Reachability of Uncertain Linear Systems Using Zonotopes*

Antoine Girard

Department of Electrical and Systems Engineering,
University of Pennsylvania, Philadelphia, PA 19104
agirard@seas.upenn.edu

Abstract. We present a method for the computation of reachable sets of uncertain linear systems. The main innovation of the method consists in the use of zonotopes for reachable set representation. Zonotopes are special polytopes with several interesting properties : they can be encoded efficiently, they are closed under linear transformations and Minkowski sum. The resulting method has been used to treat several examples and has shown great performances for high dimensional systems. An extension of the method for the verification of piecewise linear hybrid systems is proposed.

1 Introduction

Reachability computation is required in several tasks such as verification or synthesis of hybrid systems [10, 19]. Except for very specific classes of hybrid systems [4, 15], exact computation of the reachable sets is impossible. The main difficulty lies in the computation of the reachable sets of the continuous dynamics. The importance of the problem has motivated much research on approximate reachability analysis. Two main approaches have been developped. The first one includes all abstraction methods (see for instance [1, 20]). The main idea is to process the reachability analysis on a simple abstract system which approximates a more complex one. The second approach consists in computing directly approximations of the reachable sets of the system [2, 5, 7, 14, 16, 18].

The success of such methods lies in the choice of an efficient representation of the approximations of the reachable sets. Methods have been proposed using several set representations such as general polytopes [7] oriented hyperrectangles [18], orthogonal polyhedra [2], ellipsoids [14] or level sets [16]. These methods have been used and have succeeded in solving some case studies. However, they remain expensive and their use is only limited to small systems.

Thus, today, the challenge for new work on reachability is to find how we can handle large-scale (or even middle-scale) systems. Recently [21], a new method has been proposed allowing to process safety verification for linear systems of high dimension (up to dimension 100 in a reasonnable time).

* Research partially supported by the Région Rhône-Alpes (Projet CalCel).

M. Morari and L. Thiele (Eds.): HSCC 2005, LNCS 3414, pp. 291–305, 2005.

In this paper, we propose a method for the computation of an over-approximation of the reachable sets of uncertain linear systems. The reachable sets are represented as the union of zonotopes (special polytopes). The resulting approximations are of good quality. Moreover, the method can be used for large-scale systems.

The paper is organized as follows. First, we introduce the mathematical notion of zonotope. Then, we explain our algorithm for the computation of approximate reachable sets of uncertain linear systems. Afterwards, we present some experimental results. Finally, we use it for hybrid system verification. For a better readability, the proofs are state in the appendix.

2 Zonotopes: Definition and Properties

Zonotopes are a special class of convex polytopes. Traditionally, a zonotope is defined as the image of a cube under an affine projection [22]. Equivalently, a zonotope is a Minkowski sum of a finite set of line segments. In this paper, we will use the following definition:

Definition 1 (Zonotope). *A zonotope Z is a set such that:*

$$Z = \left\{ x \in \mathbb{R}^n : x = c + \sum_{i=1}^{i=p} x_i g_i,\ -1 \leq x_i \leq 1 \right\}$$

where c, $g_1, \dots, g_p$ are vectors of $\mathbb{R}^n$. We note $Z = (c, < g_1, \dots, g_p >)$.

Thus, it is clear that a zonotope is a polytope. Parallelepipeds and hyper-rectangles are particular zonotopes.

Note that a zonotope $Z = (c, < g_1, \dots, g_p >)$ is always centrally symmetric and that the point $c \in \mathbb{R}^n$ is the center of Z. The collection of vectors $g_1, \dots, g_p$ is called the set of generators of Z. On figure 1, we represented a planar zonotope with three generators. For a zonotope with p generators in $\mathbb{R}^n$, the value of p/n is called the order of the zonotope. For instance, a parallelepiped is a zonotope of order 1. From a practical point of view, the definition 1 gives an efficient representation of the set since the number of faces of a zonotope in $\mathbb{R}^n$ with p

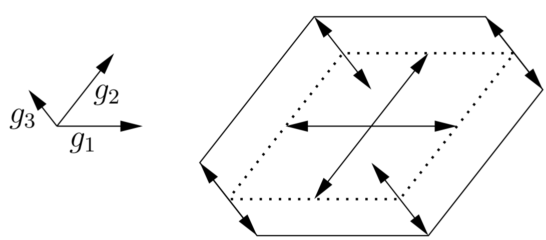

Fig. 1. Example of a zonotope with three generators

generators is in $O(p^{n-1})$ [11]. Zonotopes have long been studied in combinatorial geometry [22]. Practical application of zonotopes have been shown in various domains such as systems of polynomial equations [12], computational geometry [11] or rigorous approximation of dynamical systems [13, 9].

In this paper, we propose using zonotopes to over-approximate the reachable sets of uncertain linear systems. The use of zonotopes has been motivated by two main properties:

1. Zonotopes are closed under linear transformation. Let $\mathcal{L}$ be a linear map and $Z = (c, < g_1, \ldots, g_p >)$ a zonotope,

$$\begin{aligned}\mathcal{L}Z &= \left\{\mathcal{L}x : x = c + \textstyle\sum_{i=1}^{i=p} x_i g_i,\ -1 \leq x_i \leq 1\right\} \\ &= (\mathcal{L}c, < \mathcal{L}g_1, \ldots, \mathcal{L}g_p >).\end{aligned}$$

   The image of a zonotope by a linear map can be computed in linear time with regard to the order of the zonotope.
2. Zonotopes are closed under Minkowski sum. Let $Z_1 = (c_1, < g_1, \ldots, g_p >)$ and $Z_2 = (c_2, < h_1, \ldots, h_q >)$ be two zonotopes,

$$Z_1 + Z_2 = (c_1 + c_2, < g_1, \ldots, g_p, h_1, \ldots, h_q >).$$

   Thus, the Minkowski sum of two zonotopes can be computed by the concatenation of two lists.

