \mathscr{M} \to \mathscr{M}'$ between monoids is said a monoid homomorphism when $h(m_1 m_2) = h(m_1)h(m_2)$. A monoid $\mathscr{M}$ is said to be freely generated by a set S, when $S \subseteq \mathscr{M}$ and for any monoid $\mathscr{M}'$ and any map $i' : S \to \mathscr{M}'$, there is one and only one monoid homomorphism $h : \mathscr{M} \to \mathscr{M}'$ such that $h(s) = i'(s)$ for any $s \in S$. Freely generated monoids $\mathscr{M}$ thus have the property that to define a monoid homomorphism h from $\mathscr{M}$ to any other monoid $\mathscr{M}'$, it suffices to define h on S since a unique extension of h to $\mathscr{M}$ exists.

Appendix B. Elementary Notions of Category Theory

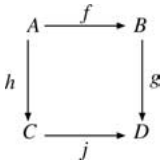
Categories

In this paper we only use elementary notions of category theory. We point the reader to Lane (1971) for further details as well to Lawvere and Schannel (1997) and Arbih and Manes (1975) for a ''softer'' introduction to the topic. Informally speaking, a category is a universe of mathematical discourse and is perhaps better described by examples. If one is interested in group theory one would certainly work in the universe of groups and group homomorphism, whereas if one is learning elementary topology the natural universe are topological spaces and continuous maps between them. In linear algebra one deals with vector spaces and linear maps, in differential geometry with smooth manifolds and smooth maps between them, etc. This idea of universe of mathematical discourse can be formally defined as follows:

DEFINITION 6.1 (category) *A category is a tuple* $(\mathscr{O}, \hom, \mathrm{id}, \circ)$ *consisting of:*

- *A class of objects* $\mathcal{O}$.
- *For each pair of objects* (A,B) *belonging to* $\mathcal{O}$*, a set* $\hom(A,B)$. *The elements of* $\hom(A,B)$ *are called morphisms from A to B. An element of this set* $f \in \hom(A,B)$ *is usually denoted graphically as* $A \xrightarrow{f} B$.
- *For each object* $A \in \mathcal{O}$ *a special morphism* $A \xrightarrow{\mathrm{id}_A} A$, *called the identity on A*.
- *A binary operation which maps a pair of morphisms* $(A \xrightarrow{f} B, B \xrightarrow{g} C)$ *to the composite*[7] $A \xrightarrow{g \circ f} C$ *while satisfying:*
  - *Associativity:* $h \circ (g \circ f) = (h \circ g) \circ f$ *whenever the composition is defined.*
  - *Identity: for a morphism* $A \xrightarrow{f} B$ *we have* $\mathrm{id}_B \circ f = f = f \circ id_A$.
- *The sets* $\hom(A,B)$ *and* $\hom(C,D)$ *are disjoint when* $A \neq C$ *or* $B \neq D$.

In the above examples the objects are the groups, topological spaces, etc., while the arrows are the group homomorphisms, continuous maps, etc., between them. As morphisms are displayed graphically, more elaborate relations between morphisms are usually displayed in commutative diagrams. We shall say that a diagram commutes iff the composition of morphisms in any path from one object to another object is the same. Consider for example the following diagram

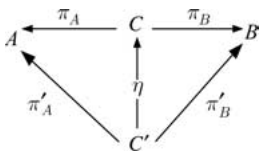


(25)

where commutativity simply means that the two existing paths from A to D are equal, that is $g \circ f = j \circ h$.

Products

Let A and B be objects in a category. The product of A and B is the triple (C, π_A, π_B) such that for any other triple (C', π'_A, π'_B) there exists one and only one morphism η making the following diagram commutative:

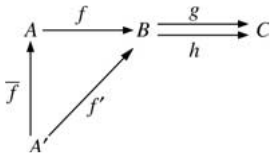


(26)

Note that the product captures the relevant notion of product with respect to the corresponding category. The product on the category of sets and maps between them is the usual Cartesian product, while in the category of groups is the direct product, in the category of topological spaces is the Cartesian product of the supports equipped with the product topology, etc. Reversing the arrows in diagram (26) leads to the dual notion of coproduct.

