Abstract: Abstracting a continuous dynamical system by a hybrid linear automaton allows to use formal verification techniques to check properties of hybrid systems. In order to build the abstract model, the state space is partitioned and the rate of each state variable is approximated. When the system is linear the properties of the continuous system can be used to split the state space in order to get a tighter abstraction with an automaton that remains simple, so that the reachability calculus is more accurate. Moreover the accuracy of the approximation can be used to aid the design of the partition. Copyright © 2002 IFAC

Keywords: hybrid systems, abstraction, model checking.

1. INTRODUCTION

Model checking aims at assuring that a system fulfil its requirements and especially its safety requirements. For hybrid systems, the system under consideration is modelled by a hybrid automaton (Alur et al., 1995) and the requirements are expressed by configurations of discrete locations and regions of the continuous state space that are forbidden. Checking is then performed by a reachability and emptiness analysis in order to establish that starting from an initial state the system can not reach a forbidden configuration (Guéguen and Zaytoon 2001). The calculation of the reachable state is not decidable for all hybrid automata (Henzinger et al., 1995a). However the reachable region can be computed by tools such as Hytech (Henzinger et al. 1995b) by iterative semidecision procedures for linear hybrid automata. If the system is not modelled by a linear automaton, a linear abstraction has to be computed (Henzinger et al., 1998) by partitioning the state space into linear regions and approximating the vector field defining the gradient of the trajectories by inclusion of this gradient in linear sets. As the reachable region of the abstraction includes the real system one, if the emptiness test is positive for the abstraction, the requirement is fulfilled by the system. The closer the approximation is, the more properties of the system can be verified using it, but the more discrete locations it needs and the more complex is the automaton.

The aim of this work is to study the linear abstraction of hybrid automata with planar affine continuous dynamics, that is dynamics modelled by equations such as \( \dot{x} = A(q)x + b(q) \) where \( x \) is a 2 dimensions vector and \( A(q) \) is non-singular. The aim is then to build a new linear hybrid automaton for each situation \( q \) of the first one, that is an abstraction of the affine continuous dynamic on the subspace defined by the invariant of the situation, and more precisely to use properties of these systems in order to get close approximations of the vector field with a simple automaton containing few locations and transitions.

This approach uses properties of affine systems such as the convexity of the vector field, which are also used in other approaches where the reachability of affine systems is concerned, as for exemple the problem of control of an affine system toward a particular set of the space (Habbets and van Schuppen 2000), but it is rather different as reachability will finally be calculated on a linear hybrid automaton and the problem is to find the regions that define this automaton.

In the sequel, hybrid automata and general principles of linear abstractions are reminded. Then the splitting method is presented and considerations on accuracy of the subsequent approximation are given. Finally an example illustrates the contribution of the method.
with regard to the abstract automaton and the accuracy of a reachability computation carried out with Hytech.

2. HYBRID AUTOMATA AND LINEAR ABSTRACTIONS

Hybrid automata have been introduced (Alur et al., 1995) in order to model the behavior of hybrid systems. The state of a hybrid automaton is given by a discrete location and the values for all continuous state variables. This state can change in two ways. Firstly by a discrete and instantaneous transition that changes the location and the values of the state variable according to the jump function associated with the transition. Secondly by a continuous transition that changes the values of the state variables according to the activities of the location. The automaton can remain in the same discrete location as long as the continuous state stays in the invariant of this location. A transition is enabled when the continuous state is in the guard of the transition.

Linear hybrid automata are a subclass of hybrid automata for which the reachability problem can be computed. This subclass is specified by the following constraints (Henzinger et al. 1995b):
- the guards and invariants must be expressed as sets of linear inequalities over state variables with rational coefficients;
- the jump functions assign to a sub-vector of the state vector a value after the jump that belongs to a region defined by linear inequalities over the values of the state vector before the jump;
- the activity of each location is specified by a rate condition that is a set of linear inequalities with rational coefficients over the first derivative of the state vector that restricts the rates of change of the state variables.

