Generating Polynomial Invariants for Hybrid Systems ⋆

Enric Rodríguez-Carbonell[1] and Ashish Tiwari[2]

[1] LSI Department, Technical University of Catalonia
Jordi Girona, 1-3 08034 Barcelona, Spain, erodri@lsi.upc.es
[2] SRI International, 333 Ravenswood Ave, Menlo Park, CA, U.S.A
Tel:+1.650.859.4774, Fax:+1.650.859.2844, tiwari@csl.sri.com

Abstract. We present a powerful computational method for automatically generating polynomial invariants of hybrid systems with linear continuous dynamics. When restricted to linear continuous dynamical systems, our method generates a set of polynomial equations (algebraic set) that is the best such over-approximation of the reach set, under the assumption that in every eigenvalue $a + ib$, the constants a and b are rational. The extension to hybrid systems is achieved using the abstract interpretation framework over the lattice defined by algebraic sets. Algebraic sets are represented using canonical Gröbner bases and the lattice operations are effectively computed via appropriate Gröbner basis manipulations.

1 Introduction

Verification of hybrid systems is a challenging problem. While testing can guarantee the correctness of a specific behavior of the system, verification attempts to provide correctness guarantee for *all* possible behaviors of the system. This extensive coverage is achieved, in most cases, by representing and manipulating *sets of states* of the system, rather than a single state. This jump from working with a single state, as in testing, to working with sets of states, as in verification, is also the main source of computational challenges in verification.

Arguably the most significant strides in the development of formal methods and verification technology were made in the form of developing effective representations for sets of states. The binary decision diagram representation provided a crucial breakthrough for hardware circuit verification, and region construction played a similar role for timed systems. In this paper, we argue that a canonical basis representation for algebraic sets provides an effective choice for a class of hybrid systems with linear continuous dynamics.

A good representation for a set of states is one that allows efficient computation of some basic operations. In the case of discrete state transition systems,

⋆ This research was partially supported by a Spanish FPU grant ref. AP2002-3693 and the projects Maverish (MCYT TIC2001-2476-C03-01) and LogicTools (TIN2004-03382) funded by the Spanish Ministry of Education and Science.

these operations are well understood. Depending on the exact verification procedure, some or all of the set union, set intersection, set complement, subset, and projection operators may be required [Hen]. In the case of hybrid systems, we additionally require that the representation behaves "nicely" along the continuous evolutions at different locations of the hybrid system.

This paper explores the representation of sets of states $Set \subseteq \mathbb{R}^n$ by the set of polynomials $P \in \mathbb{Q}[X_1, \ldots, X_n]$ that form the kernel of Set, that is, $P(\boldsymbol{s}) = 0$ for all $\boldsymbol{s} \in Set$. Such a set of polynomials has several nice algebraic properties. It is an *ideal* and has a finite basis representation. Furthermore, there is a canonical fully-reduced basis, called a Gröbner basis, which can be effectively computed (cf. ordered binary decision diagrams [Bry92]). The set union, set intersection, and set inclusion operators are efficiently computable on these canonical bases. The same is also true of the quantifier-elimination (projection) operator.

Using the above properties of the canonical ideal basis, we show that both continuous and discrete behaviors of hybrid systems can be processed. The main contributions of this paper are:
(i) We show that, for linear continuous dynamical systems where every eigenvalue $a+ib$ has *rational* real and imaginary parts, the *best* algebraic over-approximation of the reach set can be computed (Section 3). The proof of this result borrows some key insights from Lafferriere, Pappas and Yovine [LPY01], who use *semi-algebraic* sets and show that *exact* reach sets can be computed for more restricted classes of linear vector fields.
(ii) We show that the method for over-approximating reach sets for linear dynamical systems can be extended to hybrid systems using an abstract interpretation framework, thanks to the various nice computational properties of Gröbner bases (Section 4). We also present some experimental results obtained by using our method to generate polynomial invariants for hybrid systems (Section 5).

1.1 Related Work

Sankaranarayanan et al. [SSM04a] presented an approach for generating polynomial equational invariants for hybrid systems with more general (nonlinear) polynomial dynamics. However, their approach is based on *guessing* a template for the invariant and generating constraints that would guarantee that the guessed parametric polynomial equation is an *inductive* invariant. We restrict ourselves to linear dynamics, but our method is not based on guessing a template. Moreover, we provide certain completeness guarantees for our method. Each polynomial equation generated by Sankaranarayan et al. is required to be inductive; this need not be true in our case. On the other hand, any extension of our method to hybrid systems with more general continuous dynamics would require the use of heuristics, such as [TK04,SSM04a].

Region graphs suffice to compute exact reach sets for timed automata [AD94]. Polygonal sets have been used as representations for computing reachable states for linear hybrid automata [ACHH93]. For more complex continuous dynamics, various representations have been used for computing over-approximations of the reach sets, such as, union of convex polytopes [CK98], union of hyperrectangles [DM98], and ellipsoids [KV02]. Similar in the spirit of the result presented here, Kurzhanski and Varaiya [KV02] show that the best ellipsoidal overapproximation of the reach set for certain linear systems can be computed. We also note here that some of the above works use abstract interpretation ideas, most notably in the form of widening to accelerate reachability (or fixpoint) computation [HH95,DM98].

Exact reach sets for a class of linear vector fields were computed as semi-algebraic sets over state variables and special variables representing exponential or trigonometric functions [LPY01]. We contrast algebraic sets with semi-algebraic sets as a choice for representing sets of states. As mentioned above, the former admit unique canonical representations on which various set operations and quantifier-elimination operation can be efficiently performed. Algebraic sets are defined as the zeros of a finite set of polynomials equations. Semi-algebraic sets, on the other hand, are boolean combinations of sets defined by polynomial equations and inequalities. By definition, they are closed under boolean operations. However, there is no standard notion of canonical representation for semi-algebraic sets. There is a quantifier-elimination procedure, but it is quite complex, both in theory and practice.

2 Preliminaries: Ideals of Polynomials

Let $\mathbb{K}[X]$ denote the set of polynomials over the variables $X = \{x_1, \dots, x_n\}$ with coefficients in the field $\mathbb{K}$ ($\mathbb{K} = \mathbb{R}, \mathbb{Q}$). Given a set $S \subseteq \mathbb{K}^n$ of points, we are interested in those polynomials P that evaluate to 0 at S, that is, $P(\boldsymbol{s}) = 0, \forall \boldsymbol{s} \in S$. These polynomials form an *ideal*: an ideal is a set $I \subseteq \mathbb{K}[X]$ such that it includes 0, is closed under addition and if $P \in \mathbb{K}[X]$ and $Q \in I$, then $PQ \in I$.

