Proceedings of the
47th IEEE Conference on Decision and Control
Cancun, Mexico, Dec. 9-11, 2008

Composing hybrid systems

Luca Benvenuti*†, Alberto Ferrari†, Emanuele Mazzi†‡§, Alberto Sangiovanni Vincentelli†§

*Università di Roma ”La Sapienza”, Roma, Italy. Email: luca.benvenuti@uniroma1.it
†PARADES, Via di S.Pantaleo, 66, 00186 Roma, Italy. Email: {aferrari, emazzi}@parades.rm.cnr.it
‡Centro di Ricerca Interdipartimentale ”E. Piaggio”, Università di Pisa, Pisa, Italy. Email: emanuele.mazzi@ing.unipi.it
§Department of Electrical Engineering and Computer Sciences,
University of California at Berkeley, Berkeley, CA 94720, USA. Email: {alberto,emazzi}@eecs.berkeley.edu

Abstract— **Hybrid systems are useful abstractions of embedded controllers. However, they are notoriously very difficult to verify as computation complexity grows quickly with the size of the hybrid system. We address the problem of building in a systematic way a compact representation of a hybrid system obtained by composing hybrid subsystems. This technique can be used as a front-end to any hybrid formal verification tool thus freeing the designer from the cumbersome and error-prone manual calculation of the composition and of its reduction. Critical to the efficiency of the method are: i) hiding the internal signals and synchronization events between components; ii) eliminating locations that result in empty invariant conditions as well as non reachable locations; iii) using the notion of equivalent locations for a labeled transition system associated to the hybrid system to compute an equivalent minimal realization of the composed hybrid system.**

I. Introduction

In safety critical applications such as transportation systems, the electronic control system is often a networked system with interacting embedded controllers. For example, the electronic control system for automobiles is a networked system with an embedded controller for each subsystem, engine control unit, gear-box controller, anti-lock braking system (ABS), dashboard controller, and vehicle dynamic control (VDC) [1]. These embedded controllers interact asynchronously over a communication network. Their integration has become a design bottleneck due to their complexity as well as to the lack of an overall understanding of their interplay. Consequently, effective management of controller interactions can be achieved only by formulating the design and verification problems at a level of abstraction that is high enough to allow analyzing the properties of interest in a quantitative way. Hybrid systems are effective abstractions for modeling the behavior of each embedded controller as well as of the plant to be controlled. However, a more powerful way of using this formalism is to address the global verification issues where plant and controllers are considered together. We could then capture the effects of limited resources and physical constraints on the performance of the controlled system and check the correctness of the design. The problem of practically composing hybrid systems is one of great importance, as any practical hybrid model is inherently complex. Breaking up this model into simpler and accurate components and then obtaining the full model through composition would greatly increase the possibility of analyzing and understanding the overall complex model.

In this paper, we address the problem of building automatically a *compact representation* of a hybrid system obtained by composing hybrid subsystems. Critical to the efficiency of the method are: i) hiding the internal signals and synchronization events between components; ii) eliminating locations that result in empty invariant conditions as well as non reachable locations; iii) using the notion of equivalent locations for a labeled transition system associated to the hybrid system to compute an equivalent minimal realization of the composed hybrid system. A procedure of this sort could be added as a front-end to any verification tool to alleviate the difficulties of designers in using formal verification methods for hybrid systems since the composition and its reduction are today manually computed. The problem of compatibility and verification of hybrid systems composition has been investigated in [2].

Several attempts have been made in literature to tackle the parallel composition problem (see [3], [4], [5]). For example, composition via the IO approach, via variable sharing, categorically, by looking at the preservation of properties, or studying the rise of pathological ones. In this paper we instead consider the cascade and feedback composition of hybrid systems.

The paper is organized as follows. In Section II the class of hybrid system handled by the methodology is defined. In Section III, the composition of hybrid subsystems is presented. In Section IV, we show how to minimize the size of the composed hybrid systems via a number of techniques that include the computation of its minimal realization. In Section V, a water tank control example is introduced and its component models described. In Section VI, the application of the methodology for constructing the overall water tank control system model is presented. In Section VII, the reduction techniques are applied to the test case.

II. Hybrid systems

Hybrid systems are dynamical systems where the behavior of interest is determined by interacting continuous and

This research has been sponsored in parts by the European Integrated Project SPEEDS integrated project number 033471, by CHESS at UC Berkeley, by the HYCON Network of Excellence, contract number FP6-IST-511368 and COMBEST.

978-1-4244-3124-3/08/$25.00 ©2008 IEEE

discrete dynamics. In this paper, we consider the case in which the continuous–time dynamics is modeled by means of differential equations and the discrete–event dynamics is modeled by automata. The continuous part $x(t)$ of the state of the hybrid system takes on values in a set $X \subset \mathbb{R}^n$, while the discrete state q, called *location*, takes on values in a finite set Q of dimension d. Given a location q, the continuous part $x(t)$ of the state evolves in time according to the differential equations

$$\begin{array}{l} \dot{x}(t) = f(q, x(t), u(t)) \\ y(t) = h(q, x(t), u(t)) \end{array} \tag{1}$$

where $u(t)$ are the continuous input variables taking on values in $U \subset \mathbb{R}^m$ and $y(t)$ are the continuous output variables taking on values in $Y \subset \mathbb{R}^p$.