When continuous activities do not meet this last condition, Henzinger et al (1998) advocate to use linear phase-portrait approximation in order to get an abstraction of the hybrid automaton that can be analyzed. This abstraction is built by partitioning the invariant of each location into linear regions. Each of these regions is associated with a new location which invariant is the region. The rate condition of a new location is such that for each point of the region the rate defined by the vector field meets the condition. A transition from one location to an other one is introduced when the vector field defines a continuous transition from a point of the first region to a point of the second one.

If the approximation is too coarse Henzinger et al (1998) suggest to use smaller linear regions in order to get a more accurate one. However the size of the regions is not the only criterion that acts on accuracy of the approximation. The freedom of choice in selecting the hyperplanes defining the linear regions can also be exploited in order to get regions that are consistent with the continuous dynamic and so define better abstractions (Lefebvre, Guéguen and Buisson, 2001).

Fig. 1. Crossing of separating lines by the abstraction.

3. USE OF THE DYNAMIC PROPERTIES FOR THE PARTITION

Runs of the hybrid system that are introduced by the abstractions are due to the approximation of the vector field by linear rate conditions but also to discrete transitions that are introduced. For example, figure 1.a the continuous trajectories can not cross the line I that is a separating line. The abstraction of figure 1.b is based on rectangles without considering this property, so a reachability analysis on this abstraction will conclude that the region z5 is reachable from the point P. Figure 2 is an other example of the importance of the choice of the hyperplanes. It is considered that the derivative of $x_1$ is negative under the line I and positive above it. If a partition based on rectangles is used according to figure 2.a, as for some points of z1 located above the line the continuous trajectory enter z2 and conversely for some points of z2 located under it the trajectory enters z1, the abstract automaton is the one of figure 2.b. As for some points of z1 the derivative of $x_1$ is positive and for other ones it is negative, in the abstract model for each point of z1 the derivative of $x_1$ is defined by its inclusion in the interval $[l, u]$ where l is negative and u positive. The reachability analysis on this abstraction will so conclude that the striped region can be reached from point P although it can not.

Fig. 2. Unstructured abstract system.
For systems for which the vector field of each location is given by an equation such as equation (1) where $x$ is a 2 dimension vector and $A$ is non-singular, it is possible to use properties of this dynamic to define linear regions consistent with these properties in order to get an abstraction with tight approximation and few locations and transitions.

$$\dot{x} = Ax + b$$  \hspace{1cm} (1)

The first property which is used is linked to eigenvalues and eigenvectors of matrix $A$. If $A$ has a real eigenvalue, the line defined by its associated eigenvector and the equilibrium point (that is the solution of $Ax_c + b = 0$) is invariant. All continuous trajectories starting on this line are included in it, so no continuous trajectories can cross this separating line. Considering a region of the invariant of a location on one side of this line will lead to a location which is not reachable from locations associated with regions on the other side. So if $A$ has real eigenvalues the lines defined by the equilibrium point and the eigenvectors are used to split the invariant.

If this partition is too coarse or if the matrix has no real eigenvalues the following property is used. For such systems the derivative vectors for all points of a line to which the equilibrium point belongs are collinear. The proof is that such a line is defined by equation (2)

$$w^T(x - x_c) = 0$$  \hspace{1cm} (2)

which may be rewritten as:

$$w^TA^{-1}(x + A^{-1}b) = 0 \iff v^T \dot{x} = 0$$

with $v^t = w^T A^{-1}$

Furthermore with considerations on the convexity of the system it can be shown that for all points of a half line defined by the equilibrium point the derivative vectors are collinear and in the same direction. This is used to get on one hand an approximation of the vector field and, on the other hand, a simple transition system.