Given a set of polynomials $B \subseteq \mathbb{K}[X]$, the *ideal generated by* B is

$$\langle B \rangle = \{ f \in \mathbb{K}[X] \mid \exists k \geq 1 \ f = \sum_{j=1}^{k} P_j Q_j \text{ with } P_j \in \mathbb{K}[X], Q_j \in B \}.$$

For an ideal I, a set of polynomials B such that $I = \langle B \rangle$ is called a *basis* of I. By Hilbert's basis theorem, all ideals of polynomials admit a *finite* basis. Thus, any ideal is associated to a finite system of polynomial equalities: the ideal $I = \langle P_1(X), ..., P_k(X) \rangle$ corresponds naturally to the system $\{P_1(X) = 0,$ ..., $P_k(X) = 0\}$. The solutions to this system are the common zeroes of all the polynomials in I; this set of points, denoted by $\mathbf{V}(I) = \{\boldsymbol{s} \in \mathbb{K}^n \,|\, P(\boldsymbol{s}) = 0 \ \forall P \in I\}$, is called the *variety* of I (over $\mathbb{K}^n$). A variety is also called an *algebraic set.*

For instance, the ideal $\langle x(x^2 + y^2 - 1), y(x^2 + y^2 - 1) \rangle$ is associated to the system $\{x(x^2 + y^2 - 1) = 0,\ y(x^2 + y^2 - 1) = 0\}$. Its solution, which defines the variety $\mathbf{V}(\langle x(x^2 + y^2 - 1)\ , y(x^2 + y^2 - 1) \rangle)$, is the union of the circle $x^2 + y^2 = 1$ and the origin. Notice that this set, unlike convex polyhedra [HPR94,CK98], is not convex or even connected.

Reciprocally, given a set of points $S \subseteq \mathbb{K}^n$, the polynomials vanishing on this set form the ideal $\mathbf{I}(S) = \{P \in \mathbb{K}[X] | \ P(\boldsymbol{s}) = 0 \ \forall \boldsymbol{s} \in S\}$, called the *ideal of* S. Notice that, for arbitrary ideals, the inclusion $I \subseteq \mathbf{IV}(I)^1$ may be strict: the variety of the ideal of all multiples of x^2 is just the origin, $\mathbf{V}(\langle x^2 \rangle) = \{0\}$; but $\mathbf{I}(\{0\}) = \langle x \rangle$, and $x \notin \langle x^2 \rangle$. We are interested in the ideals for which the equality $\mathbf{IV}(I) = I$ holds; these ideals are *complete* in the sense that they include *all* polynomials that evaluate to 0 at the points of the variety $\mathbf{V}(I)$ they represent. Since any ideal I satisfying $\mathbf{IV}(I) = I$ is the ideal of the variety $\mathbf{V}(I)$, such an ideal is called an *ideal of variety.*

3 Linear Systems

A *linear (continuous dynamical) system* CS is a tuple $(X, \mathit{Init}, A, \boldsymbol{b})$ where $X = \{x_1, ..., x_n\}$ is a finite set of variables interpreted over the reals $\mathbb{R}$, $\mathbf{X} = \mathbb{R}^n$ is the set of all valuations of the variables X, $\mathit{Init} \subseteq \mathbf{X}$ is the set of initial states, and $A \in \mathbb{Q}^{n \times n}$ and $\boldsymbol{b} \in \mathbb{Q}^{n \times 1}$ are the matrices that constrain the dynamics of CS by the differential equation $\dot{\boldsymbol{x}} = A\boldsymbol{x} + \boldsymbol{b}$. Since interest is in computational feasibility, the matrices A and $\boldsymbol{b}$ are assumed to contain rational entries.

The semantics, $[[CS]]$, of a linear system $CS = (X, \mathit{Init}, A, \boldsymbol{b})$ over an interval $I = [t_0, t_1] \subseteq \mathbb{R}$ is a collection of mappings $\boldsymbol{x} : I \mapsto \mathbf{X}$ satisfying (i) the initial condition: $\boldsymbol{x}(t_0) \in \mathit{Init}$, and (ii) the continuous dynamics: for all $t \in [t_0, t_1]$, $\dot{\boldsymbol{x}}(t) = A\boldsymbol{x}(t) + \boldsymbol{b}$. In case the interval I is left unspecified, it is assumed to be the interval $[0, \infty)$.

We say that a state $\boldsymbol{s} \in \mathbf{X}$ is *reachable* in a continuous dynamical system CS if there exists a function $\boldsymbol{x} \in [[CS]]$ such that $\boldsymbol{s} = \boldsymbol{x}(t)$ for some $t \in I$. The set, $\mathit{Reach}(CS)$, is defined as the set of all reachable states of the system CS.

The problem of computing the exact reachability set $\mathit{Reach}(CS)$ for a given dynamical system CS is intractable in general. However, for purposes of verification of safety properties, it often suffices to compute an *over-approximation* (or superset) of the reachable set of states—if the over-approximation does not intersect the set of bad states, then the original system will never reach a bad state. An over-approximation of the reachable states is also called an *invariant* of the system. The most precise invariant of a system is its exact reach set.

Lafferriere, Pappas and Yovine showed that the exact reach set can be computed for a subclass of linear continuous dynamical systems [LPY01]. Subsequently, it was shown that invariants (that is, over-approximations) could be effectively constructed for more general classes of linear systems [Tiw03]. We show here that the most precise *equational invariant* for a class of linear systems (that allows for more complex dynamics than the one in [LPY01]) can be computed.

Assume that the eigenvalues of A are of the form $a + bi$, where $a, b \in \mathbb{Q}$ and $i^2 = -1$. We do *not* assume that A is diagonalizable. The solution to the system

[1] We write $\mathbf{IV}$ instead of $\mathbf{I} \circ \mathbf{V}$ to denote the composition of $\mathbf{I}$ and $\mathbf{V}$.

of differential equations $\dot{\boldsymbol{x}} = A\boldsymbol{x} + \boldsymbol{b}$ is

$$\Phi(\boldsymbol{s^*}, t) = e^{At}\boldsymbol{s^*} + e^{At}(\int_0^t e^{-A\tau} d\tau)\ \boldsymbol{b}\ , \boldsymbol{s^*} \in \mathit{Init} \tag{1}$$

where Φ is the flow of the vector field. It can be easily proved that both e^{At} and $\int_0^t e^{-A\tau} d\tau$ can be written as sums of terms of the form $ct^k e^{\pm at}\cos(bt)$, $ct^k e^{\pm at}\sin(bt)$, where $c \in \mathbb{Q}$, $k \in \mathbb{N}$ and the complex numbers $\lambda = a + bi$ are the eigenvalues of the matrix A.

