Approximate Reachability for Linear Systems*

Ashish Tiwari

SRI International,
333 Ravenswood Ave,
Menlo Park, CA, U.S.A
tiwari@csl.sri.coma
Tel/Fax:+1.650.859.4774/2844

Abstract. We describe new techniques to construct, and subsequently refine, over-approximations of the reachability sets for linear dynamical systems. Our approach extracts information from eigenvectors to generate invariants of the system. It can be integrated with the qualitative abstraction tool [10] to generate refined abstractions of hybrid systems with linear continuous dynamics and we illustrate this on a collision-avoidance example from automobile cruise control problem, which was handled completely automatically by our tool.

1 Introduction

Establishing safety properties of hybrid and dynamical systems is one of the most interesting, but equally challenging, problem for formal methods. With the increased embedding of digital controllers inside physical devices, such as automobiles and aircraft, the need for automated tools and techniques for formal analysis and verification has become more pressing. Exhaustive testing via simulation is, in most cases, neither possible nor practical.

Reachability and safety are now being recognized as central problems in designing controllers. While issues related to stability and controllability are well-studied, there are not many results on computing the reachable set of hybrid systems. Known classes of hybrid systems for which reachability problem is decidable are timed automata [2], multirate automata [1], rectangular hybrid automata [8, 5], and certain subclasses of linear hybrid systems [6]. The most general decidability result [6] enforces stringent conditions on the continuous dynamics, where the matrix representing the linear dynamics is required to be diagonalizable with certain restricted kinds of eigenvalues. Moreover, the reach set computation algorithm uses the decision procedure for real closed fields to perform quantifier elimination on large and complex formulas, which is quite impractical.

One natural question then is whether we can relax the conditions and get an over-approximation of the reach set efficiently. So, for instance, if only a subset of eigenvalues of a linear system are rational, then can we still say something

* Full version of this paper is available at *http://www.csl.sri.com/users/tiwari/hscc03.ps*

about the set of reachable states of the system? What about non-rational eigenvalues? Furthermore, can we get better over-approximations as more and more eigenvalues turn out to be rationals? This paper presents techniques that answer these questions in the affirmative. Furthermore, the decision procedure for reals is applied only on relatively small formulas in a failure tolerant mode.

We also describe experimental results from using the new methods inside an abstraction framework. In [10], we presented a technique to construct qualitative abstractions of hybrid systems. For systems that were presented using only polynomials (possibly non-linear), the method was automated using a decision procedure for the real closed fields (the proof obligations that the decision procedure needs to handle are small and failure tolerant). Abstractions are constructed by using the sign abstraction of polynomials that appear in the problem specification. In many cases, the resulting abstractions were found to be too weak to prove the properties of interest. This is because success crucially depends upon the the choice of the seed polynomial set which is used to construct the abstraction. The new results in this paper suggest the "correct" set of seed polynomials for systems with linear dynamics.

The basic idea proposed in this paper is that certain eigenvectors can be used to construct polynomial expressions whose value can be bounded for all reachable states. An important feature of the incorporation of the eigenvector information in the abstraction procedure is that the eigenvectors do not need to be *explicitly* computed. They can be represented using symbolic coefficients and these symbolic coefficients can be constrained using algebraic equations. The abstraction algorithm treats the symbolic coefficients as parameters. With this improvement, our abstraction based approach for proving safety properties can now automatically handle several non-trivial systems.

1.1 Preliminaries: Linear Continuous Dynamical Systems

A *linear (continuous dynamical) system* CS is a tuple (X, Init, A) where X is a finite set of variables interpreted over the reals $\mathbb{R}$, $\mathbf{X} = \mathbb{R}^X$ is the set of all valuations of the variables X, $\mathit{Init} \subseteq \mathbf{X}$ is the set of initial states, and $A \in \mathbb{Q}^{n \times n}$ is the matrix which constrains the dynamics of CS by the differential equation $\dot{\boldsymbol{x}} = A\boldsymbol{x}$.

The semantics, $[[CS]]$, of a linear system $CS = (X, \mathit{Init}, A)$ 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 $t \in [t_0, t_1]$, $\dot{\boldsymbol{x}}(t) = A\boldsymbol{x}(t)$. 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 a set of bad states, then the original system will never reach a bad state. Note that the linear continuous dynamical systems we consider here are autonomous, that is, they have no inputs.