The evolution of the discrete part q of the state may be described by means of a transition relation

$$R : Q \times X \times \Sigma \times U \to 2^{Q \times X \times \Gamma}$$

where σ are the input events taking on values in a finite set of symbols Σ and γ are the output events taking on values in a finite set of symbols Γ. The sets Σ and Γ include the special symbols ϵ representing the absence of an input or output event. The evolution may be also described by means of a digraph (Q, E), or its corresponding adjacency matrix M, with vertices corresponding to the locations q, and edges $E \subset Q \times Q$ representing the possible transitions between locations

$$\begin{array}{rcl} E & = & \{(q, q') \in Q \times Q | (q', x', \gamma) \in R(q, x, \sigma, u) \\ & & \text{for some } x, x' \in X, \sigma \in \Sigma, u \in U \text{ and } \gamma \in \Gamma\} \end{array}$$

The transition from location q to location $q\prime$ is possible only for some state and input values: this is modeled associating to each edge a guard

$$\begin{array}{rcl} G(q, q') & = & \{x, \sigma, u \in X \times \Sigma \times U | (q', x', \gamma) \in R(q, x, \sigma, u) \\ & & \text{for some } x' \in X \text{ and } \gamma \in \Gamma\} \end{array}$$

and an output event $\gamma(q, q') \in \Gamma$. For each location q, the continuous part $x(t)$ of the state may evolve until some invariant conditions are verified, that is $(x(t), \sigma, u(t)) \in D(q)$ with $D \subset X \times \Sigma \times U$ Moreover, the initial state of the hybrid system must be in the set $Init \subset Q \times X$

In summary, a hybrid system $\mathcal{H}$ is formally described by the collection

$$\mathcal{H} = ((Q, X), (\Sigma, U), (\Gamma, Y), (f, h), (E, G, \gamma), D, Init)$$

III. Composing hybrid systems

When considering the cascade and feedback composition of two hybrid systems $\mathcal{H}_1$ and $\mathcal{H}_2$ as shown in figure 1, the hybrid system $\mathcal{H}$ modeling the composition has the following properties:

- the finite set Q of discrete states is the cartesian product of the sets Q_1 and Q_2, that is $Q \subset Q_1 \times Q_2$;
- the set X of continuous states is obtained by the union of the set X_1 and X_2, that is $X = X_1 \cup X_2$;

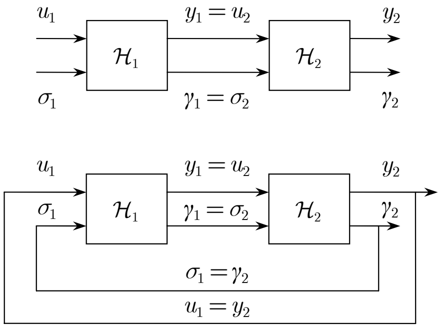

Fig. 1. Hybrid systems cascade and feedback composition

- the input and output sets, in the cascade composition, are: $\Sigma = \Sigma_1$, $U = U_1$, $\Gamma = \Gamma_2$, $Y = Y_2$, while, in the feedback composition, the output set is $\Gamma = \Gamma_2$, $Y = Y_2$ and no input is defined.
- when in location $q = (q_i, q_j)$, with $q_i \in Q_1$ and $q_j \in Q_2$, the continuous part of the state evolves according to the following differential equations:

  $$\begin{array}{rcl} \dot{x_1}(t) & = & f_1(q_i, x_1(t), u_1(t)) \\ \dot{x_2}(t) & = & f_2(q_j, x_2(t), y_1(t)) \\ y(t) & = & h_2(q_j, x_2(t), y_1(t)) \end{array}$$

  when considering the cascade composition, and to

  $$\begin{array}{rcl} \dot{x_1}(t) & = & f_1(q_i, x_1(t), y_2(t)) \\ \dot{x_2}(t) & = & f_2(q_j, x_2(t), y_1(t)) \\ y(t) & = & h_2(q_j, x_2(t), y_1(t)) \end{array}$$

  when considering the feedback composition.
- when in location $q = (q_i, q_j)$, some variables may be subject to more than one invariant conditions. For example, x_1 may be subject to the invariant conditions related to location q_i and to the invariant conditions on $u_2 = y_1 = h_1(q_i, x_1, \sigma_1, u_1)$ related to location q_j. As a consequence, the invariant conditions related to disjoint variables are the union of the invariant conditions on these variables, while those related to joint variables are their intersection. We adopt the symbol $\oplus$ to indicate such composition, i.e. $D((q_i, q_j)) = D(q_i) \oplus D(q_j)$.
- the continuous part of the set $Init \subset (Q_1 \times Q_2) \times (X_1 \times X_2)$ of initial states is obtained, for each location $q = (q_i, q_j)$, as

  $$\{x_1 \in X_1, x_2 \in X_2 | (q_i, x_1) \in Init_1, (q_j, x_2) \in Init_2\}$$

- the set E of edges corresponds to the adjacency matrix $M \in \mathbb{R}^{(d_1 \cdot d_2) \times (d_1 \cdot d_2)}$ obtained by the following combination of the adjacency matrices $M^1 \in \mathbb{R}^{d_1 \times d_1}$ and $M^2 \in \mathbb{R}^{d_2 \times d_2}$ associated to digraphs (Q_1, E_1) and (Q_2, E_2) respectively:

  $$M = \begin{pmatrix} M_{1,1} & \cdots & M_{1,d_1} \\ \vdots & & \vdots \\ M_{d_1,1} & \cdots & M_{d_1,d_1} \end{pmatrix}, M_{i,j} = \begin{cases} M^2 & \text{if } i = j \\ m^1_{i,j}(I \vee M^2) & \text{if } i \neq j \end{cases}$$

where $m^1_{i,j}$ is the (i, j) element of the matrix M^1;

- if there exists an edge between locations $(q_i, q_h) \in Q_1 \times Q_2$ and $(q_j, q_k) \in Q_1 \times Q_2$, that is $M_{i,j}(h, k) = 1$, then the guard conditions G associated to it is obtained by the combination of the guards G_1 and G_2 as follows:

$$G((q_i, q_h), (q_j, q_k)) = \begin{cases} G_1(q_i, q_j) \text{ if } h = k \\ G_2(q_h, q_k) \text{ if } i = j \\ G_1(q_i, q_j) \oplus G_2(q_h, q_k) \text{ otherwise} \end{cases}$$