The set of reachable states of CS is

$$\mathit{Reach}(CS) = \{\boldsymbol{s} \in \mathbb{R}^n : \exists \boldsymbol{s^*}, t.\ (t \geq 0\ \wedge\ \boldsymbol{s^*} \in \mathit{Init}\ \wedge\ s = \Phi(\boldsymbol{s^*}, t))\} \tag{2}$$

We can express the solution $\Phi(\boldsymbol{s^*}, t)$ given in Equation 1 in terms of polynomials using up to four auxiliary variables u, v, w, z. Specifically, since we assume that all eigenvalues of A are of the form $a + bi$ with $a, b \in \mathbb{Q}$, we can find positive rational numbers p, q such that, for any eigenvalue $\lambda = a + bi$ of A, there exist *integers* c_λ, d_λ such that $c_\lambda = a/p$ and $d_\lambda = b/q$. Now we just need to replace e^{pt} by u, e^{-pt} by v, $\cos(qt)$ by w and $\sin(qt)$ by z: for any eigenvalue $\lambda = a + bi$, we replace e^{at} by $u^{|c_\lambda|}$ or $v^{|c_\lambda|}$ depending on whether $a > 0$ or $a < 0$ respectively; $\cos(bt)$ and $\sin(bt)$ can be similarly expressed in terms of w and z. Therefore, we can express the flow Φ as a polynomial over the initial conditions and the dummy variables t, u, v, w, z. The reach set from Equation 2 can now be written as

$$\begin{aligned} \exists \boldsymbol{s^*}, t, u, v, w, z\ .\ (t \geq 0\ \wedge\ \boldsymbol{s^*} \in \mathit{Init}\ \wedge\ s = \Phi(\boldsymbol{s^*}, t, u, v, w, z)\ \wedge \\ u = e^{pt}\ \wedge\ v = e^{-pt}\ \wedge\ w = \cos(qt)\ \wedge\ z = \sin(qt)) \end{aligned} \tag{3}$$

The exponentials and the trigonometric functions are eliminated by introducing new equations $uv = 1$ and $w^2 + z^2 = 1$ that capture the dependencies between e^{pt}, e^{-pt}, $\cos(qt)$ and $\sin(qt)$. Clearly, the resulting formula, given below, represents an invariant of CS.

$$\begin{aligned} \exists \boldsymbol{s^*}, t, u, v, w, z\ .\ (t \geq 0\ \wedge\ u \geq 1\ \wedge\ \boldsymbol{s^*} \in \mathit{Init}\ \wedge\ s = \Phi(\boldsymbol{s^*}, t, u, v, w, z)\ \wedge \\ uv = 1\ \wedge\ w^2 + z^2 = 1) \end{aligned} \tag{4}$$

Using quantifier elimination for reals, this method gives a semi-algebraic invariant for the linear system CS. Unfortunately, the formula above does not capture all semi-algebraic relationships that exist between t, u, v, w and z.

One of the main observations of this paper is that the two equations $uv = 1$ and $w^2 + z^2 = 1$ are sufficient to capture *all algebraic invariants* of CS. Furthermore, to compute the algebraic invariants, the expensive step that involves doing quantifier elimination over the reals can be replaced by a Gröbner basis [CLO96] computation step, which is simpler and often more efficient in practice. Since we use Gröbner bases to eliminate variables, we need to employ an elimination term ordering in which the auxiliary variables are the biggest. In summary, the method to compute the strongest algebraic invariants of CS is to use Gröbner bases to eliminate the quantified variables in Equation 4.

The main result of the paper is that, if the initial conditions are described by means of an ideal of variety, we obtain *all* polynomials that evaluate to 0 at the exact reachability set of CS.

Theorem 1. *Let $CS = (X, \mathbf{V}(I^*), A, \boldsymbol{b})$ be a linear system, where $I^* \subseteq \mathbb{Q}[X^*]$ is the ideal of variety of initial states. Let $P_1, ..., P_n \in \mathbb{Q}[X^*, t, u, v, w, z]$ be the polynomials approximating the flow Φ defined above. Then,*

$$\mathbf{I}(\mathit{Reach}(CS)) = \langle I^*, -x_1 + P_1, \ldots, -x_n + P_n, uv - 1, w^2 + z^2 - 1\rangle \cap \mathbb{R}[X]$$

Proof. The $\supseteq$ inclusion is obvious. For the $\subseteq$ inclusion, take an arbitrary polynomial $q \in \mathbf{I}(\mathit{Reach}(CS))$. Normalize the polynomial q using the following rewrite rules[2] to get a new polynomial r:

$$x_1 \to P_1, \ldots, x_n \to P_n,\ uv \to 1,\ w^2 \to -z^2 + 1$$

Our goal is to prove that $r \in \langle I^*\rangle$ (as an ideal in $\mathbb{R}[X, X^*, t, u, v, w, z]$). Since we have eliminated all occurrences of uv, w^2 and x_i, the polynomial r must be of the form

$$\sum_{l,m,n\geq 0} a_{lmn}(X^*)t^l u^m z^n + b_{lmn}(X^*)t^l u^m w z^n + c_{lmn}(X^*)t^l v^m z^n + d_{lmn}(X^*)t^l v^m w z^n$$

with a finite number of non-vanishing terms. We need to prove that the polynomials $a_{lmn}(X^*)$, $b_{lmn}(X^*)$, $c_{lmn}(X^*)$, and $d_{lmn}(X^*)$ are in $\mathbf{IV}(I^*) = I^*$. So, we will prove that $\forall \boldsymbol{s^*} \in \mathbf{V}(I^*)$, $a_{lmn}(\boldsymbol{s^*}) = b_{lmn}(\boldsymbol{s^*}) = c_{lmn}(\boldsymbol{s^*}) = d_{lmn}(\boldsymbol{s^*}) = 0$.

Fix $\boldsymbol{s^*} \in \mathbf{V}(I^*)$. Under the substitution $x_i \mapsto P_i, u \mapsto e^{pt}, v \mapsto e^{-pt}, w \mapsto \cos(qt), z \mapsto \sin(qt), X^* \mapsto \boldsymbol{s^*}$, the polynomial q evaluates to 0 (for all $t \geq 0$), and so do the polynomials $uv - 1, w^2 + z^2 - 1, -x_i + P_i$. Therefore, we have that for all $t \geq 0$, $R(t) := r(\boldsymbol{s^*}, t, e^{pt}, e^{-pt}, \cos(qt), \sin(qt)) = 0$, or equivalently

$$\sum_{l,m\geq 0} t^l e^{mpt}(\sum_{n\geq 0} a_{lmn}(\boldsymbol{s^*})\sin^n(qt) + b_{lmn}(\boldsymbol{s^*})\sin^n(qt)\cos(qt)) +$$
$$t^l e^{-mpt}(\sum_{n\geq 0} c_{lmn}(\boldsymbol{s^*})\sin^n(qt) + d_{lmn}(\boldsymbol{s^*})\sin^n(qt)\cos(qt)) = 0$$

Since this function evaluates to 0 for *all* $t \geq 0$, we claim without proof that $a_{lmn}(\boldsymbol{s^*}) = b_{lmn}(\boldsymbol{s^*}) = c_{lmn}(\boldsymbol{s^*}) = d_{lmn}(\boldsymbol{s^*}) = 0$. This completes the proof. □

Example 1. Consider the following system of differential equations, which describes the dynamics of a charged particle under the influence of a magnetic

[2] Simplification of q by a rewrite rule $l \to r$ simply means that you replace l by r in q. Experts in Gröbner bases will notice that we are using the term ordering $\mathbf{lex}(X > u > v > w > z > t > X^*)$.

field:

$$\begin{pmatrix} \dot{x} \\ \dot{y} \\ \dot{v_x} \\ \dot{v_y} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1/2 \\ 0 & 0 & 1/2 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ v_x \\ v_y \end{pmatrix}$$

