HYBRID ABSTRACTIONS OF
AFFINE SYSTEMS

Marie-Anne Lefebvre
Hervé Guéguen

Supélec - IETR
BP 81127 Cesson-Sévigné Cedex, France

Abstract: This paper considers the problem of building a set of hybrid abstractions for affine systems in order to compute over approximations of the reachable space. Each abstraction is based on a partition of the continuous state space that is defined by hyperplanes generated by linear combinations of two vectors. The choice of these vectors is based on considerations on the dynamics of the system and uses, for example, the left eigen vectors of the matrix that defines this dynamics. It is shown how the reachability calculus can then be performed on a composition of such abstractions and how its accuracy depends on the choice of hyperplanes that defines the abstraction but also on the number of abstractions that are composed. *Copyright © 2005 IFAC*

Keywords: Hybrid systems, reachability, abstractions

1. INTRODUCTION

Recent advances in control and the increasing needs for integration and validation of control applications have led to the development of research in automated verification for continuous and hybrid systems. Most of the approaches are based on a reachability calculus that includes the representation of regions in the continuous state space and computation of the reachable continous state space (Guéguen and Zaytoon, 2004). However this is a rather complex task when the continuous dynamics is non-trivial and the solutions that have been proposed are mostly based on the fact that for a relevant class of properties, it may be sufficient to compute an over-approximation of the reachable space in order to conclude.

This can be done by abstracting the concrete initial model and compute the reachable space of the abstraction that is an over-approximation of the one of the concrete system. Some of these abstracting methods aim at extracting a finite state-model of the continuous dynamics (Chutinan and Krogh, 2001) in order to use classical model checking tools. Other approaches, called "hybridization-based" methods in (Asarin and Dang, 2004), aim at extracting a hybrid automaton with simpler dynamics from the continuous systems (Henzinger, *et al.*, 1998). The goal is then to get a linear hybrid automaton with differential inclusions as abstract model in order to be able to compute reachability for example with a tool such as Hytech (Henzinger, *et al.*, 1995).

In these "hybridization-based" methods, in order to abstract the continuous dynamics, the continuous state space is partitioned by linear constraints and a location is associated in the abstract model to each element of the partition. A polyhedron that includes the vector field for all points of this element is then computed and associated to the relative location as its continuous dynamics. Finally a transition from a location to an other one is introduced if their relative region in the concrete system have a common frontier and there exist at least one continuous trajectory that crosses this frontier from the first region to the second.

Of course the abstraction introduces some spurious trajectories and the reachable space of the abstract model is an over-approximation of the one of the concrete system. The problem with these approaches is then to find a trade-off between the accuracy of the abstraction and its simplicity i.e. mostly the number of locations that are introduced. (Lefebvre, *et al.*, 2002) proposed a method to guide the partition of the state space to abstract affine planar regular systems. This method uses some properties of the continuous dynamics in order to get an abstraction that is quite simple to analyze but does not introduce too much spurious trajectories.

This paper proposes a generalization of this approach to higher dimension systems that may also be singular. In section 2 the approach for planar systems is shortly presented in order to illustrate the basic ideas of the

approach. The properties of affine systems that are used to guide the abstraction are then presented in section 3. The resulting abstraction and the way the reachabilty calculus is performed are detailed in section 4. Finally section 5 considers the question of accuracy of the abstraction and gives some considerations that are illustrated by an example specified in section 6.

2. PLANAR REGULAR SYSTEMS

In this section the system under study is a planar affine system that is regular and the equilibrium point is denoted $\mathbf{x}_e$ (equation 1).

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{b}$$
$$\mathbf{x}_e = -\mathbf{A}^{-1}\mathbf{b} \tag{1}$$

It is then possible to show (see (Lefebvre, *et al.*, 2002) for details) that for all points of a given line that starts at the equilibrium point, the derivative vectors are collinear. So for all points of a sector defined by two such lines the vector field is in the sector defined by the two derivative vectors on the boundary as illustrated fig. 1. For a line defined by the first equation of (2) it is then possible to characterize the vector field by the second equation of (2).

$$\mathbf{q}^T(\mathbf{x} - \mathbf{x}_e) = 0$$
$$\mathbf{u}^T\dot{\mathbf{x}} = 0 \; with \; \mathbf{u} = (\mathbf{A}^T)^{-1}\mathbf{q} \tag{2}$$

Moreover if the border of such a sector is defined by a real left eigen vector of matrix $\mathbf{A}$ it can't be crossed by continuous trajectory. Otherwise it is always crossed in the same direction.