IV. Reduction techniques

a) Transition elimination: Some transitions can be eliminated when considering the composed hybrid system. In particular, the generic transition from location (q_i, q_h) to location (q_j, q_k) will never take place if:

1) the guards conditions composition results in an empty set, i.e. $G((q_i, q_h), (q_j, q_k)) = \emptyset$;
2) transition from location q_h to location q_k of the hybrid system $\mathcal{H}_2$ is forced by an input event which is not generated as output when the transition from location q_i to location q_k takes place in the hybrid system $\mathcal{H}_1$ (also the vice versa holds true when considering a feedback composition);
3) transition from location q_i to location q_k of the hybrid system $\mathcal{H}_1$ produces an output event forcing, in the hybrid system $\mathcal{H}_2$, a transition different from that from location q_h to location q_k (also the vice versa holds true when considering a feedback composition);
4) the guards conditions composition is equal to $G_1(q_i, q_j) \wedge G_2(q_h, q_k)$ and there exists a sequence of two transitions starting from location (q_i, q_h) and leading to location (q_j, q_k) (passing through an halfway location) that take place at the same time and are activated by the guards condition $G_1(q_i, q_j)$ and $G_2(q_h, q_k)$. In this case the given transition can be eliminated since it is redundant.

b) Location elimination: The number of locations necessary to describe the hybrid systems composition may be reduced and may be much lesser than $d_1 \cdot d_2$. In fact, the location (q_i, q_j) of the hybrid system $\mathcal{H}$ can be eliminated if one of the following condition holds:

1) the invariant conditions associated to the location is the empty set;
2) the location is not reachable, that is in the digraph (Q, E) there does not exist a path to the location from a vertex $q \in Q$ such that $q \in Init$ for some $x_1 \in X_1$ and $x_2 \in X_2$;

c) Equivalent location elimination: Finally, the number of locations of the hybrid system can be further reduced computing the minimal order hybrid system, that is unifying locations that result to be equivalent. To do this, the hybrid system model is projected to the discrete domain, by abstracting away continuous dynamics (see [6]). A *labeled transition system*, referred to as $\mathcal{T}$, associated to the hybrid system $\mathcal{H}$ is introduced and it is characterized by the same sets Q and E of discrete states and edges of the hybrid model $\mathcal{H}$. To each guard condition is associated the discrete event $\omega \in \Omega$ activating the corresponding transition as soon as the guard condition is satisfied. Moreover, the labeled transition system $\mathcal{T}$ is characterized by a set $\pi(q) \in \Pi$ of observations and $\langle\langle\cdot\rangle\rangle$ is the observation map that associates to $\pi(q)$ the vector fields f, h regulating the evolution of the continuous time state and output in location $q \in Q$, according to equation (1). The labeled transition system $\mathcal{T}$ is formally described by the collection $\mathcal{T} = (Q, \Omega, E, \Pi, \langle\langle\cdot\rangle\rangle)$ (see [7], [8]).

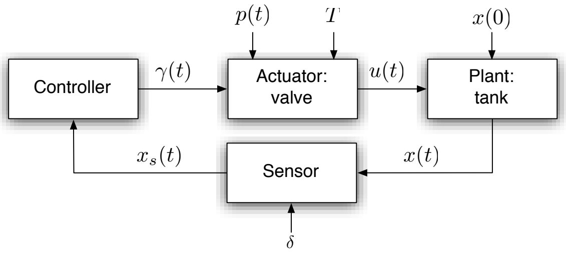

Fig. 2. Feedback composition of the components

The transition system $\mathcal{T}$ can be used to identify equivalent locations (see [9]):

Definition 1: Two states q_i and q_j belonging to the labeled transition system $\mathcal{T}$ are equivalent if the corresponding outputs $\pi(q_i)$ and $\pi(q_j)$ are equal and for all discrete inputs ω the next states $q_i \xrightarrow{\omega} q'_i$ and $q_j \xrightarrow{\omega} q'_j$ are equivalent too.

Equivalence relations are computed by the *Table of Implications*, obtained as follows:

- the symbol $\nsim$: if states are not equivalent;
- the symbol $\sim$: if states are equivalent;
- a pair of states whose equivalence implies the equivalence of the states corresponding to the entry.

By solving the implications defined in the third type of entries, the table of implications is refined until all entries are assigned to $\nsim$ or $\sim$. The refined table defines the candidate equivalence classes and hence a possible minimal label transition system equivalent to $\mathcal{T}$. Since the equivalence definition does not take into account the invariant conditions $D(q)$, the equivalent states of the hybrid system are a subset of the equivalent states of the transition system. Refining the equivalence relation to take into consideration $D(q)$ is immediate.

V. The Water Tank Control Example

We consider a simple control problem consisting of controlling the water level in a cylindric tank equipped with an inlet pipe at the top and an outlet pipe at the bottom. The outlet flow is assumed to be proportional to the water level while the inlet flow is controlled by a valve whose aperture changes linearly in time in response to a position command. The control scheme is shown in figure 2. and include a water level sensor and a controller that on the basis of sensor readings actuates the valve.