The solution is given by

$$\begin{cases} x = x^* + 2\sin(t/2)\, v_x^* + (2\cos(t/2) - 2)\, v_y^* & v_x = cos(t/2)\, v_x^* - sin(t/2)\, v_y^* \\ y = y^* + (-2\cos(t/2) + 2)\, v_x^* + 2\sin(t/2)\, v_y^* & v_y = sin(t/2)\, v_x^* + cos(t/2)\, v_y^* \end{cases}$$

where x^*, y^*, v_x^*, v_y^* stand for the initial values. In this case the eigenvalues of the system matrix are 0, $i/2$ and $-i/2$, which is consistent with the fact that the non-algebraic terms in the solution are $\cos(t/2)$, $\sin(t/2)$. By introducing the variables w and z to replace $\cos(t/2)$ and $\sin(t/2)$ respectively, we can rewrite the solution as follows (there are no exponential terms in this case):

$$\begin{cases} x = x^* + 2zv_x^* + (2w - 2)v_y^* & v_x = wv_x^* - zv_y^* \\ y = y^* + (-2w + 2)\, v_x^* + 2zv_y^* & v_y = zv_x^* + wv_y^* \end{cases}$$

Now assume that the initial conditions satisfy $v_x^* = 2$, $v_y^* = -2$. Therefore we have to eliminate x^*, y^*, v_x^*, v_y^*, w, z from the ideal

$$\langle v_x^* - 2, v_y^* + 2, -x + x^* + 2zv_x^* + (2w - 2)v_y^*, -y + y^* + (-2w + 2)\, v_x^* + 2zv_y^*,$$
$$-v_x + wv_x^* - zv_y^*, -v_y + zv_x^* + wv_y^*, w^2 + z^2 - 1\rangle$$

The elimination of the auxiliary variables yields the ideal $\langle v_x^2 + v_y^2 - 8\rangle$, which corresponds to the law of conservation of energy. □

The method for generating the most precise equational (algebraic) invariants of linear systems can be extended to handle state invariants that are specified as polynomial equations. Before eliminating the quantified variables from Equation 4, we add all the equations representing any state invariant that may be true.

It is difficult to generalize the method to compute the best semi-algebraic invariant. Whereas the two equations $uv = 1$ and $w^2 + z^2 = 1$ capture all algebraic relationships between the functions $e^{pt}, e^{-pt}, \sin(qt)$ and $\cos(qt)$, there is no *finite* set (basis) of inequalities that captures all the semi-algebraic relationships between these functions. This also partly explains why the decidability results [LPY99,LPY01] are not easy to generalize.

3.1 Generalization to Arbitrary Eigenvalues

The ideas proposed above to handle exponential and trigonometric terms can be generalized to arbitrary eigenvalues as follows.

Let $\mathcal{L}$ be the set of all eigenvalues of the matrix A. First, let us deal with the exponential terms. To that end, we define $\mathcal{R} = \{\pm\mathrm{Re}(\lambda) \mid \lambda \in \mathcal{L}\} \setminus \{0\}$. Since $\mathcal{R}$ is finite, we can obtain a finite basis $\mathcal{B} = \{p_1, ..., p_k\}$ of the $\mathbb{Q}$-vector space generated by $\mathcal{R}$. By definition, this set has the properties that:

1. $\forall a \in \mathcal{R}$, $\exists c_1^a, ..., c_k^a \in \mathbb{Q}$ such that $a = \sum_{i=1}^{k} c_i^a p_i$.
   ($\mathcal{B}$ is a system of generators)
2. $\forall c_1, ..., c_k \in \mathbb{Q}$ such that $\sum_{i=1}^{k} c_i p_i = 0$, $c_1 = \cdots = c_k = 0$.
   ($\mathcal{B}$ is $\mathbb{Q}$-linearly independent)

Further, by multiplying the elements in $\mathcal{B}$ by appropiate correction factors, we can ensure that the coefficients c_i^a are *integers*, i.e. $\forall a \in \mathcal{R}$, $\exists c_1^a, ..., c_k^a \in \mathbb{Z}$ such that $a = \sum_{i=1}^{k} c_i^a p_i$. By introducing the auxiliary variables $u_i = e^{p_i t}, v_i = e^{-p_i t}$:

$$e^{at} = e^{\sum_{i=1}^{k} c_i^a p_i t} = \prod_{i=1}^{k} e^{c_i^a p_i t} = \prod_{i=1}^{k} \begin{cases} u_i^{|c_i^a|} & \text{if } \operatorname{sign}(c_i^a) = 1 \\ v_i^{|c_i^a|} & \text{if } \operatorname{sign}(c_i^a) = -1 \end{cases}$$

So we can substitute the exponentials by means of the auxiliary variables.

Example 2. Let us consider that $\mathcal{L} = \{\lambda_1, \lambda_2, \lambda_3, \lambda_4\} = \{1+\sqrt{2}, 1-\sqrt{2}, 1/2, 1/3\}$. Taking $\mathcal{B} = \{p_1, p_2\} = \{1 + \sqrt{2}, 1/6\}$ as a basis, all coefficients are integers: $\lambda_1 = p_1$, $\lambda_2 = -p_1 + 12p_2$, $\lambda_3 = 3p_2$, $\lambda_4 = 2p_2$. So, if $u_1 = e^{(1+\sqrt{2})t}, v_1 = e^{-(1+\sqrt{2})t}, u_2 = e^{(1/6)t}, v_2 = e^{-(1/6)t}$, then for instance $e^{(1-\sqrt{2})t} = v_1 u_2^{12}$. □

As regards trigonometric terms, the same ideas apply: we define $\mathcal{I} = \{\operatorname{Im}(\lambda) \mid \lambda \in \mathcal{L}\} \setminus \{0\}$ and introduce $2l$ auxiliary variables w_j, z_j standing for $\cos(q_j t)$, $\sin(q_j t)$ for $1 \leq j \leq l$ for certain $\mathbb{Q}$-linearly independent $q_1, ..., q_l \in \mathbb{R}$.

The following theorem (which we claim without proof) is an extension of Theorem 1:

Theorem 2. *Let $CS = (X, \mathbf{V}(I^*), A, \boldsymbol{b})$ be a linear system, where $I^* \subseteq \mathbb{Q}[X^*]$ is the ideal of variety of initial states. Let $P_1, ..., P_n \in \mathbb{Q}[X^*, t, u_1, v_1, ..., u_k, v_k, w_1, z_1, ..., w_l, z_l]$ be the polynomials approximating the flow Φ. Then,*

$$\begin{aligned}\mathbf{I}(\mathit{Reach}(CS)) = \langle I^*, -x_1 + P_1, \ldots, -x_n + P_n, \\ u_1 v_1 - 1, ..., u_k v_k - 1, w_1^2 + z_1^2 - 1, ..., w_l^2 + z_l^2 - 1\rangle \cap \mathbb{R}[X]\end{aligned}$$

4 Hybrid Systems

In this section we extend the technique for generating algebraic invariants to hybrid systems using abstract interpretation [CC77]. At each location, we restrict ourselves to linear continuous dynamics.