Equalizers

Let g and h be morphisms in a category. The equalizer of g and h is the morphism f satisfying $g \circ f = h \circ f$ and such that for any other morphism f' satisfying $g \circ f' = h \circ f'$ there is one and only one morphism $\overline{f}$ such that the following diagram commutes:



(27)

Acknowledgments

This research was performed while the first author was a Ph.D. student at the Institute for Systems and Robotics, Instituto Superior Técnico and a visiting student at the Department of Electrical and Systems Engineering at the University of Pennsylvania. This research was partially supported by Fundação para a Ciência e Tecnologia under grant PRAXIS XXI/BD/18149/98, and the National Science Foundation Information Technology Research Grant CCR01-21431. The authors would like to thank Esfandiar Haghverdi for extremely stimulating discussions on category theory, and its use for hybrid systems.

Notes

1. Nondeterministic transition relations can also be captured by parameterizing the nondeterminism. This can be accomplished by modeling Σ as $\Sigma = \Sigma_c \times \Sigma_u$, where the labels in Σ_c are regarded as controllable inputs, while the labels in Σ_u are regarded as uncontrollable inputs or disturbances. This allows to model nondeterminism since $\delta(q, (\sigma_c, \sigma_u))$ is a set of states parameterized by the labels $\sigma_u \in \Sigma_u$, which are independent of the choice σ_c.
2. Technically speaking, we allow only classes of maps $u(t)$ for which the solution of $f(x(t), u(t))$ is well defined. However, our results are independent of the chosen class.
3. There exists only one function from $[0, t]$ to a singleton, the constant map.
4. See, for example, Appendix B for a definition of coproduct.
5. This notion of product corresponds to the product in the category of abstract control systems. See, for example, Appendix B for a definition of product in a category.

6. Continuous abstractions are discussed in Pappas et al. (2000) for linear systems and in Pappas and Simic (2002) for nonlinear systems. However, in these references abstractions of a single control system are considered whereas in the present situation it may be necessary to determine an abstraction of several control systems for which the results of Pappas et al. (2000) and Pappas and Simic (2002) can be easily extended. Consider, for example, two control affine systems defined by the affine distributions $X_1 + \Delta_1$ and $X_2 + \Delta_2$ and an aggregation map $\phi : M \to N$. If $T_x\phi(X_1(x)) = T_x\phi(X_2(x))$ for every $x \in M$, then the abstraction of both control systems is simply given by $T\phi(X_1 + \Delta_1) + T\phi(X_2 + \Delta_2)$, otherwise we can take as an abstraction $T\phi(X_1 + \Delta_1) + \text{span}(T\phi(X_2)) + T\phi(\Delta_2)$ or $T\phi(X_2 + \Delta_2) + \text{span}(T\phi(X_1)) + T\phi(\Delta_1)$.
7. Note that composition of f and g is only defined if the target of f equals the source of g.

References

Alur, R., Belta, C., Ivancic, F., Kumar, V., Mintz, M., Pappas, G. J., Rubin, H., and Schug, J. 2001. Hybrid modeling and simulation of biomolecular networks. In Maria Domenica Di Benedetto and Alberto Sangiovanni-Vicentelli (eds), *Hybrid Systems: Computation and Control*, volume 2034 of *Lecture Notes in Computer Science*, Springer Verlag, Rome, Italy pp. 19–32.

Alur, R., Courcoubetis, C., Halbwachs, N., Henzinger, T. A., Ho, P. H., Nicollin, X., Olivero, A., Sifakis, J., and Yovine, S. 1995. Hybrid automata: An algorithmic approach to specification and verification of hybrid systems. *Theoretical Computer Science* 138(1): 3–34.

Asarin, E., Caspi, P., and Maler, O. 2002. Timed regular expressions. *Journal of the ACM* 49(2): 172–206.

Alur, R., Henzinger, T., Lafferriere, G., and Pappas, G. J. 2000. Discrete abstractions of hybrid systems. *Proceedings of the IEEE* 88(7): 971–984.

Arbib, M., and Manes, E. G. 1974. Machines in a category: An expository introduction. *SIAM Review* 16(2): 163–192.