The reachability set computation problem has been shown to be decidable for a subclass of linear continuous dynamical systems. In particular, if the set *Init* of initial states is algebraic and either (1) A is a nilpotent matrix (that is, $A^m = 0$ for some $m \geq 0$), or (2) A is a diagonalizable matrix with rational eigenvalues, or (3) A is a diagonalizable matrix with purely imaginary eigenvalues of the form ir with $r \in \mathbb{Q}$, then the set $\mathit{Reach}(CS)$ was shown to be computable [7]. In fact, this decidability result was established for systems with inputs from a certain restricted set.

Let $CS = (X, \mathit{Init}, A)$ be a linear system. Then the set $[[CS]]$ contains all mappings $\boldsymbol{x}(t)$ defined by $\boldsymbol{x}(t) = e^{At}\boldsymbol{s}$, where $\boldsymbol{s} \in \mathit{Init}$ and the matrix exponential e^{At} is defined by the series $e^{At} = \sum_{k=0}^{\infty} \frac{t^k}{k!} A^k$. Therefore, the set of reachable states is

$$\mathit{Reach}(CS) = \{\boldsymbol{s} \in \mathbb{R}^n : \exists t, \boldsymbol{s_0}.\ (t \geq 0 \ \wedge\ \boldsymbol{s_0} \in \mathit{Init} \ \wedge\ s = e^{At}\boldsymbol{s_0})\}.$$

Example 1 (Collision Avoidance in Cruise Control). Consider a part of the leader control developed in [4] and also discussed in [9]. The control is applied during safety-critical situations when the inter-vehicle distance is small, or the relative velocity between vehicles is large. Let gap, v_f, v, and a respectively represent the gap between the two cars, the velocity of the leading car, and the velocity and acceleration of the rear car.

$$\dot{v} = a,\ \dot{a} = -3a - 3(v - v_f) + (\mathit{gap} - (v + 10)),\ \dot{\mathit{gap}} = v_f - v.$$

Formally, this describes a linear dynamical system with $X = \{v, v_f, a, \mathit{gap}\}$. Assuming the variable v_f is a parameter (unchanging symbolic constant), the dynamics can be written as $\dot{\boldsymbol{x}} = A\boldsymbol{x} + B$, where

$$A = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ -4 & 3 & -3 & 1 \\ -1 & 1 & 0 & 0 \end{bmatrix} \qquad B = \begin{bmatrix} 0 \\ 0 \\ -10 \\ 0 \end{bmatrix}$$

By a change of variables, $\mathit{rgap} \leftarrow \mathit{gap} - 10$, we get $\dot{\boldsymbol{x}} = A\boldsymbol{x}$, where $\boldsymbol{x} = [v, v_f, a, \mathit{rgap}]^T$. The set *Init* of initial states is left unspecified. We have also not formalized invariant sets here, but we will use bounds on the acceleration and other state variables later in the analysis. For a given set of possible initial states, the problem is to verify that the rear car would never collide with the car in front, that is, always $\mathit{gap} > 0$, or $\mathit{rgap} > -10$. It can be easily verified that the matrix A does not satisfy any of the three conditions specified above and hence, this example falls out of the class of systems for which reachability is known to be decidable.

2 Linear Systems with Real Eigenvalues

Let $CS = (X, Init, A)$ be a linear system with $A \in \mathbb{Q}^{n \times n}$. If λ is a real eigenvalue of A and $\boldsymbol{c} = [c_1, \ldots, c_n]^T$ is an eigenvector of A^T corresponding to λ, then we consider the polynomial $p = \boldsymbol{c}^T \boldsymbol{x}$, where $\boldsymbol{x}$ is the vector of state variables X. The derivative of this polynomial p is

$$\dot{p} = \boldsymbol{c}^T \dot{\boldsymbol{x}} = \boldsymbol{c}^T A \boldsymbol{x} = (A^T \boldsymbol{c})^T \boldsymbol{x} = (\lambda \boldsymbol{c})^T \boldsymbol{x} = \lambda p,$$

and hence, the value of this polynomial over any trajectory of CS is given by $p(t) = e^{\lambda t} p(0)$, where $p(0)$ is the value of p in an initial state of CS. Since $\lambda \in \mathbb{R}$, therefore, the components c_i of $\boldsymbol{c}$ are also reals. Therefore, an over-approximation of the reachable states is given by the formula

$$\exists t, s_0. \, (t \geq 0 \ \wedge \ \boldsymbol{c}^T \boldsymbol{x} = e^{\lambda t} \boldsymbol{c}^T s_0 \ \wedge \ s_0 \in Init).$$

Doing an approximate quantifier-elimination, we notice that the value of $\boldsymbol{c}^T \boldsymbol{x}(t)$ will either (i) monotonically increase or decrease while remaining sign-invariant (if $\lambda > 0$), or (ii) asymptotically converge to 0 (if $\lambda < 0$), or (iii) remain constant (if $\lambda = 0$). We formally state this in Theorem 1.