A *hybrid system* $HS = (\mathcal{L}, X, \mathcal{T}, (Init)_{\ell \in \mathcal{L}}, (A)_{\ell \in \mathcal{L}}, (\boldsymbol{b})_{\ell \in \mathcal{L}})$ consists of a finite set $\mathcal{L}$ of *locations*; a finite set of continuous dynamical systems $(X, Init_\ell, A_\ell, \boldsymbol{b}_\ell)$, one associated with each location $\ell \in \mathcal{L}$; and a finite set $\mathcal{T} \subset \mathcal{L} \times \mathcal{L} \times 2^{\mathbf{X}} \times (\mathbf{X} \rightarrow \mathbf{X})$ of discrete *transitions*. A discrete transition $\tau = (\ell, \ell', \gamma, \alpha) \in \mathcal{T}$ consists of a *source location* $\ell \in \mathcal{L}$, a *target location* $\ell' \in \mathcal{L}$, a *guard* γ which is a boolean function of the variables X, and an *action* α which is a multiple assignment of the variables. A *state* of the system HS is given by a location $\ell \in \mathcal{L}$ and a valuation $\boldsymbol{s} \in \mathbf{X} = \mathbb{R}^n$ of the variables over the real numbers.

The semantics, $[[HS]]$, of a hybrid system HS is a collection of infinite sequences of states $(\ell, \boldsymbol{s}) \in \mathcal{L} \times \mathbf{X}$ of the form $(\ell_0, \boldsymbol{s_0}), (\ell_1, \boldsymbol{s_1}), (\ell_2, \boldsymbol{s_2}), \ldots$ such that $\boldsymbol{s_0} \in \mathit{Init}_{\ell_0}$ specifies an *initial state*, and for each pair of consecutive states $(\ell_i, \boldsymbol{s_i})$, $(\ell_{i+1}, \boldsymbol{s_{i+1}})$ one of the two *transition conditions* holds:
- *discrete transition*: there exists a transition $\tau = (\ell_i, \ell_{i+1}, \gamma, \alpha) \in \mathcal{T}$ which is enabled, i.e. $\gamma(\boldsymbol{s_i}) = \mathit{true}$, and such that $\boldsymbol{s_{i+1}} = \alpha(\boldsymbol{s_i})$.
- *continuous transition*: the control location does not change, in other words $\ell_i = \ell_{i+1} = \ell$; and there is a trajectory going from $\boldsymbol{s_i}$ to $\boldsymbol{s_{i+1}}$ along the flow determined by $A_\ell, \boldsymbol{b_\ell}$, i.e. there exist a time interval $\delta \geq 0$ and a differentiable function $\boldsymbol{x} : [0, \delta] \to \mathbf{X}$ such that $\boldsymbol{x}(0) = \boldsymbol{s_i}$, $\boldsymbol{x}(\delta) = \boldsymbol{s_{i+1}}$ and $\dot{\boldsymbol{x}}(t) = A_\ell \boldsymbol{x} + \boldsymbol{b_\ell}$ (and the state invariant, if any, holds).

A state $(\ell, \boldsymbol{s})$ is *reachable* if there exists a sequence in $[[HS]]$ where it appears. The set of all reachable states of a hybrid system HS is denoted by $\mathit{Reach}(HS)$.

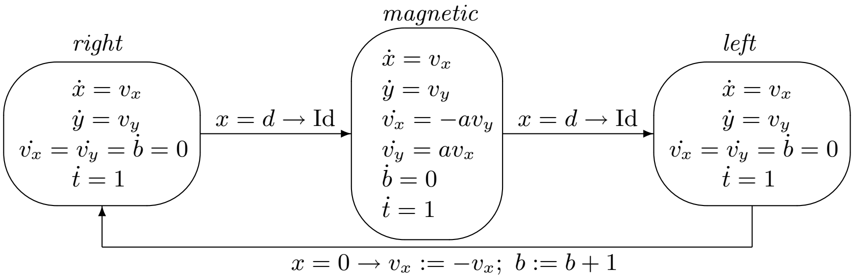

Fig. 1. Dynamics of a charged particle

Example 3. The hybrid system in Figure 1, taken from [SSM04b], models the position (x, y) and the velocity (v_x, v_y) of a charged particle on a plane with a reflecting barrier at $x = 0$ and a magnetic field perpendicular to the plane in the region $x \geq d$ (where $d \geq 0$ is a parameter of the system). The variable b counts the number of times the particle has collided against the reflecting barrier, and t is a clock that measures the total time elapsed.

The hybrid system has three locations: in locations *left* and *right*, the particle is moving freely under no external force, either toward or away from the barrier, while in location *magnetic* it is moving under the effect of the magnetic field. The three discrete transitions model the movement of the particle in and out of the magnetic field and its collision with the barrier. In our analysis, we assume that initially the particle is moving *right* with $v_x = 2$, $v_y = -2$ and $x = y = t = b = 0$; also, the parameters d and a are set to 2 and 1/2 respectively. □

4.1 Reachable States as Fixpoints

Let us denote by $\mathit{Reach} = \mathit{Reach}(HS)$ the set of all reachable states of a hybrid system HS. Given a location ℓ, we also write Reach_ℓ to represent the set of all reachable states at location ℓ, i.e. $\mathit{Reach}_\ell = \{\boldsymbol{s} \mid (\ell, \boldsymbol{s}) \in \mathit{Reach}\}$.

We first characterize the (tuple of) reachable states $(\mathit{Reach}_\ell)_{\ell\in\mathcal{L}}$ using a system of fixpoint equations. Consider a discrete transition $\tau = (\ell, \ell', \gamma, \alpha)$. The states at location ℓ where transition τ is enabled are given by $\mathit{Reach}_\ell \cap \gamma$. After firing the transition, the new states reached are given by $\alpha(\mathit{Reach}_\ell \cap \gamma)$, where α represents the mapping that updates the values of the variables. The set of states in which location ℓ' is entered is obtained by summing up over all discrete transitions that lead to ℓ':

$$\mathit{Init}_{\ell'} \cup (\bigcup_{(\ell,\ell',\gamma,\alpha)\in\mathcal{T}} \alpha(\mathit{Reach}_\ell \cap \gamma)) \,.$$

The above states provide the initial conditions for the continuous evolution at ℓ'. Now, $\mathit{Reach}_{\ell'}$ is obtained thus:

$$\mathit{Reach}_{\ell'} = \bigcup_{t\geq 0} \mathit{\Phi}_{\ell'}(\mathit{Init}_{\ell'} \cup (\bigcup_{(\ell,\ell',\gamma,\alpha)\in\mathcal{T}} \alpha(\mathit{Reach}_\ell \cap \gamma)), t) \,. \qquad (5)$$

The above system of equations defines $(\mathit{Reach})_{\ell\in\mathcal{L}}$ in terms of itself. The least fixpoint of this system of equations (with respect to the inclusion $\subseteq$ ordering) is the *exact* set of reachable states of HS. However, any fixpoint (not necessarily the least) will give an over-approximation of the exact reach set.