3 Approximation of Reachable Sets

Let us consider the following uncertain linear system :

$$x'(t) = Ax(t) + u(t),\ \|u(t)\| \leq \mu \tag{1}$$

where A is an $n \times n$ matrix and $\|.\|$ denotes the infinity norm on $\mathbb{R}^n$ ($\|x\| = \max_{i=1}^{i=n} |x_i|$). Given a set of possible initial values I, the reachable set of the system at the time t is

$$\Phi_t(I) = \{y \in \mathbb{R}^n : \exists x \text{ solution of } (1)\ ,\ x(0) \in I \wedge x(t) = y\}.$$

The reachable set on the interval $[\underline{t}, \overline{t}]$ from the set of initial values I can therefore be defined by

$$\mathcal{R}_{[\underline{t},\overline{t}]}(I) = \bigcup_{t \in [\underline{t},\overline{t}]} \Phi_t(I).$$

In [10], a method using the maximum principle has been proposed for the computation of the reachable sets of uncertain linear systems such as (1). In [5], a general method for uncertain systems is proposed. This method works for any uncertain system provided you can compute the reachable sets of an associated deterministic system. This technique makes intensive use of the Minkowski sum.

Hence, it is generally expensive (particularly for high dimensional systems). For the reasons mentioned in the previous section, the use of zonotopes may be a good solution to avoid expensive computations of the Minkowski sum.

Let T be a positive real number, we want to compute an over-approximation of the reachable set $\mathcal{R}_{[0,T]}(I)$. Our method has similarities with the flow pipe technique [7] which has been used successfully for deterministic systems. Let $r > 0$ be the time step, we assume that $N = T/r$ is an integer. The reachable set $\mathcal{R}_{[0,T]}(I)$ can be decomposed in the following way:

$$\mathcal{R}_{[0,T]}(I) = \bigcup_{i=0}^{i=N-1} \mathcal{R}_{[ir,(i+1)r]}(I). \tag{2}$$

Thus, if we are able to compute over-approximations of the sets $\mathcal{R}_{[ir,(i+1)r]}(I)$, we can compute an over-approximation of the set $\mathcal{R}_{[0,T]}(I)$. Moreover, we have

$$\mathcal{R}_{[ir,(i+1)r]}(I) = \Phi_r(\mathcal{R}_{[(i-1)r,ir]}(I)).$$

Therefore, we need to define conservative approximations of the maps $\mathcal{R}_{[0,r]}$ and Φ_r, for r arbitrary small. Moreover, since we aim to use zonotopes, these conservative approximations must map zonotopes into zonotopes.

3.1 Conservative Approximation of Φ_r

Let Z be a zonotope in $\mathbb{R}^n$. Let $x \in Z$, $y \in \Phi_r(x)$, there exists an admissible input u such that

$$y = e^{rA}x + \int_0^r e^{(r-s)A}u(s)ds.$$

Therefore,

$$\|y - e^{rA}x\| \leq \int_0^r e^{(r-s)\|A\|}\mu ds = \frac{e^{r\|A\|} - 1}{\|A\|}\mu. \tag{3}$$

Let us note $\beta_r = \frac{e^{r\|A\|}-1}{\|A\|}\mu$, from the previous equation, $\Phi_r(Z)$ is included in the set $e^{rA}Z + \Box(\beta_r)$ where $\Box(\beta_r)$ denotes the ball of center 0 and of radius β_r for the infinite norm. Note that $\Box(\beta_r)$ is actually a hypercube and consequently it is a zonotope. Hence, the set $e^{rA}Z + \Box(\beta_r)$ over-approximating $\Phi_r(Z)$ is a zonotope. Moreover, we can show that the quality of the approximation is good for the Hausdorff distance.

Definition 2 (Hausdorff distance). *The Hausdorff distance between two subsets of* $\mathbb{R}^n$, S_1 *and* S_2 *is*

$$d_H(S_1, S_2) = \max\left(\sup_{x_1 \in S_1} \inf_{x_2 \in S_2} \|x_1 - x_2\|, \sup_{x_2 \in S_2} \inf_{x_1 \in S_1} \|x_1 - x_2\|\right).$$

Lemma 1 (Conservative approximation of Φ_r)

1. *Conservative approximation:* $\Phi_r(Z) \subseteq e^{rA}Z + \Box(\beta_r)$
2. *Convergence:* $d_H(\Phi_r(Z), e^{rA}Z + \Box(\beta_r)) \leq \mu\|A\|e^{r\|A\|}r^2$.

3.2 Conservative Approximation of $\mathcal{R}_{[0,r]}$

The over-approximation process of $\mathcal{R}_{[0,r]}$ is a bit more complex. Let $Z = (c, < g_1, \ldots, g_p >)$ be a zonotope; using (3) it is clear that

$$\mathcal{R}_{[0,r]}(Z) \subseteq \left(\bigcup_{t \in [0,r]} e^{tA} Z \right) + \square(\beta_r). \tag{4}$$

Thus, we shall over-approximate the reachable set of the deterministic linear system $x' = Ax$ using a zonotope, and then add the set $\square(\beta_r)$. Our method for the approximation of the reachable set of the deterministic system is quite similar to the one of [7] or [10] but with zonotopes.