Water tank. The dynamics of the water level in the tank can be described by the hybrid system $\mathcal{H}_t$ shown in figure 3 where the continuous state variable $x(t)$ represents the water

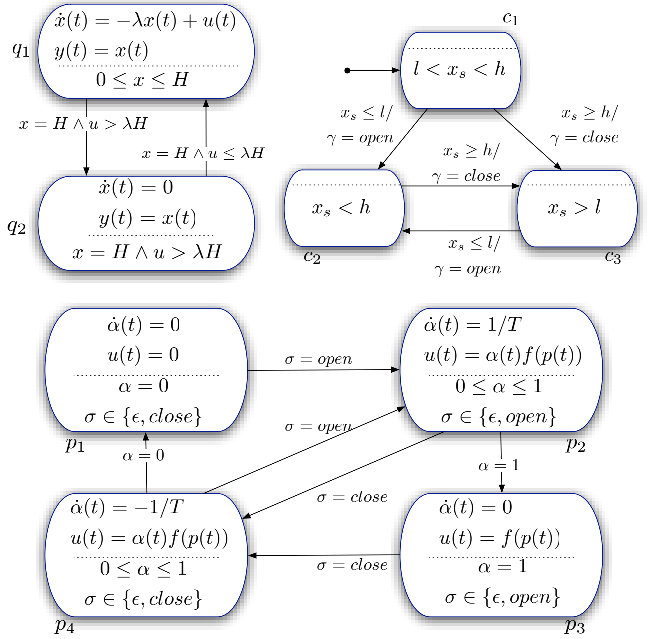

Fig. 3. Hybrid models of the tank (upper–left), controller (upper–right) and valve (bottom)

level in the tank and the continuous input variable $u(t)$ is equal to the inlet flow per tank section area. Location q_1 represents the situation in which there is no water overflow. The hybrid system remains in this location as long as the water level is lower than H. If the water level reaches the top of the tank and the inlet flow is greater than the outlet flow, then the system switches to location q_2 that describes the water overflow situation in which the water level remains constant and equal to H. The system remains in this location until the inlet flow is greater than the outlet flow, otherwise the system switches back to location q_1.

Valve. The inlet flow $u(t)$ to the tank depends on the supply inlet pressure $p(t)$ and it is controlled by a valve that may get a position command from a controller. It is assumed that the inlet flow is proportional to the valve aperture $\alpha(t)$, with $0 \leq \alpha \leq 1$, and that in response to a position command (*open* or *close*), the valve aperture changes linearly in time at rate $1/T$. Hence, $u(t) = \alpha(t) f(p(t))$ with $f(p(t)) > \lambda H$ for all possible values of $p(t)$. The hybrid model $\mathcal{H}_v$ describing the behavior of the valve is represented in figure 3. In location p_1 the valve is closed and the output $u(t)$ toward the container is constantly zero, independently from the value assumed by the inlet pressure $p(t)$. In locations p_2 and p_4 the valve is opening and closing, respectively. In these locations the output $u(t)$ depends on the inlet pressure $p(t)$ and the aperture of the valve $\alpha(t)$. Finally, in location p_3 the valve is open and the supply outlet flow $u(t)$ depends only on the inlet pressure $p(t)$.

Sensor. The sensor provides a measure $x_s(t)$ of the water level $x(t)$ in the tank with a random bounded error, that is

$$|x_s(t) - x(t)| \leq \delta \tag{2}$$

as long as $x \in [0, H]$.

Controller. The controller provides a position command *open* or *close* to the valve on the basis of the measured water level $x_s(t)$ and it is designed in order to regulate the water level in a given bounded interval thus preventing water overflow. The control law is based on a hysteresis loop: when the water level is decreasing, the controller provides the *open* command when $x_s(t) \leq l$ while, when the water level is increasing, the controller provides the *close* command when $x_s(t) \geq h$, with $\delta < l < h < H - \delta$. The controller behavior can be described by the hybrid system $\mathcal{H}_c$ shown in figure 3 where c_1 is the initial location.

VI. Closed loop composition

In this section we will show how to perform the composition of the hybrid models describing each component of the overall system in order to obtain the hybrid model of the closed loop system.

The hybrid model composition methodology is illustrated step by step, starting by the composition of the sensor $\mathcal{H}_s$, controller $\mathcal{H}_c$ and tank $\mathcal{H}_t$ hybrid models (see subsection VI-A), and then composing the resulting tank-sensor-controller $\mathcal{H}_{tsc}$ hybrid model with the valve $\mathcal{H}_v$ hybrid model (see subsection VI-B), obtaining the final hybrid model $\mathcal{H}_{tscv}$ of the overall system.

A. Tank-sensor and controller composition

As it has been showed in Section V, the sensor model is simply represented by the algebraic equation 2, but for the composition point of view, it can be modeled by a hybrid model $\mathcal{H}_s$ with an unique discrete location r_1 without transitions. The invariant condition is defined on the input variable $x(t)$ and is $x(t) \in [0, H]$, while the set X_s of the continuous time vector state is empty.

We now show how to perform each step of the composition methodology previously described.

Computation of the set Q of locations. The set Q_{tsc} of the hybrid model $\mathcal{H}_{tsc}$ of the composition of the tank, sensor and controller hybrid models is obtained computing the cartesian product of the sets $Q_t = \{q_1, q_2\}$, $Q_s = \{r_1\}$ and $Q_c = \{c_1, c_2, c_3\}$ of locations as follows:

$$Q_{tsc} = \{q_1, q_2\} \times \{r_1\} \times \{c_1, c_2, c_3\} = \{s_1, s_2, s_3, s_4, s_5, s_6\} =$$
$$= \{(q_1,r_1,c_1),(q_1,r_1,c_2),(q_1,r_1,c_3),(q_2,r_1,c_1),(q_2,r_1,c_2),(q_2,r_1,c_3)\}$$

Computation of the continuous–time dynamics. Since the sets X_c and X_s of the continuous state variables of the controller and the sensor are empty, while the hybrid model $\mathcal{H}_t$ is characterized by $X_t = \{x(t)\}$, then $X_{tsc} = X_s \cup X_c \cup X_t = \{x(t)\}$. As a consequence, the continuous time dynamics associated to the locations of the composed hybrid model $\mathcal{H}_{tsc}$ are due only to the tank hybrid model dynamics, that is:

$$\begin{array}{ll} (q_1, r_1, c_i): & \dot{x}(t) = -\lambda x(t) + u(t) \\ (q_2, r_1, c_i): & \dot{x}(t) = 0 \end{array} \text{, for } i = 1, 2, 3.$$