Arbib, M. A., and Manes, E. G. 1975. *Arrows, Structures and Functors—The Categorical Imperative*. New York: Academic Press Inc.

Balluchi, A., Benvenuti, L., Di Benedetto, M. D., Pinello, C., and Sangiovanni-Vicentelli, A. L. 2000. Automotive engine control and hybrid systems: Challenges and opportunities. *Proceedings of the IEEE* 88(7): 888–912.

Balluchi, A., Benvenuti, L., Miconi, G. M., Pozzi, U., Villa, T., Di Benedetto, M. D., Wong-Toi, H., and Sangiovanni-Vincentelli, A. L. 2000c. Maximal safe set computation for idle speed control of an automotive engine. In Nancy Lynch and Bruce H. Krogh (eds), *Hybrid Systems: Computation and Control*, volume 1790 of *Lecture Notes in Computer Science*, Springer Verlag, pp. 32–44.

Barret, G., and Lafortune, S. 1998. Bisimulation, the supervisor control problem and strong model matching for finite state machines. *Journal of Discrete Event Systems* 8(4): 337–429.

Cury, J. E. R., Krogh, B. H., and Ninomi, T. 1998. Synthesis of supervisory controllers for hybrid systems based on approximating automata. *IEEE Transactions on Automatic Control: Special Issue on Hybrid Systems* 43(4): 564–568.

Cassandras, C., and Lafortune, S. 1999. *Introduction to Discrete Event Systems*. Boston, MA: Kluwer Academic Publishers.

Caines, P. E., and Wei, Y. J. 1998. Hierarchical hybrid control systems: A lattice theoretic formulation. *IEEE Transactions on Automatic Control: Special Issue on Hybrid Systems* 43(4): 501–508.

de Alfaro, L., and Henzinger, T. A. 2001. Interface theories for component-based design. In *Proceedings of the First International Workshop on Embedded Software*, volume 2211 of *Lecture Notes in Computer Science*, pp. 148–165.

Gokbayrak, K., and Cassandras, C. G. 2000. Hybrid controller for hierarchically decomposed systems. In Nancy Lynch and Bruce H. Krogh (eds), *Hybrid Systems: Computation and Control*, volume 1790 of *Lecture Notes in Computer Science*, Springer Verlag, pp. 117–129.

Hespanha, J., Bohacek, S., Obraczka, K., and Lee, J. 2001. Hybrid modeling of tcp congestion control. In Maria Domenica Di Benedetto and Alberto Sangiovanni-Vicentelli (eds), *Hybrid Systems: Computation and Control*, volume 2034 of *Lecture Notes in Computer Science*, Springer Verlag, pp. 291–304.

Henzinger, T. A. 1996. The theory of hybrid automata. In *Proceedings of the 11th Annual IEEE Symposium on Logic in Computer Science*, IEEE Computer Society Press, pp. 278–292.

Howie, J. M. 1995. *Fundamentals of Semigroup Theory.* Oxford Science Publications.

Hopcroft, J. E., and Ullman, J. D. 1979. *Introduction to Automata Theory, Languages and Computation*. USA: Addison-Wesley Publishing Company.

Johansson, K. H., Egersted, M., Lygeros, J. and Sastry, S. 1999. On the regularization of hybrid automata. *Systems and Control Letters* 38: 141–150.

Kumar, R., and Garg, V. K. *Modeling and Control of Logical Discrete Event Systems*. Kluwer Academic Publishers.

Lane, S. M. 1971. *Categories for the Working Mathematician*. Springer-Verlag.

Lawvere, F. W., and Schannel, S. H. 1997. *Conceptual Mathematics: A First Introduction to Categories*. New York: Cambridge University Press.

Lynch, N., Segala, R., and Vaandrager, F. 2001. Hybrid I/O automata revisited. In *Hybrid Systems: Computation and Control*, volume 2034 of *Lecture Notes in Computer Science*, Springer Verlag, pp. 403–417.

Moor, T., and Davoren, J. M. 2001. Robust controller synthesis for hybrid systems using modal logic. In *Hybrid Systems: Computation and Control*, volume 2034 of *Lecture Notes in Computer Science*, Springer Verlag, pp. 433–446.