The ability to compute a fixpoint of the above equations depends on the choice of the representation for sets of states. Some choices are convex polyhedra [CK98], algebraic sets, semi-algebraic sets [LPY01], and ellipsoidal sets [KV02]. We have used algebraic sets in Section 3 to represent sets reachable under continuous flow. Using the results from Section 3, in the next subsections we will show how algebraic solutions of the Fixpoint Equation 5 can be computed. The general framework (originally defined for discrete transition systems) is called *abstract interpretation* [CC77].

4.2 Abstract Interpretation

Abstract interpretation [CC77] is a general framework for discovering invariant properties for a given discrete transition system. It works by solving a fixpoint equation $X = F(X)$ (which determines the reachable sets for that system) over an *abstract domain*. The abstract domain is defined by the representation used for specifying sets of states. The application of abstract interpretation involves:

1. *Choosing an abstract domain* A: Each element in the abstract domain represents a set of states. The original fixpoint equation $X = F(X)$ (defined over arbitrary sets of states X) is transformed into a fixpoint equation $Y = G(Y)$ over the sets of states Y *defined* by the abstract domain.
2. *Computing a solution of the fixpoint equation $Y = G(Y)$ over the abstract domain iteratively*: A solution of the equation $Y = G(Y)$ is obtained by computing a fixpoint of the recurrence $Y_0 = \bot$ (the least element of the abstract domain), $Y_{k+1} = G(Y_k)$. This recurrence may not necessarily converge in a finite number of steps; in this case the termination is forced by means of the application of a *widening* operator $\nabla : A \times A \to A$, at the cost of further over-approximation. Such an operator must satisfy:

- $\forall Y_1, Y_2 \in A$, $Y_1 \subseteq Y_1 \nabla Y_2$ and $Y_2 \subseteq Y_1 \nabla Y_2$.
- For any increasing chain $Y_0 \subseteq Y_1 \subseteq \cdots$, the new increasing chain defined by $Y'_0 = Y_0$, $Y'_{k+1} = Y'_k \nabla Y_{k+1}$ is not strictly increasing (that is, it finitely converges).

Under these hypotheses, the last element of the finite sequence $Y'_0, Y'_1, Y'_2, \ldots$ yields a solution of the fixpoint equation.

4.3 Operations with Ideals of Variety

We now show that the abstract domain of algebraic sets, represented as ideals of variety, can be used to compute polynomial invariants for hybrid systems. In Section 2 we presented this domain, and Section 3 showed how to handle continuous evolution (that is, the Φ function in the Fixpoint Equation 5). We now show how the rest of the operators used in Equation 5, viz. the assignment transformation α, the set union $\cup$ and the set intersection $\cap$, can be effectively computed over our choice of abstract domain. We will also present a widening operator to guarantee termination.

Specifically, we use the following operations on algebraic sets (represented as ideals) to abstract the corresponding operations on (arbitrary) sets, see [RCK04]:

Assignment Transformation → Elimination of Variables. Given an ideal of variety $I = \langle P_1(X), ..., P_k(X)\rangle$ and a multiple (polynomial) assignment $(x_1, \ldots, x_n)$ $:= (\alpha_1(X), \ldots, \alpha_n(X))$, we introduce auxiliary variables $\bar{X} = \{\bar{x}_1, \ldots, \bar{x}_n\}$, to denote the values of the variables *before* the assignment. Then the relationship between the values before and after the assignment is described by the ideal

$$\langle P_1(\bar{X}), \ldots, P_k(\bar{X}), x_1 - \alpha_1(\bar{X}), \ldots, x_n - \alpha_n(\bar{X})\rangle.$$

The output ideal of variety can be obtained by eliminating the auxiliary variables $\bar{X}$ in the ideal above by means of well-known elimination techniques based on Gröbner bases [CLO96].

Union of States → Intersection of Ideals. Given two ideals of variety I and J, the union of the states represented by I and J is represented by the ideal $\mathbf{I}(\mathbf{V}(I) \cup \mathbf{V}(J))$, which is equal to $I \cap J$ by duality. Therefore, the output ideal of variety is the intersection ideal $I \cap J$.

Intersection of States → Sum and Quotient of Ideals. Given two ideals of variety $I = \langle P_1, ..., P_k\rangle$ and $J = \langle Q_1, ..., Q_l\rangle$, we distinguish two cases:

- We want to represent $\mathbf{V}(I) \cap \mathbf{V}(J)$ (this is the case when guards have *polynomial equalities* like $x = 0$). The *sum* of ideals $I + J = \langle P_1, ..., P_k, Q_1, ..., Q_l\rangle$, which is generated by the union of the bases, has the property that $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$. However, $I + J$ may not be an ideal of variety; therefore we have to compute its closure $\mathbf{IV}(I + J)$[3].

[3] If we take the complex numbers $\mathbb{C}$ as the field for the coefficients instead of $\mathbb{R}$, by Hilbert's Nullstellensatz $\mathbf{IV} = \mathit{Rad}$, the radical operator, which can be effectively computed.

– We want to represent $\mathbf{V}(I) \cap (\mathbb{K}^n \setminus \mathbf{V}(J)) = \mathbf{V}(I) \setminus \mathbf{V}(J)$ (this is the case when guards have *polynomial disequalities* like $x \neq 0$). The *quotient* $I : J$ of ideals satisfies that $I : J = \mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J))$, i.e. it is the maximal set of polynomials that evaluate to 0 at $\mathbf{V}(I) \setminus \mathbf{V}(J)$. Thus we take $I : J$ as the output ideal of variety.

Widening Operator. Given two ideals of variety I and J, we are interested in *under*-approximating the ideal $I \cap J$ so that we can guarantee termination of the fixpoint computation. One way to achieve this is to restrict $I \cap J$ to polynomials that have degree less or equal than a prefixed degree bound d. As the ideal generated by these polynomials may not be an ideal of variety, the closure operator $\mathbf{IV}$ must be applied. Formally, given two ideals of variety I, J and a degree bound d, the widening is defined as:

$$I \nabla_d J = \mathbf{IV}(\{P \in GB(I \cap J, \succ) \mid \text{degree}(P) \leq d\}),$$

where $GB(K, \succ)$ stands for a Gröbner basis of an ideal K with respect to the graded term ordering[4] $\succ$. We are experimenting with other widening operators that would allow the generalization of Theorem 1 to hybrid systems.

It is well-known in computational algebraic geometry that canonical representation for $I \cap J$, $I \cup J$, $I : J$, and elimination ideals can be effectively computed from the corresponding representations for I and J.