It is then possible to extract from a partition of the state space with such sectors, an abstraction such as each location is the source and the target of at most one transition (as illustrated fig 2. for a system with complex eigen values) and its continuous dynamics is given by the inclusion (3) where the two vectors $\mathbf{u}_1$ and $\mathbf{u}_2$ are given by (2).

$$\left(\mathbf{u}_1^T\dot{\mathbf{x}} \leq 0\right) \wedge \left(\mathbf{u}_2^T\dot{\mathbf{x}} \geq 0\right) \tag{3}$$
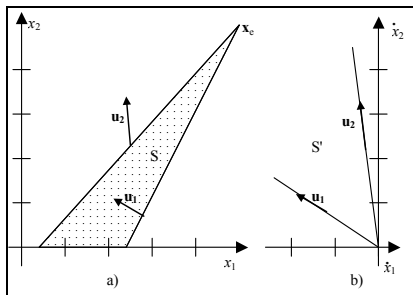

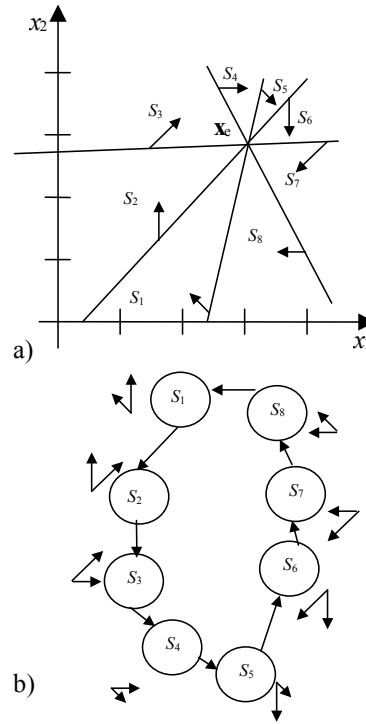Fig. 1 Sectors and differential inclusions for planar systems

Fig 2. The partition of the state space (a) and the associated automaton (b)

It may be noticed that (3) imposes constraints only on the direction and not on the norm of the vector field but as the abstraction is used to calculate the reachable space this is not a problem and even more it makes this calculus very easy.

3. GENERAL SYSTEMS

In order to abstract an affine continuous system by a hybrid linear automaton it is necessary to partition the state space and to associate to each region a differential inclusion. The study of planar regular systems has shown that some lines have particular properties to define this partition. The aim is then to generalize this to general affine dynamics specified by equation (4) and find hyperplanes to partition the state space such as the abstract hybrid systems have some 'good' properties for the reachability calculus. When defining the hyperplanes the objective are twofold:

– for all points of a plane the vector field must be normal to the same vector,

– whenever possible the continuous trajectories must cross the border of a region in the same direction.

The first point will ensure that the differential inclusion can be easily computed and the second one that each border will be associated with at most one transition.

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{b} \tag{4}$$

3.1 First criterion

The first criterion that a hyperplane defined by equation (5) has to fulfill can be formalized by the equation (6).

$$P = \left\{ \mathbf{x} / \mathbf{q}^{\mathbf{T}}\mathbf{x} = k \right\} \qquad (5)$$

$$\exists \boldsymbol{\gamma} \quad s.a \ \forall \mathbf{x} \in P, \ \boldsymbol{\gamma}^{T}\dot{\mathbf{x}} = 0 \qquad (6)$$

Property 1: the conditions that must hold on $\mathbf{q}$, $\boldsymbol{\gamma}$ and k in order that equation (6) is verified are given by equations (7).

$$\mathbf{q} = \mathbf{A}^{T}\boldsymbol{\gamma}$$
$$k = -\boldsymbol{\gamma}^{T}\mathbf{b} \qquad (7)$$