In [10], for instance, the method proposed is the following. First, the reachable set is approximated by the convex hull of Z and $e^{rA}Z$. Secondly, this set is bloated in order to over-approximate the reachable set. The convex hull of two zonotopes is generally not a zonotope, hence, we can not apply directly this method to our problem. For instance, we can replace the convex hull by the smallest zonotope enclosing Z and $e^{rA}Z$. This problem is complex and might be very expensive to solve for high dimensional systems (see [11]). Therefore, we take a rougher approximation which is very simple to compute:

$$P = \left(\tfrac{c+e^{rA}c}{2}, < \tfrac{g_1+e^{rA}g_1}{2}, \ldots, \tfrac{g_p+e^{rA}g_p}{2}, \tfrac{c-e^{rA}c}{2}, \tfrac{g_1-e^{rA}g_1}{2}, \ldots, \tfrac{g_p-e^{rA}g_p}{2} >\right). \tag{5}$$

The center and the p first generators of the zonotope gives the mean value of the zonotopes Z and $e^{rA}Z$. The $p+1$ other generators are small (their norm is $O(r)$) and allow to enclose both sets Z and $e^{rA}Z$. Afterwards, this set is bloated. This is done by adding a ball of radius α_r to the zonotope P. α_r must be big enough so that $P + \square\alpha_r$ contains the reachable set of the deterministic system (the computation of the value of α_r can be found in appendix). The principle of the over-approximation of the reachable set is shown on figure 2.

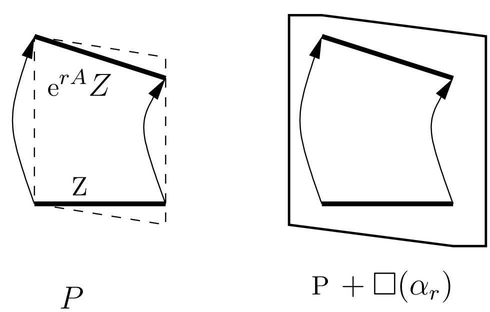

Fig. 2. Principle of the over-approximation of the reachable set

Lemma 2 (Conservative approximation of $\mathcal{R}_{[0,r]}$). *Let P be defined as in equation 5.*

1. *Conservative approximation:* $\mathcal{R}_{[0,r]}(Z) \subseteq P + \Box(\alpha_r + \beta_r)$
2. *Convergence:*
$d_H(\mathcal{R}_{[0,r]}(Z), P + \Box(\alpha_r + \beta_r)) \leq r\|A\|e^{r\|A\|}\left(\frac{\mu}{\|A\|} + (\frac{1}{2} + r)\sup_{x\in Z}\|x\|\right)$

with $\alpha_r = (e^{r\|A\|} - 1 - r\|A\|)\sup_{x\in Z}\|x\|$.

3.3 Reachability Algorithm

We can now present the reachability algorithm. The principle is similar to the one of the method presented in [5]. First, the reachable set is initialized using the method presented in the section 3.2. Afterwards, the image of the reachable set by the flow of the deterministic system $x' = Ax$ is computed and bloated as explained in the section 3.1.

Input: A zonotope of initial values $I = (c, < g_1, \ldots, g_p >)$
Result: An approximation of the reachable set $\mathcal{R}_{[0,T]}(I)$

$N = \frac{T}{r}$
$\alpha_r = (e^{r\|A\|} - 1 - r\|A\|)\sup_{x\in I}\|x\|$
$\beta_r = \frac{e^{r\|A\|}-1}{\|A\|}\mu$

$P_0 = (\frac{c+e^{rA}c}{2}, < \frac{g_1+e^{rA}g_1}{2}, \ldots, \frac{g_p+e^{rA}g_p}{2}, \frac{c-e^{rA}c}{2}, \frac{g_1-e^{rA}g_1}{2}, \ldots, \frac{g_p-e^{rA}g_p}{2} >)$
$Q_0 = P_0 + \Box(\alpha_r + \beta_r)$
$R_0 = Q_0$
for $i \leftarrow 1$ ***to*** $N-1$ **do**
  $P_i = e^{rA}Q_{i-1}$
  $Q_i = P_i + \Box(\beta_r)$
  $R_i = R_{i-1} \cup Q_i$
end
return R_N

Algorithm 1: Approximating the reachable set of system (1)

This algorithm, whose implementation is very simple, allows to compute an over-approximation of the reachable set $\mathcal{R}_{[0,T]}(I)$. The approximation converges to the reachable set as the time step becomes smaller.

Theorem 1 (Conservative approximation of $\mathcal{R}_{[0,T]}(I)$). *Let R_{N-1} be the set computed by algorithm 1.*

1. *Conservative approximation:* $\mathcal{R}_{[0,T]}(I) \subseteq R_{N-1}$
2. *Convergence:*

$$d_H(\mathcal{R}_{[0,T]}(I), R_{N-1}) \leq r\|A\|e^{\|A\|T}\left(\frac{2\mu}{\|A\|} + (\frac{1}{2} + r)\sup_{x\in Z}\|x\|\right).$$

3.4 Controlling the Expansion of the Order of Zonotopes

At each iteration of the loop of algorithm 1, the set Q_{i+1} is obtained by computing the image of Q_i by a linear map and by adding the set $\square(\beta_r)$. Consequently, the order of the zonotope Q_{i+1} equals the order of Q_i plus 1. Therefore, the order of the zonotope Q_i is $O(i)$. The memory allocation needed to encode the over-approximation of the set $\mathcal{R}_{[0,T]}(I)$ is in $O(N^2)$. We can also show that the time needed for its computation is also $O(N^2)$. For large value of N the over-approximation of $\mathcal{R}_{[0,T]}(I)$ can thus be quite expensive in memory and in time.