As seen, each line to which the equilibrium point belongs, is equivalently defined by equation (3).

$$\left\{ x / v^TAx + v^Tb = 0 \right\}$$  \hspace{1cm} (3)

Each sector defined by the equilibrium point and two half lines can then be characterised by equation (4).

$$\left\{ x / (v_1^TAx + v_1^Tb \geq 0) \land (v_2^TAx + v_2^Tb \leq 0) \right\}$$  \hspace{1cm} (4)

This is equivalent to the fact that for each point of the sector, the derivative vector satisfies the inequalities of equation (5).

$$v_1^T \dot{x} \geq 0, v_2^T \dot{x} \leq 0$$  \hspace{1cm} (5)

These inequalities defines a linear region in the derivative space, the borders of which are defined by the derivative vectors ($u_i$) ($u_i$ orthogonal with $v_i$) on the borders of the sector of the state space as shown figure 3. The activity of the location associated with the sector in the abstraction will so be defined by the inclusion of the derivative vector in the region defined by the two derivative vectors on the borders of the sector.

If the border of such a sector is not a separating line, continuous trajectories cross the border in one direction. Moreover if no separating line is included in the sector it can be shown, with considerations on continuity, that if trajectories cross one border to get inside the sector they cross the other one to get outside. If one border is a separating line it can of course not be crossed, the sector is either a terminal one in which trajectories remain, either an initial one.

As a consequence, when such linear sectors are used to partition the invariant, there is at most one incoming transition and one outgoing transition for each new location and the subsequent automaton is very simple as it can be seen figure 4. For each new location, the vector field is then approximated by the linear region defined by the derivative vectors on the borders of the sector that can be closed by lower and upper bounds of derivatives of each state variable.

![Fig. 3. A sector (S) and the related region (S') in the derivative space.](image)

![Fig. 4. Sectors splitting and structuring of the abstract system.](image)
4 ERROR CONSIDERATIONS

Of course the accuracy of the abstraction is linked to the number of sectors that are used to partition the invariant but also to their position. In order to qualify the splitting, it is necessary to get a bound of the approximation induced by the abstraction.

For a point $x$ of the sector, if $x_0$ is the intersection of the outgoing border with the half line defined by the point $x$ and the derivative on the incoming border, and $x_1$ the intersection with the half line defined by the derivative on the outgoing border, the space that is computed as reachable from $x$ in the sector is the triangle $(x_0, x_1, x_2)$ as it can be seen figure 5. The length of the segment $(x_i, x_j)$ can then be used to quantify the approximation induced for this point, and the upper bound of this length for all points of the sector can be used to quantify the approximation induced by the sector.

The point for which the upper bound is reached can be determined by geometric considerations. For all points of the sector the reachable triangles are similar, so this point is the one for which the length of the segment $(x_0, x_1)$ is maximal. This point is the intersection of the incoming border of the sector with the border of the invariant $(x_0)$ if the intersection of the outgoing border with the same border of the invariant exists. If this is not the case it is more difficult to find the point that gives the upper bound of the length of the segment $(x_0, x_1)$ but it is easy to find a point that gives an overvaluation of it.

If this is considered more closely, it can be seen that in fact this point $x_0$ defines the upper bound of the length of the segment $(x_1, x_2)$ but as the reachable state is the intersection of the triangle $(x_0, x_1, x_2)$ with the sector and with the invariant it may happen that this bound is an overvaluation of the approximation. This is not very significant except when the 'outgoing' border is a separating line defined by a real eigenvalue of matrix $A$. The overvaluation is then infinite and not really useful. It is then necessary to consider more precisely the reachable space within the intersection of the sector with the invariant in order to bound the approximation.

Fig. 5. Approximation induced by abstraction.

Fig. 6. Reachable space with separating line border.

Figure 6 this reachable space is drawn for a stable system and it is possible to see that the approximation is then the length of the segment $(x_1, x_2)$. Similar considerations on triangles can then be used to find the upper bound of the approximation induced by abstraction.

These results can be used as criteria to partition the invariant of locations. The problem to solve is then to find the outgoing border of a sector, the incoming border of which is known, in order that the approximation remains smaller than a fixed value.