This can be proven by considering that if $\mathbf{x}_1 \in P$ *and* $\mathbf{x}_2 \in P$ then $\mathbf{q}^{T}(\mathbf{x}_1 - \mathbf{x}_2) = 0$

and if $\boldsymbol{\gamma}$ is such as $\boldsymbol{\gamma}^{T}\dot{\mathbf{x}}_1 = 0$, then:

$$\begin{aligned}
\boldsymbol{\gamma}^{T}\dot{\mathbf{x}}_2 &= \boldsymbol{\gamma}^{T}\left(\mathbf{A}\mathbf{x}_2 + \mathbf{b}\right) \\
&= \boldsymbol{\gamma}^{T}\left(\mathbf{A}\mathbf{x}_1 + \mathbf{b} + \mathbf{A}\left(\mathbf{x}_1 - \mathbf{x}_2\right)\right) \\
&= \boldsymbol{\gamma}^{T}\mathbf{A}\left(\mathbf{x}_1 - \mathbf{x}_2\right)
\end{aligned}$$

so if $\boldsymbol{\gamma}^{T}\dot{\mathbf{x}}_2 = 0$, $\mathbf{q}$ and $\mathbf{A}^{T}\boldsymbol{\gamma}$ are collinear and as the direction of these vectors is the only important point, the first part of equation of (7) holds without loss of generality, and then:

$$\begin{aligned}
\boldsymbol{\gamma}^{T}\dot{\mathbf{x}}_1 &= \boldsymbol{\gamma}^{T}\left(\mathbf{A}\mathbf{x}_1 + \mathbf{b}\right) \\
&= \mathbf{q}^{T}\mathbf{x}_1 + \boldsymbol{\gamma}^{T}\mathbf{b} \\
&= k + \boldsymbol{\gamma}^{T}\mathbf{b}
\end{aligned}$$

this proves the second part of (7).

3.2 Differential inclusion and reachable space

Property 2: For all points of a region defined by (8) where the borders are hyperplanes such as (7) holds the inequalities on the vector field (9) are true.

$$\mathbf{q_1^T}\mathbf{x} \geq k_1$$
$$\mathbf{q_2^T}\mathbf{x} \leq k_2 \qquad (8)$$

$$\boldsymbol{\gamma_1^T}\dot{\mathbf{x}} \geq 0$$
$$\boldsymbol{\gamma_2^T}\dot{\mathbf{x}} \leq 0 \qquad (9)$$

Property 2 is directly proven by:

$$\begin{aligned}
\boldsymbol{\gamma}_1^{T}\dot{\mathbf{x}} &= \boldsymbol{\gamma}_1^{T}\left(\mathbf{A}\mathbf{x} + \mathbf{b}\right) \\
&= \mathbf{q}_1^{T}\mathbf{x} - k_1 \\
&\geq 0
\end{aligned}$$

An over-approximation of the reachable space from a point $\mathbf{x}_1$ of the region defined by (8), within this region, is then given by the conjunction of (8) and

$$\boldsymbol{\gamma_1^T}\left(\mathbf{x} - \mathbf{x_1}\right) \geq 0$$
$$\boldsymbol{\gamma_2^T}\left(\mathbf{x} - \mathbf{x_1}\right) \leq 0 \qquad (10)$$

3.3 Second criterion

The second criterion that is used to choose the hyperplanes that define the partition is the direction in which continuous trajectories cross an hyperplane defined by (5). From a general point of view this direction changes according to an other hyperplane (Pettit, 1995) defined by:

$$\mathbf{q}^{T}\left(\mathbf{A}\mathbf{x} + \mathbf{b}\right) = 0$$

Generally, nothing can be said on this hyperplane but some special cases are worthwhile to be considered.