A solution to avoid this quadratic expansion is to limit the order of the zonotopes Q_i. Let m be the maximum order allowed for the zonotopes Q_i. If the order of the zonotope Q_i is m, then following algorithm 1, the order of Q_{i+1} should be $m+1$ which is greater to the maximum order allowed. We must have recourse to a reduction step. It consists in taking $2n$ generators of Q_{i+1}, $h_1, \dots, h_{2n}$, and to replace them by n generators, such that the new zonotope of order m contains Q_{i+1} (see figure 3). Equivalently, we have to over-approximate the zonotope $(0, < h_1, \dots, h_{2n} >)$ by a zonotope with n generators and whose center is 0. Let x be a point of the zonotope $(0, < h_1, \dots, h_{2n} >)$, then $x = \sum_{i=1}^{i=2n} x_i h_i$, where $x_i \in [-1, 1]$. x^j, the j-th component of x, is bounded in absolute value by $\sum_{i=1}^{i=2n} |h_i^j|$ where h_i^j is the j-th component of h_i. Therefore, $(0, < h_1, \dots, h_{2n} >)$ is included in the interval hull

$$\left[-\sum_{i=1}^{i=2n} |h_i^1| \,,\, \sum_{i=1}^{i=2n} |h_i^1|\right] \times \cdots \times \left[[-\sum_{i=1}^{i=2n} |h_i^n| \,,\, \sum_{i=1}^{i=2n} |h_i^n|\right]$$

which is a zonotope with n generators $h'_1, \dots, h'_n$ such that all the components of the vector h'_j are equal to 0 except the j-th one which is given by $\sum_{i=1}^{i=2n} |h_i^j|$.

The choice of the $2n$ generators of Q_{i+1} to be replaced is important for the quality of the approximation. The best selection consists in taking the vectors $h_1, \dots, h_{2n}$ such that the over-approximation of the zonotope $(0, < h_1, \dots, h_{2n} >)$ by an intervall hull is as good as possible (intervall hulls are zonotopes whose generators have only one non zero component). Let $Q_{i+1} = (c, < g_1, \dots, g_{(m+1)n} >)$ and let us assume that the generators have been sorted so that:

$$\|g_1\|_1 - \|g_1\|_\infty \le \|g_2\|_1 - \|g_2\|_\infty \le \cdots \le \|g_{(m+1)n}\|_1 - \|g_{(m+1)n}\|_\infty.$$

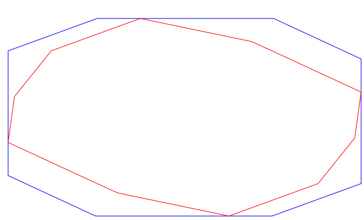

Fig. 3. Example of over-approximation of a zonotope by a zonotope of lower order

We choose for $i \in \{1, \dots, 2n\}$, $h_i = g_i$. These vectors are closed to vectors with only one non zero component and therefore $(0, < h_1, \dots, h_{2n} >)$ is well approximated by an intervall hull.

Other heuristics for the reduction step can be found in [13, 9].

4 Experimental Results

The method has been implemented in the free scientific software package Scilab. We used our method to compute the reachable set of numerous uncertain linear systems of various size. In this section, we present some of our results.

First, we considered the two dimensional system defined by :

$$A = \begin{pmatrix} -1 & -4 \\ 4 & -1 \end{pmatrix},\ \mu = 0.05.$$

We computed an over-approximation of the reachable set $\mathcal{R}_{[0,2]}(I)$ for the set of initial values $I = [0.9, 1.1] \times [-0.1, 0.1]$. The over-approximation has been computed using a time step of 0.02 (100 iterations). The maximum order allowed for zonotopes is 10 (20 generators). The result is shown on figure 4. We can see that the quality of the approximation is good.

We also computed an over-approximation of the reachable set $\mathcal{R}_{[0,1]}(I)$ of a five dimensional system where the Jordan form of the matrix A is

$$\begin{pmatrix} -1 & -4 & 0 & 0 & 0 \\ 4 & -1 & 0 & 0 & 0 \\ 0 & 0 & -3 & 1 & 0 \\ 0 & 0 & -1 & -3 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{pmatrix}$$

The perturbations are bounded by $\mu = 0.01$. The over-approximation has been computed using a time step of 0.005 (200 iterations) and the maximum order

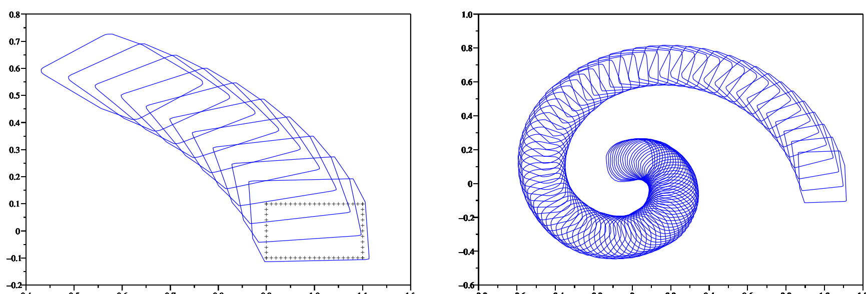

Fig. 4. Reachable set of the two dimensional example. Left: first iterations of the algorithm. Right: over-approximation of the reachable set $\mathcal{R}_{[0,2]}(I)$