Milner, R. 1989. *Communication and Concurrency.* Prentice Hall.

Manna, Z., and Pnueli, A. 1992. *The temporal Logic of Reactive and Concurrent Systems: Specification*. Berlin: Springer-Verlag.

Manna, Z., and Pnueli, A. 1995. *Temporal Verification of Reactive Systems: Safety.* Berlin: Springer-Verlag, January.

Madhusudan, P., and Thiagarajan, P. S. 2002. Branching time controllers for discrete event systems. *Theoretical Computer Science* 274: 117–149.

Niebert, P. and Yovine, S. 2000. Computing optimal operation schemes for chemical plants in multi-batch mode. In Nancy Lynch and Bruce H. Krogh (eds), *Hybrid Systems: Computation and Control*, volume 1790 of *Lecture Notes in Computer Science*, Springer Verlag, pp. 338–351.

Pappas, G. J. 2003. Bisimilar linear systems. *Automatica* 39(12): 2025–2033.

Pappas, G. J., Lafferriere, G., and Sastry, S. 2000. Hierarchically consistent control systems. *IEEE Transactions on Automatic Control* 45(6): 1144–1160.

Pappas, G. J., and Simic, S. 2002. Consistent hierarchies of affine nonlinear systems. *IEEE Transactions on Automatic Control* 47(5): 745–756.

Park, D. M. R. 1980. *Concurrency and automata on infinite sequences*, volume 104 of *Lecture Notes in Computer Science*. Springer-Verlag.

Roggenbach, M., and Majster-Cederbaum, M. 2000. Towards a unified view of bisimulation: A comparative study. *Theoretical Computer Science* 1(238): 81–130.

Raisch, J., and O'Young, S. D. 1998. Discrete approximations and supervisory control of continuous systems. *IEEE Transactions on Automatic Control: Special Issue on Hybrid Systems* 43(4): 569–573.

Rutten, J. J. M. M. 2000. Universal coalgebra: A theory of systems. *Theoretical Computer Science* 249(1): 3–80.

Ramadge, P. J., and Wonham, W. M. 1982. Supervisory control of discrete event processes. In A. V. Balakrishnan and M. Thoma (eds), *Feedback Control of Linear and Nonlinear Systems*, volume 39 of *Lecture Notes in Control and Information Sciences*, Berlin: Springer-Verlag, pp. 202–214.

Sontag, E. D. 1998. *Mathematical Control Theory*, volume 6 of *Texts in Applied Mathematics*, 2nd edition. New-York: Springer-Verlag.

Tabuada, P., and Pappas, G. J. 2001. Hybrid abstractions that preserve timed languages. In Marica Domenica di Benedetto and Alberto L. Sangiovanni-Vincentelli (eds), *Hybrid Systems: Computation and Control*, volume 2034 of *Lecture Notes in Computer Science*, Springer Verlag, pp. 501–514.

Tabuada, P., and Pappas, G. J. 2002a. Bisimilar control affine systems. In *Proceedings of the 41st IEEE Conference on Decision and Control*, Las Vegas, NV, December.

Tabuada, P., and Pappas, G. J. 2002b. Quotients of fully nonlinear control systems. In D. Gilliam and J. Rosenthal, (eds), *Proceedings of 15th International Symposium on Mathematical Theory of Networks and Systems*, South Bend, Indiana, August. Extended version available at www.nd.edu/ ∼ ptabuadap

Tabuada, P., Pappas, G. J., and Lima, P. 2002. Composing abstractions of hybrid systems. In Claire Tomlin and Mark R. Greenstreet (eds), *Hybrid Systems: Computation and Control*, volume 2289 of *Lecture Notes in Computer Sience*, Springer-Verlag, pp. 436–450.

Tomlin, C., Pappas, G. J., and Sastry, S. 1998. Conflict resolution for air traffic management: A study in muti-agent hybrid systems. *IEEE Transactions on Automatic Control* 43(4): 509–521.

Winskel, G., and Nielsen, M. 1994. Models for concurrency. In Abramsky, Gabbay, and Maibaum (eds), *Handbook of Logic and Foundations of Theoretical Computer Science*, volume 4. London: Oxford University Press.