The first one is the case when the hyperplanes are defined by a left eigen vector $\mathbf{w}$ of $\mathbf{A}$ associated with a real eigen value. (7) then gives:

$$\boldsymbol{\gamma} = \frac{1}{\lambda}\mathbf{w} + \sum \alpha_i \mathbf{w}_{0i}$$
$$k = -\frac{1}{\lambda}\mathbf{w}^{T}\mathbf{b} - \sum \alpha_i \mathbf{w}_{0i}{}^{T}\mathbf{b} \qquad (11)$$

where the $\mathbf{w}_{0i}$ are the left eigen vectors potentially associated with a null eigen value. If all the $\mathbf{w}_{0i}{}^{T}\mathbf{b}$ are null, for example if $\mathbf{A}$ is regular, $\mathbf{w}$ defines only one useful hyperplane according to criterion 1 and it is such as:

$$\begin{aligned}
\mathbf{w}^{T}\dot{\mathbf{x}} &= \mathbf{w}^{T}\left(\mathbf{A}\mathbf{x} + \mathbf{b}\right) \\
&= \lambda\mathbf{w}^{T}\mathbf{x} + \mathbf{w}^{T}\mathbf{b} \\
&= \lambda\left(\mathbf{w}^{T}\mathbf{x} + \frac{1}{\lambda}\mathbf{w}^{T}\mathbf{b}\right) \\
&= 0
\end{aligned}$$

This hyperplane is then a separating one that can't be crossed by the continuous trajectories. If in (11) one $\mathbf{w}_{0i}{}^{T}\mathbf{b}$ is not null then k is free and $\mathbf{w}$ defines a family of hyperplanes. Each of these hyperplanes is always crossed in the same direction as $\mathbf{w}^{T}\dot{\mathbf{x}} = \lambda k + \mathbf{w}^{T}\mathbf{b}$ is constant.

The hyperplane associated with $\mathbf{q} = \alpha_1\mathbf{w}_1 + \alpha_2\mathbf{w}_2$ where $\mathbf{w}_1$ and $\mathbf{w}_2$ are left eigen vectors of $\mathbf{A}$ associated with real eigen values is also an interesting case. Equation (7) then gives:

$$\boldsymbol{\gamma} = \frac{\alpha_1}{\lambda_1}\mathbf{w}_1 + \frac{\alpha_2}{\lambda_2}\mathbf{w}_2 + \sum \alpha_{0i}\mathbf{w}_{0i}$$
$$k = -\frac{\alpha_1}{\lambda_1}\mathbf{w}_1{}^{T}\mathbf{b} - \frac{\alpha_2}{\lambda_2}\mathbf{w}_2{}^{T}\mathbf{b} - \sum \alpha_{0i}\mathbf{w}_{0i}{}^{T}\mathbf{b} \qquad (12)$$

If all the $\mathbf{w}_{0i}^T\mathbf{b}$ are null (12) defines only one hyperplane and then:

$$\mathbf{q}^T\dot{\mathbf{x}} = \alpha_1\lambda_1\mathbf{w}_1^T\mathbf{x} + \alpha_2\lambda_2\mathbf{w}_2^T\mathbf{x} + \alpha_1\mathbf{w}_1^T\mathbf{b} + \alpha_2\mathbf{w}_2^T\mathbf{b}$$

$$= \lambda_1\left(\alpha_1\mathbf{w}_1^T\mathbf{x} + \alpha_2\mathbf{w}_2^T\mathbf{x} + \frac{\alpha_1}{\lambda_1}\mathbf{w}_1^T\mathbf{b} + \frac{\alpha_2}{\lambda_2}\mathbf{w}_2^T\mathbf{b}\right)$$

$$-\alpha_2\lambda_1\mathbf{w}_2^T\mathbf{x} + \alpha_2\lambda_2\mathbf{w}_2^T\mathbf{x} - \alpha_2\frac{\lambda_1}{\lambda_2}\mathbf{w}_2^T\mathbf{b} + \alpha_2\mathbf{w}_2^T\mathbf{b}$$

$$= \alpha_2(\lambda_2 - \lambda_1)\left(\mathbf{w}_2^T\mathbf{x} + \frac{1}{\lambda_2}\mathbf{w}_2^T\mathbf{b}\right)$$

The sign of this expression only depends on the position of $\mathbf{x}$ with respect of the separating hyperplane defined by $\mathbf{w}_2$ and is constant if the partition of a half space defined by this hyperplane is considered. If one of the $\mathbf{w}_{0i}^T\mathbf{b}$ is not null, k is free and criterion 1 specifies a family of hyperplanes for each (α_1, α_2). However according to this second criterion the only member of this family that is interesting is defined by $\alpha_{0i}=0$. The previous result still holds and the plane is crossed in one direction on each side of the separating plane.