Theorem 1. *Let $CS = (X = \{x_1, \ldots, x_n\}, Init, A)$ be a linear dynamical system with the matrix $A \in \mathbb{Q}^{n \times n}$. Let λ be a real eigenvalue of the matrix A^T, $\boldsymbol{c} = [c_1, c_2, \ldots, c_n]^T$ be a corresponding eigenvector (of A^T), and $p = c_1 x_1 + c_2 x_2 + \cdots + c_n x_n = \boldsymbol{c}^T \boldsymbol{x}$ be the corresponding polynomial.*

Then, the components c_i of the eigenvector $\boldsymbol{c}$ are all real and
(i) if $\lambda > 0$, then the polynomial p is sign invariant for CS; more specifically, if $d_{min} > 0$, then $p \geq d_{min}$ always, if $d_{max} < 0$, then $p \leq d_{max}$ always, and if $d_{min} = d_{max} = 0$, then $p = d$ always;
(ii) if $\lambda < 0$, then the value of the polynomial p asymptotically converges to 0; more specifically, it is always true that $min\{0, d_{min}\} \leq p \leq max\{0, d_{max}\}$; and
(iii) if $\lambda = 0$, then the polynomial p is an invariant function for CS, that is, it is always the case that $p = p(0)$.

Here the constants d_{min} and d_{max} are respectively the minimum and maximum values in the set $\{\boldsymbol{c}^T \boldsymbol{x}(0) : \boldsymbol{x}(0) \in Init\}$.

Theorem 1 gives a method to generate over-approximations of the reach set. It can be applied repeatedly to give several different formulas which over-approximate the reach set, and the conjunction (set intersection) of these formulas (sets) will still be an over-approximation. In particular, the more real eigenvalues the matrix A has, the more refined reach set computation will result. This points to the results in [7] where the exact reach set is shown to be computable when matrix A has exactly n rational eigenvalues. The exact connection will be explored in Section 3.

Representation and Computability Issues Theorem 1 gives a way to generate formulas representing over-approximations of the reach set whenever matrix

A has a real eigenvalue. But, for purposes of computing, we need finite representations of the real eigenvalue λ and the eigenvector $\boldsymbol{c}$. We use polynomials for this purpose and we show below (Proposition 2) that this representation suffices.

Definition 1. *A real number $\alpha \in \mathbb{R}$ is algebraic over a commutative ring K if it is a zero of some polynomial in $K[X]$. If the base ring K is unspecified, then it is assumed to be the field of rationals $\mathbb{Q}$.*

The vector space generated by a finite set of algebraic numbers (over $\mathbb{Q}$) is finite-dimensional (over the field $\mathbb{Q}$). The following facts on algebraic numbers can be proved using either linear algebra (dimension argument) or symmetric functions.

Proposition 1. *If $\alpha \in \mathbb{R}$ is algebraic over $\mathbb{Q}[\beta]$, where β is algebraic over $\mathbb{Q}$, then α is algebraic over $\mathbb{Q}$. Furthermore, the set of algebraic numbers is closed under addition, subtraction, multiplication, and division. If α is an algebraic number over K, then so is $c\alpha$ and $\alpha + c$ for any constant $c \in K$.*

The following is an obvious observation about eigenvectors.

Proposition 2. *The components of an eigenvector $\boldsymbol{c}$ of a matrix $A \in \mathbb{Q}^{n\times n}$ corresponding to an eigenvalue λ are algebraic over $\mathbb{Q}[\lambda]$. Since λ is algebraic, so are the components of $\boldsymbol{c}$.*

The fact that the eigenvalue is algebraic and that the eigenvectors have algebraic components (Proposition 2) is crucial since it implies that the polynomial p can be expressed in terms of polynomials *over* $\mathbb{Q}$.

Example 2. Consider the linear system of Example 1. The characteristic polynomial for A, $\lambda(\lambda^3+3\lambda^2+4\lambda+1)$, has exactly two real zeros. The nonzero eigenvalue, denoted by λ, lies between $-1/3$ and $-1/4$. Now, if $\boldsymbol{c} = [c_1, c_2, c_3, c_4]^T$ is an eigenvector of A^T corresponding to λ, then $A^T\boldsymbol{c} = \lambda\boldsymbol{c}$. We assume, without loss of generality, that $c_4 = 1$, and hence we get an eigenvector $[c_1, c_2, c_3, 1]^T$ where c_1, c_2 and c_3 satisfy the equations $c_3 = \lambda$, $c_1 = \lambda^2+3\lambda$, and $c_2 = -c_1-1$. Therefore, the polynomial corresponding to this eigenvector, $p = c_1v - (c_1+1)v_f + c_3a + rgap$, asymptotically converges to 0 as the linear system evolves (by Theorem 1).