Example 4. In the hybrid system model of the charged particle, let us denote by I_{right}, $I_{magnetic}$ and I_{left} the ideals of variety corresponding to the states *right*, *magnetic* and *left* respectively. As the initial state is *right* with $v_x = 2$, $v_y = -2$, $x = y = b = t = 0$, we get the following system of fixpoint equations:

$$\begin{cases} I_{right} = \phi_{right}(\langle v_x - 2, v_y + 2, x, y, t, b\rangle \cap \alpha(\mathbf{IV}(I_{left} + \langle x \rangle))) \\ I_{magnetic} = \phi_{magnetic}(\mathbf{IV}(I_{right} + \langle x - d\rangle)) \\ I_{left} = \phi_{left}(\mathbf{IV}(I_{magnetic} + \langle x - d\rangle)) \end{cases}$$

where α transforms (v_x, b) into $(-v_x, b+1)$ and leaves the rest of the variables unchanged, and the ϕ's are the mappings abstracting the flows in continuous transitions, taking as input an ideal of initial conditions and returning an ideal of invariant polynomials (computed using the technique described in Section 3).

We approximate the fixpoint of this equation by using the widening operator ∇_2. We get the following invariants:

$$I_{right} = \langle v_y + 2, v_x^2 - 4\rangle \qquad I_{left} = \langle v_y + 2, v_x^2 - 4\rangle$$
$$I_{magnetic} = \langle x - 2v_y - 4 - d, v_x^2 + v_y^2 - 8\rangle$$

The reason why we get $v_x^2 = 4$ both at *right* and *left* is that our hybrid system allows undesired behaviors, such as the particle in mode *right* making a transition to *magnetic* and then instantly moving again to *left* with no time elapse.

[4] Gröbner bases and graded term orderings are used in this definition because they allow us to prove that, when employing this widening operator, the fixpoint computation yields all the polynomial invariants of degree $\leq d$, see [CLO96,RCK04].

However, using the implicit invariants $v_x \geq 0$ at *right* and $v_x \leq 0$ at *left*, we deduce that $v_x = 2$ at *right* and $v_x = -2$ at *left*. Now we can get a more precise result by adding these invariants to the guards. After this second computation, finally we obtain

$$\begin{cases} I_{right} = \langle v_y + 2, v_x - 2, 2db - 8b + y + x \rangle \\ I_{magnetic} = \langle x - 2v_y - 4 - d, v_x^2 + v_y^2 - 8, 2v_x + y + 2db - 8b - 4 + d \rangle \\ I_{left} = \langle v_y + 2, v_x + 2, 2db - 8b + y - 8 - x \rangle \end{cases}$$

5 Examples

In this section we apply our method for generating invariant polynomial equations to some hybrid systems taken from the literature. As an optimization, we did not compute the closure **IV** always; nonetheless, the obtained invariants sufficed for proving the properties of interest. We have implemented the techniques presented here in the algebraic geometry tool Macaulay 2 [GS] using a PC running Linux with a 2.5 GHz. processor and 512 MB of memory.

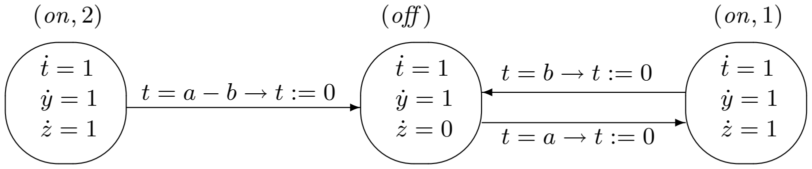

Fig. 2. Hybrid system for a thermostat

Thermostat. Figure 2 shows a hybrid system, taken from [HHWT98], modeling a thermostat. The system has three locations: in $(on, 1)$ and $(on, 2)$ the thermostat is on, while in (off) the thermostat is off. There are three clocks: t tracks the time elapsed at the current location, y tracks the total time, and z tracks the time the thermostat has been on. There are also two parameters a and b that limit the maximum time the thermostat is in the locations. The initial state is $(on, 2)$ with $t = y = z = 0$. Using ∇_2, in 0.44 seconds we get the invariants

$$\begin{cases} I_{(on,2)} = \langle y - t, z - t \rangle \\ I_{(off)} = \langle -a^2 + ab + az + bz - by + bt \rangle \\ I_{(on,1)} = \langle a^2 - 2ab - az - bz + by + at \rangle \end{cases}$$

In [HHWT98] it was proved that, for $a = \ln(3)$, $b = \ln(2)$, the thermostat is on between $23.17/60 \approx 38.6\%$ and $23.51/60 \approx 39.2\%$ of the time within the first 60 time units of operation. We can use the polynomial invariants above to refine these bounds. At location (off), from the implicit invariant $0 \leq t \leq a$ and $-a^2 + ab + az + bz - by + bt = 0$ we get that

$$\frac{a^2 - 2ab + by}{a + b} \leq z \leq \frac{a^2 - ab + by}{a + b} \ .$$

We also get the same inequalities at location $(on, 1)$ by using the implicit invariant $0 \leq t \leq b$ and $a^2 - 2ab - az - bz + by + at = 0$. Substituting $a = \ln(3)$, $b = \ln(2)$, $y = 60$, we get the interval $[23.03/60, 23.46/60] \approx [38.4\%, 39.1\%]$, which provides us with a better upper bound.

Train System. The hybrid system shown in Figure 3 and taken from [SSM04b] models a train accelerating (location *acc*), moving at constant speed (location *cons*) and decelerating until stopping (location *dec*). Once the train has halted, it remains quiet for 2 seconds. There are four variables: the position of the train x, its velocity v, a clock t and a counter s of the number of stops made so far. The initial state is *acc* with $x = v = s = t = 0$.

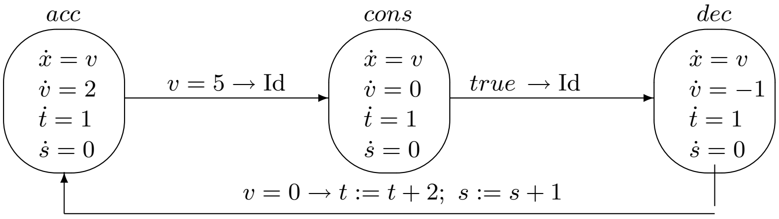

Fig. 3. Train system

We obtain the following invariants in 0.32 seconds using ∇_2:

$$\begin{aligned} I_{acc} &= \langle -4x + v^2 - 115s + 20t - 10v \rangle \\ I_{dec} &= \langle 4x + 115s - 20t - 20v + 75 + 2v^2 \rangle \\ I_{cons} &= \langle v - 5, 4x + 115s - 20t + 25 \rangle \end{aligned}$$

Note that these invariants, e.g. $4x + 115s - 20t - 20v + 75 + 2v^2 = 0$ at *dec*, can be found analytically by computing the distance covered x in terms of the other variables.

Charged Particle Revisited. Consider the hybrid system of the charged particle. Assume now that both the distance parameter d and the magnetic field magnitude a are left unknown (which is a more general setting than in [SSM04b]). Under these conditions the vector field in *magnetic* is no longer linear. However, notice that, since a is constant, the solution to the system of differential equations still has the same structure as in Section 3, with the difference that a may appear in a denominator. We overcome this problem by introducing a new auxiliary variable a' to represent the value a^{-1} (we assume that $a \neq 0$; the case $a = 0$ is straightforward to analyze). We also employ the polynomial $aa' - 1$ to represent the equation $aa^{-1} = 1$.