Due to place consideration it not possible to detail all the cases but this result is still valid if $\mathbf{q}$ is defined as a real combination of two conjugate complex left eigen vectors. When $\mathbf{q}$ is a combination of a real left eigen vector with a combination of complex eigen vectors the plane that defines the change of crossing direction only depends on the considered vectors and must be computed only once for all combinations(Lefebvre, 2004).

These results are consistent with the previous ones for regular planar systems as the hyperplanes that respect (7) are then the lines to which the equilibrium point belongs.

4. ABSTRACTION AND REACHABILITY

4.1 Basic idea

The basic idea of the proposed approach is that it is easier to consider a set of partitions that defines a set of abstractions than to build a global abstraction. Each partition is then defined by a set of hyperplanes for which equation (7) holds in order to use property 2 to determine the differential inclusion. This set of hyperplanes is defined either by a given vector $\mathbf{q}$ for which it is possible to choose different values of k in (5) or, considering that $(\mathbf{q}_1, \boldsymbol{\gamma}_1, k_1)$ and $(\mathbf{q}_2, \boldsymbol{\gamma}_2, k_2)$ define two hyperplanes that respect property 1, by the linear combinations of $\mathbf{q}_1$ and $\mathbf{q}_2$ as for all (α_1, α_2), $(\alpha_1\mathbf{q}_1+\alpha_2\mathbf{q}_2, \alpha_1\boldsymbol{\gamma}_1+\alpha_2\boldsymbol{\gamma}_2, \alpha_1k_1+\alpha_2k_2)$ defines a hyperplane that also respects this property.

Associated with the second criterion, this leads to build abstractions generated by:

- firstly, each real left eigen vector of matrix $\mathbf{A}$ that defines invariant subspaces and separating hyperplanes and the set of hyperplanes normal to this vector when this is possible,

- secondly, the linear combinations of two left real eigen vectors,

- thirdly, the real linear combination of two conjugate left eigen vectors,

- fourthly, the linear combination of one real left eigen vector and a real combination of two conjugate left eigen vectors,

- finally, the linear combination of two vectors that can be chosen among the principal vectors (i.e. vectors associated to left eigen vectors to define the Jordan form of the matrix) in order to be sure that they are not dependant of the previous one and that this abstraction will explore complementary dimensions of the state space.

4.2 Reachability calculus and Composition

Each point of the state space belongs to a region of each partition and its vector field is then defined by the conjunctions of all the constraints associated with these regions. The global abstract model is then the composition of all the elementary abstract models and the reachability calculus can then be performed on this global model. However it is not necessary to explicitly compute this global model to perform the reachability calculus as it can be done on the set of parallel elementary abstractions by considering local conjunctions of constraints. For a given region defined as the intersection of a set of regions (each associated with a partition) the reachable space from a point $\mathbf{x}_1$ within the given region is the conjunction of the sets of equations (8) and (10).

Moreover, as the reachability calculus from a polyhedral region is based on the calculus from its vertices, it is possible to perform the reachability calculus as soon as this previous intersection can be expressed by its vertices. If the subspace that is considered for the abstraction is bounded (for example by the invariant of the concrete location) it is then possible to compute the reachable space for only one elementary abstraction.

Considering a set of abstract models based on elementary partitions the reachable space for the composition can then be computed by locally composing, on the fly, the constraints of each abstraction or it can be estimated by computing the reachable space for each elementary abstraction and then their intersection.
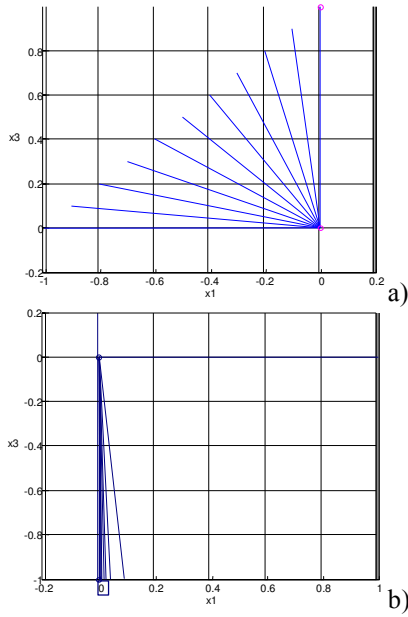
Fig. 3. Example partition of the state space (a) and corresponding vector fields.