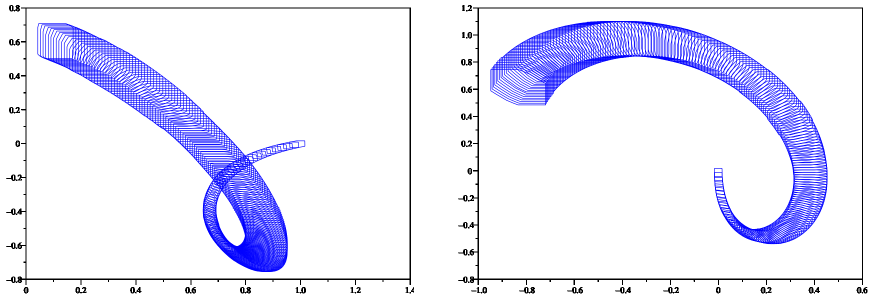

Fig. 5. Reachable set of the five dimensional example: projection on coordinates x_1 and x_2 (left), x_4 and x_5 (right)

Table 1. Computation times of the reachable set of uncertain linear systems of several dimensions. (Implementation: Scilab; Machine: Pentium III, 1 GHz)

Dimension	5	10	20	50	100
Cputime (s)	0.05	0.33	1.5	9.91	43.7

allowed for zonotopes is 40 (200 generators). Projections of the reachable set are shown on figure 4.

We also used our method for high dimensional systems. Experimental results are shown in table 1. We computed an over-approximation of the reachable set $\mathcal{R}_{[0,1]}(I)$ of uncertain linear systems of several dimensions (with $\mu = 0.01$). We used a time step equal to 0.01 (100 iterations) and the maximum order allowed for zonotopes is 5. The matrices were chosen at random and then normalized (for the infinity norm). We can see that our algorithm has great performances. Moreover, it particularly fits high-dimensional systems since it computes the reachable set of a hundred dimensional system in less than 1 minute.

5 Verification of Hybrid Systems

Our method can of course be incorporated in a hybrid system verification process. It is compatible with high level algorithms used by the toolboxes d/dt [3] and CheckMate [8]. Let us consider hybrid systems where the continuous dynamics are given by uncertain linear differential equations such as (1). In each mode, the reachable set of the hybrid system can be computed efficiently by our method. It remains for us to incorporate an event detection process which checks at each step wether the reachable set intersects the guards of the system or not. We will assume that the guards are specified by switching planes:

$$G_{q,q'} = \{x \in \mathbb{R}^n : d_{q,q'}^T x = e_{q,q'}\}, \text{ where } d_{q,q'} \in \mathbb{R}^n,\ e_{q,q'} \in \mathbb{R}.$$

5.1 Detecting Intersection with Switching Planes

Thus, at each step of algorithm 1, we have to check if Q_i the over-approximation of $\mathcal{R}_{[ir,(i+1)r]}(I)$ intersects the planes. This problem is equivalent to check if a zonotope intersects a hyperplane.

Let $Z = (c, < g_1, \dots, g_p >)$ be a zonotope and $G = \{x \in \mathbb{R}^n : d^T x = e\}$ a hyperplane, the intersection of Z and G is not empty if and only if

$$\exists x_1 \in [-1,1], \dots, x_p \in [-1,1],\ d^T c + \sum_{i=1}^{i=p} d^T g_i x_i = e.$$

Thus, the zonotope Z intersects the hyperplane G, if and only if

$$(e - d^T c) \in \left[-\sum_{i=1}^{i=p} |d^T g_i|, \sum_{i=1}^{i=p} |d^T g_i| \right].$$

Hence, we can see that it is very easy to check if a zonotope intersects a hyperplane. Moreover, this is done in linear time with regard to the number of generators of the zonotope as well as the dimension of the system.

5.2 Checking Robustness of the Two Tank System

The two-tank system (see figure 6) has been presented in [17] as an illustration of limit cycles arising in hybrid systems. The system consists of two tanks and two valves. The first valve allows to add water in the first tank, while the second one allows to drain off the second tank. There are also a constant inflow in tank 1 and a constant outflow in tank 2. The system is obtained by linearization about an operating point. The objective is to keep the water levels within some limits using a feedback on/off switching strategy for the valves.

The two valve settings result in four discrete states for our piecewise linear hybrid system. The discrete dynamics are given by the automaton presented on figure 6. The continuous dynamics are given by affine differential equations $x' = A_q x + b_q$, $q \in \{1,2,3,4\}$ with

$$A_1 = \begin{pmatrix} -1 & 0 \\ 1 & 0 \end{pmatrix} A_2 = \begin{pmatrix} -1 & 0 \\ 1 & 0 \end{pmatrix} A_3 = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} A_4 = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$$

$$b_1 = \begin{pmatrix} -2 & 0 \end{pmatrix}^t \ b_2 = \begin{pmatrix} 3 & 0 \end{pmatrix}^t \quad b_3 = \begin{pmatrix} -2 & -5 \end{pmatrix}^t \ b_4 = \begin{pmatrix} 3 & -5 \end{pmatrix}^t$$