Definition of invariant conditions. To compute the invariant conditions of the composed hybrid model $\mathcal{H}_{tsc}$, we note that part of the invariant conditions of the hybrid models $\mathcal{H}_s$, $\mathcal{H}_c$ and $\mathcal{H}_t$ are defined on the variables $x(t)$ and $x_s(t)$, related by relation (2). As a consequence, the invariant conditions of the composed hybrid model $\mathcal{H}_{tsc}$ are obtained by the intersection of the invariant conditions on $x(t)$ of the hybrid models $\mathcal{H}_s$, $\mathcal{H}_c$ and $\mathcal{H}_t$, and by the union of the invariant conditions related to different variables:

$$(q_1,r_1,c_1):\begin{cases} x(t)\in[0,H] \\ x_s(t)\in(l,h) \\ x(t)\in[0,H] \end{cases} \Rightarrow x(t)\in(l-\delta,h+\delta)$$

$$(q_1,r_1,c_2):\begin{cases} x(t)\in[0,H] \\ x_s(t)\in(-\infty,h) \\ x(t)\in[0,H] \end{cases} \Rightarrow x(t)\in[0,h+\delta)$$

$$(q_1,r_1,c_3):\begin{cases} x(t)\in[0,H] \\ x_s(t)\in(l,\infty) \\ x(t)\in[0,H] \end{cases} \Rightarrow x(t)\in(l-\delta,H]$$

$$(q_2,r_1,c_1):\begin{cases} x(t)=H \\ u(t)>\lambda H \\ x_s(t)\in(l,h) \\ x(t)\in[0,H] \end{cases} \Rightarrow \begin{array}{l} x(t)\in\emptyset \\ u(t)>\lambda H \end{array}$$

$$(q_2,r_1,c_2):\begin{cases} x(t)=H \\ u(t)>\lambda H \\ x_s(t)\in(-\infty,h) \\ x(t)\in[0,H] \end{cases} \Rightarrow \begin{array}{l} x(t)\in\emptyset \\ u(t)>\lambda H \end{array}$$

$$(q_2,r_1,c_3):\begin{cases} x(t)=H \\ u(t)>\lambda H \\ x_s(t)\in(l,\infty) \\ x(t)\in[0,H] \end{cases} \Rightarrow \begin{array}{l} x(t)=H \\ u(t)>\lambda H \end{array}$$

Since locations (q_2,r_1,c_1) and (q_2,r_1,c_2) have an empty invariant set, they can be eliminated so that the composed hybrid model is characterized only by the following set Q_{tsc} of locations:

$$\begin{aligned} Q_{tsc} &= \{s_1,s_2,s_3,s_6\} = \{s_1',s_2',s_3',s_4'\} = \\ &= \{(q_1,r_1,c_1),(q_1,r_1,c_2),(q_1,r_1,c_3),(q_2,r_1,c_3)\} \end{aligned}$$

Computation of the sets E and G of edges and guards. The edges between discrete locations can be computed by means of the adjacency matrices M^s, M^t and M^c associated to the hybrid systems $\mathcal{H}_s$, $\mathcal{H}_t$ and $\mathcal{H}_c$, respectively. Since

M^t	q_1	q_2
q_1	0	1
q_2	1	0

M^s	r_1
r_1	0

M^c	c_1	c_2	c_3
c_1	0	1	1
c_2	0	0	1
c_3	0	1	0

one has

M^{tsc}	s_1	s_2	s_3	s_4	s_5	s_6
s_1	0	1	1	1	1	1
s_2	0	0	1	0	1	1
s_3	0	1	0	0	1	1
s_4	1	1	1	0	1	1
s_5	0	1	1	0	0	1
s_6	0	1	1	0	1	0

where $M_{i,j}^{tsc}(h,k)=1$ means that there is a transition from location (q_i,r_1,c_h) to location (q_j,r_1,c_k), with $i,j=1,2$ and $h,k=1,2,3$. To eliminate locations (q_2,r_1,c_1) and (q_2,r_1,c_2) characterized by empty invariant sets, we have to set the following elements of the adjacency matrix to 0:

$$\begin{array}{ll} M_{2,j}^{tsc}(h,k)=0 & \text{for } j,h=1,2 \quad k=1,2,3 \\ M_{i,2}^{tsc}(h,k)=0 & \text{for } i,k=1,2 \quad h=1,2,3 \end{array}$$

To compute the guard conditions associated to the edges we refer to the adjacency matrix M^{tsc}. The guard-condition composition is an important step that may lead to the reduction of the number of edges of the automaton associated to the hybrid system. Considering the sensor, controller and tank composition we have that the intersection of the guards

$$\begin{cases} G_1(q_2,q_1): x=H\wedge u\le\lambda H \\ G_2(c_3,c_2): x\le l+\delta \end{cases}$$

is empty so that we can set $M_{2,1}^{tsc}(3,2)=0$.

The final adjacency matrix representing the minimal sets of locations and edges and the associated output events are the following

M^{tsc}	s_1'	s_2'	s_3'	s_4'
s_1'	0	1	1	1
s_2'	0	0	1	1
s_3'	0	1	0	1
s_4'	0	0	1	0

γ	s_1'	s_2'	s_3'	s_4'
s_1'	0	*open*	*close*	*close*
s_2'	0	0	*close*	*close*
s_3'	0	*open*	0	ϵ
s_4'	0	0	ϵ	0

B. Tank-sensor-controller and valve composition

We illustrate how to compose the hybrid model H_{tsc} of the tank-sensor and controller obtained above with the hybrid model of the valve H_v.