As before, due to imprecisions in our modeling, we first obtain the following invariants:

$$\begin{aligned} I_{right} &= \langle v_y + 2, v_x^2 - 4 \rangle \qquad I_{left} = \langle v_y + 2, v_x^2 - 4 \rangle \\ I_{magnetic} &= \langle ax - ad - v_y - 2, v_x^2 + v_y^2 - 8 \rangle \end{aligned}$$

These polynomials were computed in 1.80 seconds with ∇_2. Again, by using the implicit invariants $v_x \geq 0$ at *right* and $v_x \leq 0$ at *left*, we deduce that $v_x = 2$ at *right* and $v_x = -2$ at *left*. Adding these invariants to the guards and recomputing the fixpoint, in 0.70 seconds we get:

$$\begin{cases} I_{right} = \langle v_y + 2, v_x - 2, -ax + 4b - 2adb - ay \rangle \\ I_{magnetic} = \langle ax - ad - v_y - 2, v_x^2 + v_y^2 - 8, ay - 4b + 2adb - 2 + ad + v_x \rangle \\ I_{left} = \langle v_y + 2, v_x + 2, 4b - 2adb - ay + 4 - 2ad + ax \rangle \end{cases}$$

Let us see some properties of the system that these invariants allow us to prove. First, by using the invariant $ax + ay = 4b - 2adb$ at *right* we can compute the height where the particle collides as a function of the bounce counter b: by setting $x = 0$ we get $y = 2b(2-ad)/a$. In particular, if $ad = 2$ the particle returns to the origin for every bounce. Moreover, the invariants $ax = ad + v_y + 2$ and $v_x^2 + v_y^2 = 8$ let us find the maximum horizontal distance covered by the particle: the maximum distance is achieved when $\dot{x} = v_x = 0$, i.e. $v_y = \pm 2\sqrt{2}$; then this distance is $x = d + (2\sqrt{2} + 2)/a$ when $a > 0$, $x = d + (-2\sqrt{2} + 2)/a$ when $a < 0$ (the feasible solutions satisfy $x \geq d$).

6 Conclusions

We presented a computational method for generating the most precise algebraic invariant for linear dynamical systems whose eigenvalues have rational real and imaginary components. We then extended this method to compute equational invariants for hybrid systems using an abstract interpretation approach. The main computational technique is based on Gröbner basis computation and we do not use the prohibitively expensive (quantifier elimination) decision procedures for the reals. Canonical Gröbner bases provide a useful representation for sets of states as they have several important properties such as canonicity, closure under boolean operations and quantifier elimination. We showed results of running the proposed method on example hybrid systems discussed in the literature.

As future work, we plan to integrate our techniques with other approaches dealing with inequalities. The resulting method would allow a much more precise analysis of hybrid systems with a wider range of applicability.

References

[ACHH93] R. Alur, C. Courcoubetis, T. A. Henzinger, and P.-H. Ho. Hybrid automata: An algorithmic approach to the specification and verification of hybrid systems. In R. L. Grossman, A. Nerode, A. P. Ravn, and H. Rischel, editors, *HS*, volume 736 of *LNCS*, pages 209–229. Springer, 1993.

[AD94] R. Alur and D. Dill. A theory of timed automata. *Theoretical Computer Science*, 126:183–235, 1994.

[AP04] R. Alur and G. J. Pappas, editors. *Hybrid Systems: Computation and Control, 7th International Workshop, HSCC 2004*, volume 2993 of *LNCS*. Springer, 2004.

[Bry92] R. Bryant. Symbolic boolean manipulation with ordered binary-decision diagrams. *ACM Computing Surveys*, 24(3):293–318, 1992.

[CC77] P. Cousot and R. Cousot. Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *POPL 1977*, pages 238–252, 1977.

[CK98] A. Chutinan and B. H. Krogh. Computing polyhedral approximations to flow pipes for dynamic systems. In *37th IEEE Conference on Decision and Control*, 1998.

[CLO96] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms.* Springer-Verlag, New York, 1996.

[DM98] T. Dang and O. Maler. Reachability analysis via face lifting. In T. A. Henzinger and S. Sastry, editors, *HSCC*, volume 1386 of *LNCS*, pages 96–109. Springer, 1998.

[GS] D. R. Grayson and M. E. Stillman. Macaulay 2: A software system for research in algebraic geometry. Available at `http://www.math.uiuc.edu/Macaulay2/`.

[Hen] T. A. Henzinger. The symbolic approach to hybrid systems. Invited tutorial. `www-cad.eecs.berkeley.edu/~tah/Talks/the_symbolic_approach_to_hybrid_sy%stems.html`.

[HH95] T. A. Henzinger and P.-H. Ho. A note on abstract interpretation strategies for hybrid automata. Volume 999 of *LNCS*, pages 252–264, Berlin, 1995. Springer-Verlag.

[HHWT98] T. A. Henzinger, P.-H. Ho, and H. Wong-Toi. Algorithmic analysis of nonlinear hybrid systems. *IEEE Transactions on Automatic Control*, 43:540–554, 1998.

[HPR94] N. Halbwachs, Y.-E. Proy, and P. Raymond. Verification of linear hybrid systems by means of convex approximations. In B. Le Charlier, editor, *SAS*, volume 864 of *LNCS*, pages 223–237. Springer, 1994.

[KV02] A. B. Kurzhanski and P. Varaiya. On ellipsoidal techniques for reachability analysis. *Dynamics of Continuous, Discrete and Impulsive Systems Series B: Applications and Algorithms*, 9:347–367, 2002.

[LPY99] G. Lafferriere, G. J. Pappas, and S. Yovine. A new class of decidable hybrid systems. In F. W. Vaandrager and J. H. van Schuppen, editors, *HSCC*, volume 1569 of *Lecture Notes in Computer Science*, pages 137–151. Springer, 1999.

[LPY01] G. Lafferriere, G. J. Pappas, and S. Yovine. Symbolic reachability computations for families of linear vector fields. *J. Symbolic Computation*, 32(3):231–253, 2001.

[RCK04] E. Rodriguez-Carbonell and D. Kapur. An abstract interpretation approach for automatic generation of polynomial invariants. In *11th Static Analysis Symposium (SAS'04)*, volume 3148 of *LNCS*, 2004.

[SSM04a] S. Sankaranarayanan, H. Sipma, and Z. Manna. Constructing invariants for hybrid systems. In Alur and Pappas [AP04], pages 539–554.

[SSM04b] S. Sankaranarayanan, H. Sipma, and Z. Manna. Constructing invariants for hybrid systems. *Formal Methods in System Design*, 2004. Preprint submitted for publication.

[Tiw03] A. Tiwari. Approximate reachability for linear systems. In O. Maler and A. Pnueli, editors, *HSCC*, volume 2623 of *LNCS*, pages 514–525. Springer, April 2003.

[TK04] A. Tiwari and G. Khanna. Nonlinear systems: Approximating reach sets. In Alur and Pappas [AP04], pages 600–614.