If $\alpha_0, \alpha_2, \beta$ are three real positive variables such that $x_0 - x_1 = \alpha_0 x_0$, $x_1 - x_2 = \alpha_2 x_1$ and $x_2 - x_1 = \beta(x_1 - x_2)$, the vector $x_1 - x_2$ is given by equation (6) where $\alpha_1$ and $\beta$ are linked by equation (7).

$$x_1 - x_2 = (1 - \beta)(\alpha_1 A + I)(x_0 - x_1)$$  \hspace{1cm} (6)

$$\alpha_1 A - \alpha_1 (1 + \alpha_1 A) + (1 - \beta)(1 + \alpha_1 A)(x_0 - x_1) = 0$$  \hspace{1cm} (7)

The case $\alpha_1 = -1/\lambda$ (where $\lambda$ is an eigenvalue of $A$) is the case where $x_1 - x_2$ is an eigenvector of $A$.

For any $\alpha_1 \neq -1/\lambda$ and if the vector $x_0 - x_e$ is not an eigenvector of $A$ then none of the borders is a separating line and equation (7) allows to compute $\beta$ and $\alpha_2$ as functions of $\alpha_1$. The value of $\alpha_1$ can then be chosen with equation (6) in order to fix the value of the norm of $x_1 - x_2$. The outgoing border of a sector can then be computed for a given incoming border and a maximum of this norm.

If the considered region is near a separating line, it is possible to use equations, such as equation (8) for a stable system, to solve the problem.

$$x_1 - x_e = -1/\lambda (A + I)(x_0 - x_e)$$  \hspace{1cm} (8)

It is then possible by solving the equations (7) or (8) to automatically compute from a fixed value, the sectors of the partition of the invariant and the automaton associated with this partition. For each sector, when the space of the sector that is reachable from one point of the sector is calculated, it is assured that the abstraction induces an approximation that remains lower than the given value. It is then
possible to compute an upper bound of the approximation induced for the invariant.

5. EXAMPLE

5.1 Presentation of the example

In order to illustrate the contributions of this method, the system described by Sylva and Krogh (2000) is used. This system has 2 modes (On, Off) with distinct dynamics and its control change from mode On to mode Off when the second component of the state vector reaches the value 2.5. The aim is to use Hytech to compute an approximation of the reachable state vector reaches the value 2.5. The aim is to use

\[
\dot{x} = \left( \begin{array}{c} -1 \\ 1 \\ -3 \end{array} \right) + \left( \begin{array}{c} 0 \\ 10 \end{array} \right)
\]

(9)

In order to compare with the approximate solutions obtained, a numerical approximated solution can be computed and gives: \( x_1 = 1.0841 \quad (x_2 = 2.5) \)

5.2 Partition by rectangles

The first partition of the invariant is based on rectangles corresponding to an interval length 1 on each component (figure 7.a). Taking into account the directions of derivatives on each border leads to the automaton of the figure 7.b. Each location of this automaton is associated with on the one hand an invariant corresponding to the rectangle and on the other hand a continuous activity obtained by computing the upper and lower bounds of each component of the derivative. The activities associated with each new location are:

- \( z_1: -1 \leq \dot{x}_1 \leq 1 \)
- \( z_2: -2 \leq \dot{x}_1 \leq 0 \)
- \( z_3: -3 \leq \dot{x}_1 \leq -1 \)
- \( 7 \leq \dot{x}_2 \leq 11 \)
- \( 8 \leq \dot{x}_2 \leq 12 \)
- \( 9 \leq \dot{x}_2 \leq 13 \)
- \( z_4: 0 \leq \dot{x}_1 \leq 2 \)
- \( z_5: -1 \leq \dot{x}_1 \leq 1 \)
- \( z_6: -2 \leq \dot{x}_1 \leq 0 \)
- \( 4 \leq \dot{x}_2 \leq 8 \)
- \( 5 \leq \dot{x}_2 \leq 9 \)
- \( 6 \leq \dot{x}_2 \leq 10 \)
- \( z_7: 1 \leq \dot{x}_1 \leq 3 \)
- \( z_8: 0 \leq \dot{x}_1 \leq 2 \)
- \( z_9: -1 \leq \dot{x}_1 \leq 1 \)
- \( 1 \leq \dot{x}_2 \leq 3 \)
- \( 2 \leq \dot{x}_2 \leq 6 \)
- \( 3 \leq \dot{x}_2 \leq 7 \)