5. ACCURACY

As stated in the introduction, the problem with these approaches of abstraction is to find a trade-off between the accuracy of the abstraction and its simplicity i.e. mostly the number of locations that are introduced. With respect with this approach, two factors are then relevant: the accuracy of each elementary abstraction and the number of abstractions that are composed for a calculus.

The accuracy of an abstraction generated by a couple of given vectors is clearly linked to the number of hyperplanes (and locations): if more hyperplanes are considered the regions are smaller and the differential inclusion are closer. However the position of the hyperplanes is also important. This point can be illustrated for the example of the next section, the various vectors that define a partition are given figure 3.a and the corresponding vectors that define the vector fields are given figure 3.b. As it can be seen, the regular disposition of the vectors in the state space corresponds to a very irregular disposition in the derivative space and the importance of all regions, with respect to the final result, is not the same.

If the precision of the abstraction is defined by the 'width' of the intersection of the reachable sub region from a point with the border of the region, this precision is intuitively linked, for a partition generated by combinations of 2 vectors (fig. 4), to the relative position of the normal vectors in the state space on the one hand and in the derivative space on the other hand The value of (13) can then be used to quantify the 'closeness' of two hyperplanes.
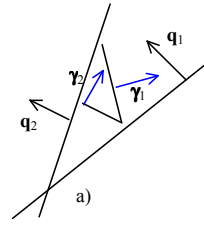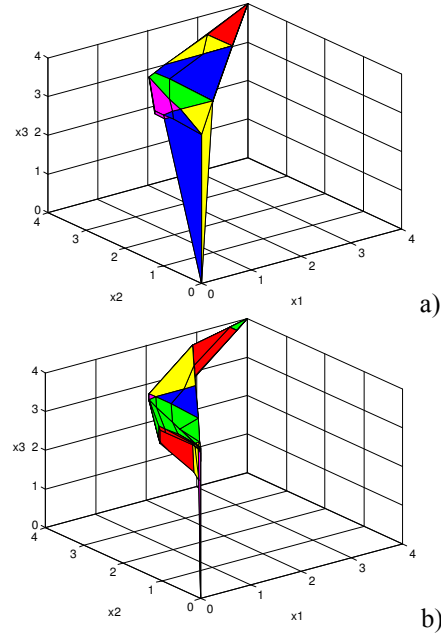

Fig 4. Accuracy of reachable space by abstraction

Fig. 5. Influence of the position of the partitioning hyperplanes.

The usefulness of this criterion can be illustrated by figure 5 where the results of the computation of the reachable space from 1 point, for the example of the next section, are given. Figure 5.a is based on a regular partition and figure 5.b is based on a partition with the same number of regions but based on the evolution of the criterion. It can be seen that for the same computation load for the reachability calculus, and a little more for the abstraction, the result is then better.

$$\frac{\mathbf{q}_1^T \mathbf{q}_2}{\|\mathbf{q}_1\| \|\mathbf{q}_2\|} \cdot \frac{\gamma_1^T \gamma_2}{\|\gamma_1\| \|\gamma_2\|} \tag{13}$$

The second factor that influence the accuracy of the reachability calculus is the number of abstractions that are composed because the more the abstractions are, the more the vector field for a given point is constrained. This can be illustrated by fig. 6 where the results of three reachability calculus are represented. The first one is based on one partition, for the second a new partition has been composed and for the third an other one has been added. It can be seen that the first result is relatively rough but can already lead to conclusion on the reachability of some regions, whereas the results are more precise when more abstractions are composed.
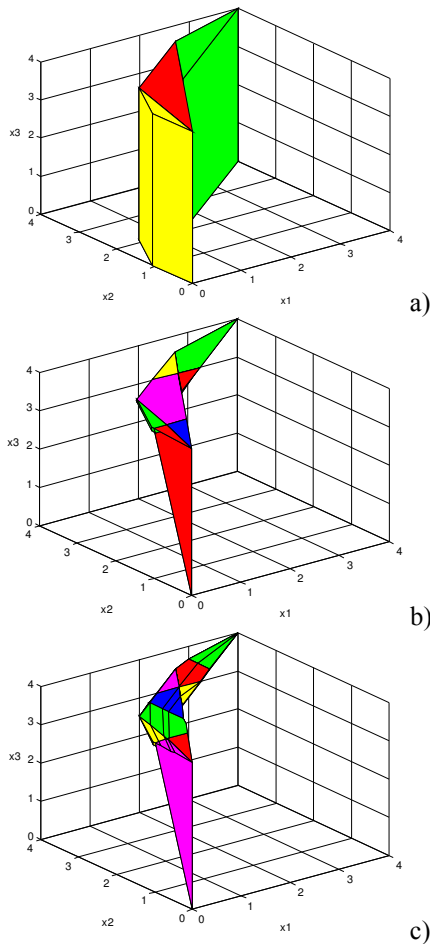
Fig 6. Reachabilty for 1 abstraction (a), 2 abstractions (b) and 3 abstractions (c)