It is well known that this system has a stable limit cycle. In this part, we propose to use our method to check the robustness of this limit cycle. Indeed, the real continuous dynamics can not be exactly known, there are uncertainties on the characteristics of the valves, variations of the inflow and of the outflow. These uncertainties can be modeled by adding a small perturbation term:

$$x'(t) = A_{q(t)} x(t) + b_{q(t)} + u(t),\ \|u(t)\| \leq \mu.$$

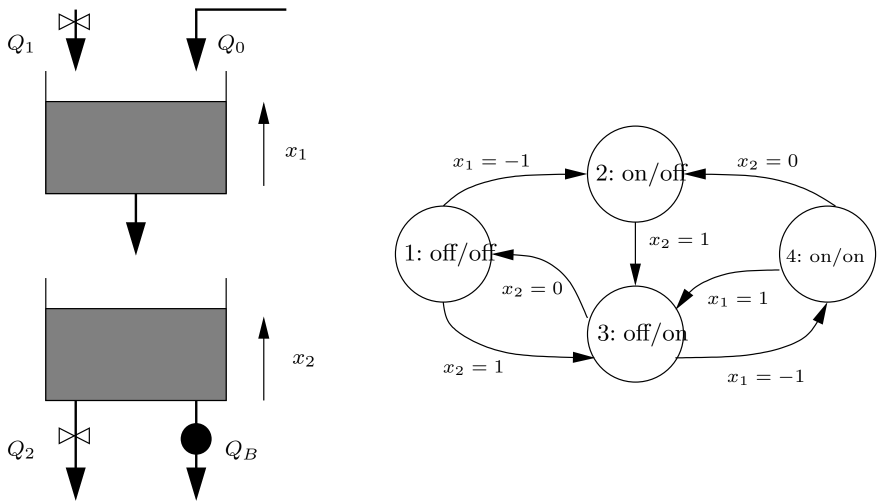

Fig. 6. The two tank system

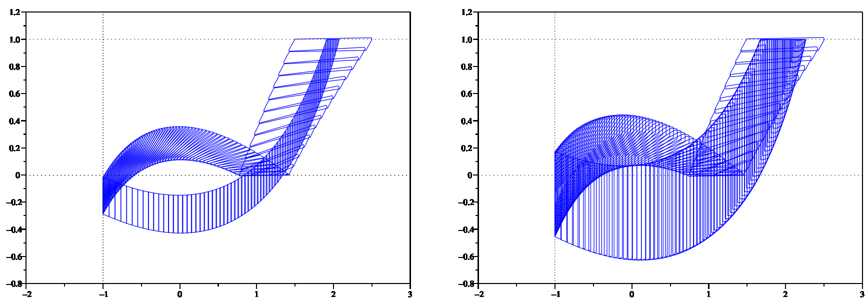

Fig. 7. Reachable set of the two tank system. Left: $\mu = 0.01$. Right: $\mu = 0.1$

The goal for us is to check if the periodic behaviour remains when we replace the deterministic dynamics by the uncertain ones. It is easy to generalize the method presented in the previous sections in order to handle uncertain affine dynamics.

We computed the reachable set of the two tank system, for the initial discrete state 3, and for the set of initial values of the continuous variable $I = [1.5, 2.5] \times \{1\}$. The reachable set has been computed for uncertainties bounded by 0.01 and then by 0.1. The result is shown on figure 7. In both cases, we can check that the periodic behaviour is conserved. Thus, the switching strategy is acceptable since the water levels in each tank remain bounded.

6 Conclusion

In this paper, we presented a method for reachability analysis of uncertain linear systems. The use of zonotopes allows an efficient implementation of the reachability algorithm. The over-approximation of the reachable set converges as the time step becomes smaller. An improvement of the algorithm has been proposed, it consists in the reduction step (approximation of zonotopes by zonotopes of lower order). Our method has been tested and has shown great performances for high-dimensional systems. Furthermore, the method can be efficiently used for reachability analysis of hybrid systems.

Future work should focus on several points. First, more general classes of linear systems should be considered. We believe that our method can be generalized to linear systems of the form:

$$x'(t) = Ax(t) + Bu(t),\ u(t) \in U$$

where U is a zonotope. For some polytopic norm, the order of approximation of the reachable set should be conserved. Secondly, a rigorous analysis of the error introduced by the reduction step should be done. It is important to quantify the influence of the maximum order allowed for zonotopes. The third important point is the extension of the method to non-linear dynamics. The combination of our method with several techniques already existing [5, 7, 13] could allow to handle such dynamics.

References

1. R. Alur, T. Dang, F. Ivancic, Reachability analysis of hybrid systems via predicate abstraction, *Hybrid Systems : Computation and Control*, C.J. Tomlin, M.R. Greenstreet (Eds), no . 2289 in LNCS, pp 35-48, 2002.
2. E. Asarin, O. Bournez, T. Dang, O. Maler, Approximate reachability analysis of piecewise linear dynamical systems, *Hybrid Systems : Computation and Control*, N. Lynch, B. H. Krogh (Eds), no. 1790 in LNCS, pp 21-31, Springer, 2000.
3. E. Asarin, T. Dang, O. Maler, d/dt: A verification tool for hybrid systems, *in the Proc. of CDC'01*, 2001.
4. E. Asarin, G. Schneider, S.Yovine. Towards computing phase portraits of polygonal differential inclusions, *Hybrid Systems : Computation and Control*, C.J. Tomlin, M.R. Greenstreet (Eds), no . 2289 in LNCS, pp 49-61, 2002.
5. E. Asarin, T. Dang, A. Girard, Reachability of non-linear systems using conservative approximations, *Hybrid Systems : Computation and Control*, O. Maler, A. Pnueli (Eds), no. 2623 in LNCS, pp 22-35, Spinger, 2003.
6. E. Asarin, T. Dang, Abstraction by projection and application to multi-affine systems, *Hybrid Systems : Computation and Control*, R. Alur, G.J. Pappas (Eds), no. 2993 in LNCS, pp 32-47, Springer, 2004.
7. A. Chutinan, B.H. Krogh, Verification of polyhedral invariant hybrid automata using polygonal flow pipe approximations. *Hybrid Systems : Computation and Control*, F. Vaandrager, J. van Schuppen (Eds), no. 1569 in LNCS, pp 76-90, Springer, 1999.