Computation of the set Q of locations. The set Q_{tscv} of the hybrid model H_{tscv} of the closed-loop composition is obtained by computing the Cartesian product of the sets $Q_v=\{p_1,p_2,p_3,p_4\}$ and $Q_{tsc}=\{s_1',s_2',s_3',s_4'\}$. This set consists of 16 elements:

$$\begin{aligned} &Q_{tscv}=\{\ell_1,\ell_2,\dots,\ell_{16}\}= \\ &=\{(p_1,s_1'),\dots,(p_1,s_4'),\quad\cdots\quad,(p_4,s_1'),\dots,(p_4,s_4')\} \end{aligned}$$

Computation of the continuous–time dynamics. The hybrid models H_v and H_{tsc} are characterized by the sets of continuous state variables $X_v=\{\alpha(t)\}$ and $X_{tsc}=\{x(t)\}$, respectively. As a consequence, the set X_{tscv} of the composed hybrid model is the union of the two sets: $X_{tscv}=X_{tsc}\cup X_v=\{x(t),\alpha(t)\}$.

The continuous time dynamics associated to the locations of the composed hybrid model H_{tscv} is the following:

$$\begin{aligned} (p_i,s_j'):&\begin{cases} \dot{x}(t)=-\lambda x(t)+\alpha(t)f(p(t)) \\ \dot{\alpha}(t)=0 \end{cases} \\ (p_2,s_j'):&\begin{cases} \dot{x}(t)=-\lambda x(t)+\alpha(t)f(p(t)) \\ \dot{\alpha}(t)=1/T \end{cases} \\ (p_4,s_j'):&\begin{cases} \dot{x}(t)=-\lambda x(t)+\alpha(t)f(p(t)) \\ \dot{\alpha}(t)=-1/T \end{cases} \\ (p_i,s_4'):&\begin{cases} \dot{x}(t)=0 \\ \dot{\alpha}(t)=0 \end{cases} \\ (p_2,s_4'):&\begin{cases} \dot{x}(t)=0 \\ \dot{\alpha}(t)=1/T \end{cases} \\ (p_4,s_4'):&\begin{cases} \dot{x}(t)=0 \\ \dot{\alpha}(t)=-1/T \end{cases} \end{aligned}$$

for $i=1,3$ and $j=1,2,3$.

Definition of invariant conditions. To compute the invariant conditions of the composed hybrid model $\mathcal{H}_{tscv}$, note that part of the invariant conditions of the hybrid models $\mathcal{H}_{tsc}$, and $\mathcal{H}_v$ are defined on the variables $\alpha(t)$ and $u(t)$, related by the algebraic equation $u(t)=\alpha(t)f(p(t))$. As a consequence, the invariant conditions of the composed hybrid model $\mathcal{H}_{tscv}$ are obtained by the intersection of the invariant conditions on $\alpha(t)$ of the hybrid models $\mathcal{H}_{tscv}$ and $\mathcal{H}_v$, and by the union of the invariant conditions related to different variables. In doing this, the invariant conditions of location $\ell_4 = (p_1, s'_4)$ results in an empty set; in fact,

$$(p_1, s'_4) : \begin{cases} \alpha(t) = 0 \\ x(t) = H \\ u(t) > \lambda H \end{cases} \Rightarrow \begin{array}{l} x(t) = H \\ \alpha(t) \in \emptyset \end{array}$$

Hence, location ℓ_4 can be eliminated.

Computation of the sets E and G of edges guards. The edges of the automaton associated to the hybrid model of the composition can be computed by means of the adjacency matrices M^{tsc} and M^v associated to the hybrid systems $\mathcal{H}_{tsc}$ and $\mathcal{H}_v$, respectively, where

M^v	p_1	p_2	p_3	p_4
p_1	0	1	0	0
p_2	0	0	1	1
p_3	0	0	0	1
p_4	1	1	0	0

and $M^{tscv}_{i,j}(h,k) = 1$ indicates that there is a transition from location (p_i, s'_h) to location (p_j, s'_k). To eliminate location $((p_1, s'_4))$ characterized by an empty invariant set, we have to set

$$\begin{array}{ll} M^{tscv}_{1,j}(4,k) = 0 & \text{for } j,k = 1,\ldots,4 \\ M^{tscv}_{i,1}(h,4) = 0 & \text{for } i,h = 1,\ldots,4 \end{array}$$

Moreover, several edges can be eliminated when the guard-condition composition is computed. In more details, edges

$$\begin{array}{ll} M^{tscv}_{i,2}(j,k) & \text{for } i = 1,4 \quad j = 1,\ldots,4 \quad k = 3,4 \\ M^{tscv}_{i,2}(j,j) & \text{for } i = 1,4 \quad j = 1,2 \end{array}$$

has to be eliminated since they corresponds to a transition for the hybrid system $\mathcal{H}_v$ forced by an *open* command and a transition for the hybrid system $\mathcal{H}_{tsc}$ not delivering such a command. The same arguments hold when considering the *close* command so that transitions associated to

$$\begin{array}{ll} M^{tscv}_{i,4}(j,j) & \text{for } i = 2,3 \quad j = 1,\ldots,4 \\ M^{tscv}_{i,4}(j,2) & \text{for } i = 2,3 \quad j = 1,3 \\ M^{tscv}_{i,4}(3,4) & \text{for } i = 2,3 \\ M^{tscv}_{i,4}(4,3) & \text{for } i = 2,3 \end{array}$$

will never take place. Further, also transitions associated to the edges

$$\begin{array}{ll} M^{tscv}_{i,i}(j,2) & \text{for } i = 1,4 \quad j = 1,3 \\ M^{tscv}_{4,1}(j,2) & \text{for } j = 1,3 \\ M^{tscv}_{2,i}(k,h) & \text{for } i = 2,3 \quad h = 1,2 \quad k = 3,4 \\ M^{tscv}_{3,3}(k,h) & \text{for } k = 1,2 \quad k = 3,4 \end{array}$$

have to be eliminated. In fact, they correspond to a transition for the hybrid system $\mathcal{H}_v$ delivering an *open/close* command and a transition for the hybrid system $\mathcal{H}_{tsc}$ different from that forced by the delivered command.