Fig. 7. Reachabilty for 2 composed abstractions

perform reachability calculus. Each abstraction is based on a partition of the state space by hyperplanes such that they also define hyperplanes for the vector fields in order to compute the differential inclusion of the abstraction. The choice of the vectors that define these hyperplanes is based on crossing considerations and then favors left eigen vectors.

An important open problem that will be the object of further work is the choice of a strategy when the reachability calculus is inconclusive: the refinement of one abstraction or the composition with a new one and which one? For example according to region of interest it is not obvious that figure 6.c is really better than 6.b and figure 7 seems worse that figure 6.b whereas they are based on the same number of abstractions.

6. EXAMPLE

The affine system that is used to illustrate how this approach can be used to over-approximate the reachable space and how the various factors can influence the accuracy of the result is defined by equation (15). The abstractions are based on combinations of couple of left eigen vectors of **A** that are the basis vectors and for the case where only one abstraction is used it is considered that the region of interest is the cube [0,4]x[0,4]x[0,4].

$$\mathbf{A} = \begin{pmatrix} -10 & 0 & 0 \\ 0 & -5 & 0 \\ 0 & 0 & -0.1 \end{pmatrix} \quad \mathbf{b} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad (15)$$

The abstractions have been computed using specific Matlab macros and the reachability computations have been performed using a specific program based on the Polylib library (Wilde, 1993).

CONCLUSION

This paper has presented an approach to abstract affine continuous systems by a set hybrid automata in order to
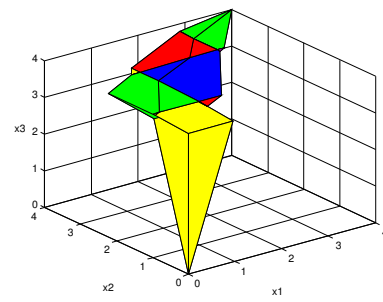
REFERENCES

Asarin, E. and T. Dang (2004). Abstraction by projection and application to multi affine systems. in HSCC04:Hybrid systems: computation and control (R. Alur and G. Pappas (Eds.))

Chutinan, A. and B. Krogh (2001). Verification of Infinite-State Dynamics Systems using approximate quotient transition systems. IEEE Trans on Automatic Control, 46, 1401-1410

Guéguen, H. and J. Zaytoon (2004). On the formal verification of hybrid systems. Control Engineering Practice, 12, 1253-1267

Henzinger, T., P. Ho and H. Wong-Toi (1995). a user guide to Hytech. in Tools and Algorithms for the Construction and Analysis of Systems

Henzinger, T., P. Ho and H. Wong-Toi (1998). Algorithmic analysis of non-linear hybrid systems. IEEE Trans on Automatic Control, 43, 540-554

Lefebvre, M.-A., H. Guéguen and J. Buisson (2002). Structured hybrid abstractions of continuous systems. in IFAC World Congress B02

Lefebvre, M.-A. (2004). Abstractions pour la vérification de sûreté des systèmes hybrides. IETR-Supelec, PhD thesis Univ Rennes 1

Pettit, N. (1995). Analysis of piecewise linear dynamical systems. UMIST Control System Center, Research Studio Press

Wilde, D. K. (1993). A library for doing polyhedral operations. IRISA, report N°785, Rennes (France)