8. A. Chutinan, B.H. Krogh, Computational techniques for hybrid system verification, *IEEE Trans. on Automatic Control*, vol. 48, no. 1, 2003, pp. 64-75.
9. Combastel C., A state bounding observer based on zonotopes, in *Proc. of European Control Conference*, 2003.
10. T. Dang, Vérification et synthèse des systèmes hybrides, *Thèse de Doctorat*, Institut National Polytechnique de Grenoble, 2000.
11. L.J. Guibas, A. Nguyen , L. Zhang, Zonotopes as bounding volumes, in *Proc. of Symposium on Discrete Algorithms*, pp 803-812.
12. B. Huber and B. Sturmfels, A polyhedral method for solving sparse polynomial systems, *Math. of Computation*, 64:1541-1555, 1995.
13. W. Kühn, Zonotope dynamics in numerical quality control, in *Mathematical Visualization*, H.-C. Hege, K. Polthier (Eds), pp 125-134, Springer, 1998.
14. A. Kurzhanski, P. Varaiya, Ellipsoidal tehcniques for reachability analysis, *Hybrid Systems : Computation and Control*, N. Lynch, B. H. Krogh (Eds), no. 1790 in LNCS, Springer, 2000.
15. G. Lafferriere, G. Pappas, S. Yovine, Reachability computation for linear systems, *Proc. IFAC World Congress*, E:7-12, 1999.
16. I. Mitchell, C. Tomlin, Level set methods for computation in hybrid systems, *Hybrid Systems : Computation and Control*, N. Lynch, B. H. Krogh (Eds), no. 1790 in LNCS, Springer, 2000.
17. M. Rubensson, B. Lennartson, S. Pettersson, Convergence to limit cycles in hybrid systems: an example, *Large Scale Systems: Theory and Applications*, pp 704-709, 1998.
18. O. Stursberg, B.H. Krogh, Efficient representation and computation of reachable sets for hybrid systems, *Hybrid Systems : Computation and Control*, O. Maler, A. Pnueli (Eds), no. 2623 in LNCS, pp 482-497, Spinger, 2003.
19. C. Tomlin, I. Mitchell, A. Bayen, and M. Oishi, Computational techniques for the verification and control of hybrid systems, *Proc. of the IEEE*, 91(7):986-1001, July 2003.
20. A. Tiwari, G. Khanna, Series of abstractions for hybrid automata, *Hybrid Systems : Computation and Control*, C.J. Tomlin, M.R. Greenstreet (Eds), no . 2289 in LNCS, pp 465-478, 2002.
21. H. Yazarel, G.J. Pappas, Geometric programming relaxations for linear system reachability, in *Proc. American Control Conference*, 2004.
22. G.M. Ziegler, Lectures on polytopes, *Graduate texts in Mathematics*, Springer-Verlag, 1995.

Appendix

Proof of Lemma 1 (Adapted from [5])

The proof of the first part of the lemma is a consequence of equation (3). Let us prove the second part.

Let $x \in e^{rA}Z + \Box\beta_r$, there exists $z \in Z$ such that $\|e^{rA}z - x\| \leq \beta_r$. Let us consider the constant input function u such that $u(s) = \frac{\|A\|}{e^{r\|A\|-1}}(x - e^{rA}z)$ for all $s \in [0, r]$. We can check that $\|u(s)\| \leq \mu$, therefore,

$$x_u = e^{rA}z + \int_0^r e^{(r-s)A}u(s)\, ds \in \Phi_r(Z).$$

Then,

$$x_u - x = e^{rA}z - x + \int_0^r e^{(r-s)A}u(s)\,ds = \int_0^r e^{(r-s)A}u(s) - \frac{1}{r}(x - e^{rA}z)\,ds$$
$$= \int_0^r e^{(r-s)A}u(s) - \frac{e^{r\|A\|}-1}{r\|A\|}u(s)\,ds$$
$$= \int_0^r e^{(r-s)A}u(s) - u(s) - \frac{e^{r\|A\|}-r\|A\|-1}{r\|A\|}u(s)\,ds.$$

Therefore,

$$\|x_u - x\| \le \mu \int_0^r (r-s)\|A\|e^{\|A\|(r-s)} + \frac{r\|A\|e^{r\|A\|}}{2}\,ds \le \mu r^2\|A\|e^{r\|A\|}.$$

Proof of Lemma 2

Let x be an element of Z, $t \in [0,r]$, it is reasonnable to approximate the value of $e^{tA}x$ by $x + \frac{t}{r}(e^{rA}x - x)$. Indeed,

$$e^{tA}x - x - \frac{t}{r}(e^{rA}x - x) = \sum_{k=2}^{k=\infty} \frac{t(t^{k-1} - r^{k-1})}{k!}A^k x.$$

It follows that

$$\|e^{tA}x - x - \frac{t}{r}(e^{rA}x - x)\| \le (e^{r\|A\|} - 1 - r\|A\|)\|x\|. \tag{6}$$

Let $\alpha_r = (e^{r\|A\|} - 1 - r\|A\|)\sup_{x\in Z}\|x\|$, from (4) and (6), we have $\mathcal{R}_{[0,r]}(Z) \subseteq Q + \square(\alpha_r + \beta_r)$ where $Q = \{x + \frac{t}{r}(e^{rA}x - x) : x \in Z, t \in [0,r]\}$. We can check that the zonotope P defined by equation (5) contains the set Q. Therefore, the first part of the lemma is proved.