Finally, some transitions are redundant and can be eliminated. In more details,

- transitions from location $\ell_5 = (p_2, s'_1)$ to location $\ell_{10} = (p_3, s'_2)$ is equivalent to the sequence of transitions with halfway location $\ell_9 = (p_3, s'_1)$;
- transitions from location $\ell_{13} = (p_4, s'_1)$ to location $\ell_3 = (p_1, s'_3)$ is equivalent to the sequence of transitions with halfway location $\ell_1 = (p_1, s'_1)$;
- transitions from location $\ell_{16} = (p_4, s'_4)$ to location $\ell_3 = (p_1, s'_3)$ is equivalent to the sequence of transitions with halfway location $\ell_{15} = (p_4, s'_3)$.

As a consequence we can set in the adjacency matrix

$$M^{tscv}_{2,3}(1,2) = M^{tscv}_{4,1}(1,3) = M^{tscv}_{4,1}(4,3) = 0$$

VII. Reducing the composition

A. Reduction by reachability analysis.

In order to compute the reachable locations for the hybrid system $\mathcal{H}_{tscv}$, consider the digraph (Q, E) associated to the adjacency matrix M^{tscv} and note that the initial locations of the hybrid system are ℓ_1, ℓ_5, ℓ_9 and ℓ_{13}. Since

$$r_{1,j} \vee r_{5,j} \vee r_{9,j} \vee r_{13,j} = [\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ ]$$

where $r_{i,j}$ is the i,j element of the reachability matrix

$$R = H(I + M_{tscv} + M^2_{tscv} + \ldots + M^{15}_{tscv})$$

and H is the Heaviside function, then locations ℓ_2, ℓ_4, ℓ_7, ℓ_8, ℓ_{11}, ℓ_{12}, and ℓ_{14} are not reachable from the initial locations. As a consequence, these locations can be eliminated and the composed hybrid model $\mathcal{H}_{tscv}$ is characterized only by the following set Q_{tscv} of locations:

$$Q_{tscv} = \{\ell_1, \ell_3, \ell_5, \ell_6, \ell_9, \ell_{10}, \ell_{13}, \ell_{15}, \ell_{16}\}$$

When considering only the previous set Q_{tscv}, the adjacency matrix M_{tscv} reduces to

M^{tscv}	ℓ_1	ℓ_3	ℓ_5	ℓ_6	ℓ_9	ℓ_{10}	ℓ_{13}	ℓ_{15}	ℓ_{16}
ℓ_1	0	1	0	1	0	0	0	0	0
ℓ_3	0	0	0	1	0	0	0	0	0
ℓ_5	0	0	0	1	1	0	0	1	1
ℓ_6	0	0	0	0	0	1	0	1	1
ℓ_9	0	0	0	0	0	1	0	1	1
ℓ_{10}	0	0	0	0	0	0	0	1	1
ℓ_{13}	1	0	0	1	0	0	0	1	1
ℓ_{15}	0	1	0	1	0	0	0	0	1
ℓ_{16}	0	0	0	0	0	0	0	1	0

B. Reduction using equivalence

The set Ω of discrete events is composed by the following elements: $\omega_1 = \{\alpha = 0\}$, $\omega_2 = \{\alpha = 1\}$, $\omega_3 = \{x \geq h - \delta\}$, $\omega_4 = \{x \leq l + \delta\}$, $\omega_5 = \{x = H \wedge u > \lambda H\}$, and $\omega_6 = \{x = H \wedge u \leq \lambda H\}$. To fill up the table of implication for the label transition system $\mathcal{T}_{sctv}$ it is useful to refer to the following *Table of Transitions*

	ω_1	ω_2	ω_3	ω_4	ω_5	ω_6
ℓ_1	ℓ_1	×	ℓ_3	ℓ_6	×	×
ℓ_3	ℓ_3	×	ℓ_3	ℓ_6	×	×
ℓ_5	ℓ_5	ℓ_9	ℓ_{15}	ℓ_6	ℓ_{16}	×
ℓ_6	ℓ_6	ℓ_{10}	ℓ_{15}	ℓ_6	ℓ_{16}	×
ℓ_9	×	ℓ_9	ℓ_{15}	ℓ_{10}	ℓ_{16}	×
ℓ_{10}	×	ℓ_{10}	ℓ_{15}	ℓ_{10}	ℓ_{16}	×
ℓ_{13}	ℓ_1	ℓ_{13}	ℓ_{15}	ℓ_6	ℓ_{16}	×
ℓ_{15}	ℓ_3	ℓ_{15}	ℓ_{15}	ℓ_6	ℓ_{16}	×
ℓ_{16}	ℓ_{16}	ℓ_{16}	ℓ_{16}	×	ℓ_{16}	ℓ_{15}

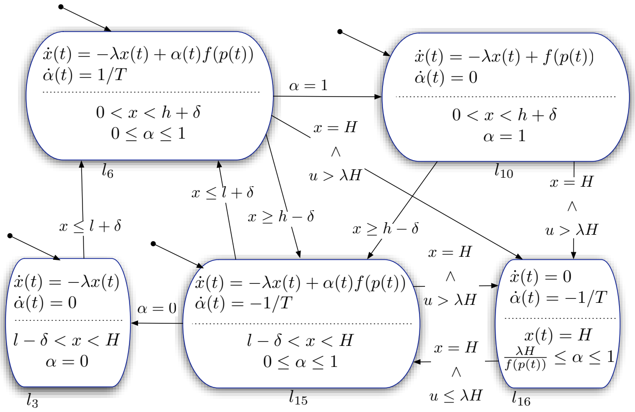

Fig. 4. Minimal hybrid system composition of the valve, tank controller and sensor

where each element contains, if any, the location reached from the location identifying the row of the table when the event identifying the column of the table takes place. Comparing the rows associated to locations with the same vector fields f, it is immediate to compute the following table of implications