The result of the computation by Hytech of the reachable space is \( 67/70 \leq x_1 \leq 17/10 \)

\( (0.957 \leq x_1 \leq 1.7) \) to which the numerical result belongs.

Fig. 7. Partition based on rectangles (a) and the corresponding automaton (b)

5.3 Partition by sectors

The equilibrium point of the dynamic system specified by equation (8) is (5,5). This system also have two separating lines but none of these crosses the invariant under consideration.

The partition is based on 5 sectors defined by the equilibrium point and 5 half lines as shown figure 8.a. The crossing of the borders of the sectors define the transitions among locations and the subsequent abstract automaton is represented figure 8.b. The activity, that is associated with each location, is defined by the derivatives on the border and upper and lower bounds for each component of the derivative on the sector. These activities are the following.

\[
\begin{align*}
& \text{s1: } -3 \leq \dot{x}_1 \leq -6/7 & \quad 46/7 \leq \dot{x}_2 \leq 13 & \quad -13/3 \leq \dot{x}_2 \leq -23/3 \dot{x}_1 \\
& \text{s2: } -3/2 \leq \dot{x}_1 \leq 0 & \quad 46/7 \leq \dot{x}_2 \leq 13 & \quad \dot{x}_2 \geq -26/3 \dot{x}_1 \\
& \text{s3: } 0 \leq \dot{x}_1 \leq 1 & \quad 7/2 \leq \dot{x}_2 \leq 10 & \quad \dot{x}_2 \geq 7 \dot{x}_1 \\
& \text{s4: } 1/2 \leq \dot{x}_1 \leq 2 & \quad 8/3 \leq \dot{x}_2 \leq 7 & \quad 2 \leq \dot{x}_2 \leq 7 \dot{x}_1 \\
& \text{s5: } 4/3 \leq \dot{x}_1 \leq 3 & \quad 1 \leq \dot{x}_2 \leq 4 & \quad 1/3 \leq \dot{x}_2 \leq 2 \dot{x}_1 \\
\end{align*}
\]

Fig. 8. Partition based on sectors (a) and corresponding automaton (b).
The result of the computation by Hytech with this abstract automaton is \[ 454/455 \leq x_1 \leq 177/124 \] (0.997.. \leq x_1 \leq 1.427..).

This result is a thinner approximation of the exact value whereas the automaton on which it is based is much simpler that the previous one.

6. CONCLUSIONS

This article has considered the problem of partitioning the invariant of a location of an hybrid automaton in order to approximate its continuous behaviour with a linear hybrid automaton. A method that uses the properties of the continuous dynamics of a class of systems in order to help the partitioning has been presented. In order to get more accurate approximation of the vector field and a simpler automata, it is based on the use of sectors defined by the equilibrium point and half lines. Moreover considerations on the accuracy of the approximation can be used to partition the invariant.

As it is exemplified, the automaton that is built by this method really allows more accurate computation of the reachable space whereas it has less locations and transitions that one built on rectangle partition. Of course in practice, a rectangular abstraction is easier to compute but the complexity that is induced by the linear region which are used is worthwhile. The number of locations and transitions is a particularly important criterion when merging the abstracting linear automata of all locations.

Future works are concerned with many points in order to improve the method. The first one is to study the abstract automata from the temporal accuracy point of view in order to define criteria to split the sectors in such a way that the error introduced on time may be bound. An other point is the use of these principles for continuous systems of higher dimension. If most of the useful properties remain it is necessary to introduce new criteria in order to choose the linear borders that split the invariant.

REFERENCES