Before proving the second part of the lemma, let us compute the distance between P and Q. Let $x \in P$, there exist $-1 \le x_i \le 1$, $-1 \le \lambda \le 1$, $-1 \le y_i \le 1$,

$$x = \frac{c + e^{rA}c}{2} + \sum_{i=1}^{i=p} \frac{g_i + e^{rA}g_i}{2}x_i + \frac{c - e^{rA}c}{2}\lambda + \sum_{i=1}^{i=p}\frac{g_i - e^{rA}g_i}{2}y_i.$$

Let y be the point defined by $y = \frac{c+e^{rA}c}{2} + \sum_{i=1}^{i=p}\frac{g_i+e^{rA}g_i}{2}x_i$. We can check that y is an element of Q. Moreover,

$$\|x - y\| \le \|\frac{c - e^{rA}c}{2}\lambda + \sum_{i=1}^{i=p}\frac{g_i - e^{rA}g_i}{2}y_i\| \le \frac{e^{r\|A\|}-1}{2}\|c\lambda + \sum_{i=1}^{i=p} g_i y_i\|.$$

Therefore, $d_H(P,Q) \le \frac{e^{r\|A\|}-1}{2}\sup_{x\in Z}\|x\|$. Now let us remark that,

$$d_H(\mathcal{R}_{[0,r]}(Z), P + \square(\alpha_r + \beta_r)) \le d_H(\mathcal{R}_{[0,r]}(Z), Q + \square(\alpha_r + \beta_r)) + d_H(P,Q).$$

Thus, let $x \in Q + \square(\alpha_r + \beta_r)$, there exists $y \in Q$ such that $\|x - y\| \leq \alpha_r + \beta_r$. There exist $z \in Z$, $t \in [0, r]$ such that $y = z + \frac{t}{r}(e^{rA}z - z)$. Let $x' = e^{tA}z$, from equation (6), $\|x' - y\| \leq \alpha_r$. Moreover since $x' \in \mathcal{R}_{[0,r]}(Z)$ we have

$$d_H(\mathcal{R}_{[0,r]}(Z), Q + \square(\alpha_r + \beta_r)) \leq 2\alpha_r + \beta_r \leq e^{r\|A\|} r^2 \sup_{x \in Z} \|x\| + e^{r\|A\|} r\mu.$$

Proof of Theorem 1 (Adapted from [5])

From lemma 2, $\mathcal{R}_{[0,r]}(I) \subseteq Q_0$. Assume that $\mathcal{R}_{[(i-1)r,ir]}(I) \subseteq Q_{i-1}$, using lemma 1

$$\mathcal{R}_{[ir,(i+1)r]}(I) = \Phi_r(\mathcal{R}_{[(i-1)r,ir]}(I)) \subseteq \Phi_r(Q_{i-1}) \subseteq e^{rA} Q_{i-1} + \square(\beta_r) = Q_i.$$

Thus, by induction, the first part of the theorem is proved. Let us note $\delta_{i-1} = d_H(\mathcal{R}_{[(i-1)r,ir]}(I), Q_{i-1})$.

$$\begin{aligned}\delta_i &= d_H(\Phi_r(\mathcal{R}_{[(i-1)r,ir]}(I)), e^{rA} Q_{i-1} + \square(\beta_r)) \\ &\leq d_H(\Phi_r(\mathcal{R}_{[(i-1)r,ir]}(I)), \Phi_r(Q_{i-1})) + d_H(\Phi_r(Q_{i-1}), e^{rA} Q_{i-1} + \square(\beta_r)).\end{aligned}$$

From lemma 1, $d_H(\Phi_r(Q_{i-1}), e^{rA} Q_{i-1} + \square(\beta_r))$ is bounded by $\mu \|A\| e^{r\|A\|} r^2$. Furthermore, it is easy to show that

$$d_H(\Phi_r(\mathcal{R}_{[(i-1)r,ir]}(I)), \Phi_r(Q_{i-1})) \leq e^{r\|A\|} d_H(\mathcal{R}_{[(i-1)r,ir]}(I), Q_{i-1}).$$

Consequently, we have $\delta_i \leq e^{r\|A\|} \delta_{i-1} + \mu \|A\| e^{r\|A\|} r^2$. Therefore, for all $i \in \{0, \ldots, N-1\}$

$$\begin{aligned}\delta_i &\leq e^{ir\|A\|} \delta_0 + \mu \|A\| e^{r\|A\|} r^2 \sum_{k=0}^{k=i-1} e^{k\|A\|r} \\ &\leq e^{ir\|A\|} \delta_0 + \mu \|A\| e^{r\|A\|} r^2 \frac{e^{ir\|A\|} - 1}{e^{r\|A\|} - 1} \leq e^{\|A\|(T-r)} \delta_0 + \mu r e^{\|A\| T}.\end{aligned}$$

The use of lemma 2 ends the proof of the second part of the theorem.