ℓ_3	$\sim$							
ℓ_5	$\nsim$	$\nsim$						
ℓ_6	$\nsim$	$\nsim$	(ℓ_9, ℓ_{10})					
ℓ_9	$\nsim$	$\nsim$	$\nsim$	$\nsim$				
ℓ_{10}	$\nsim$	$\nsim$	$\nsim$	$\nsim$	$\sim$			
ℓ_{13}	$\nsim$	$\nsim$	$\nsim$	$\nsim$	$\nsim$	$\nsim$		
ℓ_{15}	$\nsim$	$\nsim$	$\nsim$	$\nsim$	$\nsim$	$\nsim$	(ℓ_1, ℓ_3)	
ℓ_{16}	$\nsim$	$\nsim$	$\nsim$	$\nsim$	$\nsim$	$\nsim$	$\nsim$	$\nsim$
	ℓ_1	ℓ_3	ℓ_5	ℓ_6	ℓ_9	ℓ_{10}	ℓ_{13}	ℓ_{15}

from which we conclude that, when considering the transition system $\mathcal{T}_{sctv}$, we have $\ell_3 \sim \ell_1$, $\ell_{10} \sim \ell_9$, $\ell_6 \sim \ell_5$ and $\ell_{15} \sim \ell_{13}$.

Invariant condition verification

We verify now whether the candidate pairs of locations identified with the *Table of Implication* are effectively equivalent. The invariant conditions associated to the candidate pair of locations ℓ_1 and ℓ_3 are the following:

$$D(\ell_1) = \begin{cases} x(t) \in (l - \delta, h + \delta) \\ \alpha(t) = 0 \end{cases} \quad D(\ell_3) = \begin{cases} x(t) \in (l - \delta, H) \\ \alpha(t) = 0 \end{cases}$$

We verify that $D(\ell_1) \subset D(\ell_3)$ and that, when in ℓ_1, if $x(t) \in \overline{D(\ell_3) \bigcap D(\ell_1)}$, a transition from ℓ_1 to ℓ_3 takes place, hence the equivalence of locations ℓ_1 and ℓ_3.

A similar analysis can be done for the pairs of locations $\ell_{13} - \ell_{15}$, $\ell_5 - \ell_6$ and $\ell_9 - \ell_{10}$ thus proving equivalence of all the pairs. As a consequence, the number of locations of the composed hybrid system can be reduced obtaining the hybrid system shown in figure 4.

VIII. Conclusion

In this paper we addressed the problem of verifying a hybrid system given as composition of subsystems. Existing formal verification tools require the construction of the composed system by hand. This requirement can be a serious impediment for the utilization of formal methods as the construction of the model of the overall system is cumbersome and error prone. In this paper, we introduced a procedure to compute a hybrid model given its components. Even if this manual computation can be replaced by an automatic procedure, we still have the problem of complexity explosion. Formal tools for hybrid systems rarely succeed with state space dimensions that are considered routine by users and discrete formal verification tools. For this reason, we presented techniques to compact automatically the representation of the overall system including the computation of an equivalent minimal realization.

The methodology for composing hybrid subsystems and compacting the resulting model was applied to a case study: a water tank system in which the measured liquid level is regulated by a valve by means of a hybrid controller. Applying the reduction technique here proposed, the number of locations is reduced from 16 in the original composed hybrid system to 5 in the reduced one.

The code for the computation of the composed reduced hybrid model can be inserted as a front-end into any formal verification tools for hybrid systems. We plan to verify the effectiveness of the method by adding it to Ariadne [10], a hybrid system formal verification tool based on reachability analysis. We also plan to extend the algorithms used to reduce the composition to include the techniques presented in [11] that leverage the literature on continuous time system order reduction.

References

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

[2] L. Benvenuti, A. Ferrari, E. Mazzi, and A. Sangiovanni Vincentelli. Contract-based design for computation and verification of a closed-loop hybrid system. In *11th International Workshop HSCC 2008*, volume 4981 of *LNCS*, pages 58–71. Springer Berlin / Heidelberg, 2008.

[3] R. Alur and T.A. Henzinger. Modularity for timed and hybrid systems. In *9th International Conference on Concurrency Theory*, pages 74–88. Springer-Verlag, 1997.

[4] S. Bornot and J. Sifakis. On the composition of hybrid systems. In *1st International Workshop HSCC 1998*, volume 1386 of *LNCS*, pages 49–63, London, UK, 1998. Springer-Verlag.

[5] Nancy Lynch. Hybrid i/o automata revisited. In *Hybrid Systems: Computation and Control, 4th International Workshop, HSCC 2001*, volume 2034 of *LNCS*, pages 403–417. Springer-Verlag, 2001.

[6] A. Balluchi, E. Mazzi, and A. Sangiovanni Vincentelli. Complexity reduction for the design of interacting controllers. In *10th International Workshop HSCC 2007*, volume 4416 of *LNCS*. Springer Verlag, 2007.

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

[8] Antoine Girard and George J. Pappas. Approximate bisimulations for constrained linear systems. *Automatica*, 43(8):1307–1317, 2007.

[9] G. De Micheli. *Synthesis and Optimization of Digital Circuits*. McGraw-Hill, 2001.

[10] L. Benvenuti, D. Bresolin, A. Casagrande, P. Collins, A. Ferrari, E. Mazzi, A. Sangiovanni-Vincentelli, and T. Villa. Reachability computation for hybrid systems with ariadne. In *17th IFAC World Congress*, Seoul, South Korea, 2008.

[11] A. Balluchi, A. Bicchi, E. Mazzi, and A. Sangiovanni Vincentelli. Hybrid model complexity reduction. In *47th IEEE Conference on Decision and Control*, Dec 2008.