If initially $p > 0$, then assuming the invariant $a > -2$, we can prove that $rgap > -10$ always. This follows from the fact that the formula

$$p \geq 0 \ \wedge \ rgap = -10 \ \wedge \ v - v_f > 0 \ \wedge \ a > -2$$

is unsatisfiable under the condition that $-1/3 < \lambda < -1/4$. Note that for collision to occur, it should be the case that $v - v_f > 0$. This analysis was automatically done by our abstraction and model-checking tool, see Section 4.

In case $p < 0$ initially, if $rgap_0, v_0, a_0$ denote the values of variables at $t = 0$ and $rgap, v, a$ denote the values at a later time, then $rgap_0 - c_1v_f + c_1v_0 - v_f + c_3a_0 < rgap - c_1v_f + c_1v - v_f + c_3a$. Assuming initially $8v_0 - 9gap_0 + 21 < 0$, then we can again establish collision avoidance for these initial states by observing that the formula

$$p_0 < p \ \wedge \ v > 0 \ \wedge \ 8v_0 - 9gap_0 + 21 < 0$$

is unsatisfiable assuming the invariants $a < 5 \wedge a > -2 \wedge -8/9 < c_1 < -11/16$. Note that this approach also provides a way to *synthesize* switching laws that guarantee safety.

2.1 Linear Systems with Purely Imaginary Eigenvalues

Let $CS = (X, Init, A)$ be a linear system with $A \in \mathbb{Q}^{n\times n}$. Assume that ir is a purely imaginary eigenvalue of A such that $r \in \mathbb{R}$. Let $\boldsymbol{c}^T$ be an eigenvector of A^T corresponding to the eigenvalue ir. Now, clearly,

$$\frac{d}{dt}(\boldsymbol{c}^T\boldsymbol{x}) \;=\; \boldsymbol{c}^T A\boldsymbol{x} \;=\; (A^T\boldsymbol{c})^T\boldsymbol{x} \;=\; (ir)\boldsymbol{c}^T\boldsymbol{x}$$

and hence,

$$\frac{d^2}{dt^2}(\boldsymbol{c}^T\boldsymbol{x}) \;=\; (ir)^2\boldsymbol{c}^T\boldsymbol{x} \;=\; -r^2\boldsymbol{c}^T\boldsymbol{x}.$$

Since $r \in \mathbb{R}$ and $(A^T)^2\boldsymbol{c} = -r^2\boldsymbol{c}$, it follows that $\boldsymbol{c} \in \mathbb{R}^n$ (because $(A^T)^2$ is a matrix over the rationals and r^2 is a real). Therefore, $\boldsymbol{c}^T\boldsymbol{x}$ is a linear polynomial (over the state variables $\boldsymbol{x}$) with real coefficients. Theorem 2 gives bounds on the value of this polynomial, and hence, the set of reachable states is a subset of the states for which this bound is true.

Theorem 2. *Let $CS = (X, Init, A)$ be a linear dynamical system as above. Let ir be a purely imaginary eigenvalue of the matrix A^T with $r \in \mathbb{R}$, $\boldsymbol{c} = [c_1, c_2, \ldots, c_n]^T$ be a corresponding eigenvector of A^T, and $p = c_1x_1 + c_2x_2 + \cdots + c_nx_n = \boldsymbol{c}^T\boldsymbol{x}$ be the corresponding linear polynomial. Then, the components c_i of the eigenvector $\boldsymbol{c}$ are all real and*

$$-(d_1^2 + d_2^2)^{1/2} \le p \le (d_1^2 + d_2^2)^{1/2}$$

where $d_1 = max\{|\boldsymbol{c}^T\boldsymbol{x_0}| : \boldsymbol{x_0} \in Init\}$ and $d_2 = (max\{|\boldsymbol{c}^T\dot{\boldsymbol{x_0}}| : \boldsymbol{x_0} \in Init\})/r$.

Representation Issues The real numbers in Theorem 2 can be represented using polynomial expressions. We argue this as follows: the number $-r^2$ is an eigenvalue of the matrix $(A^T)^2$. Since $(A^T)^2 \in \mathbb{Q}^{n\times n}$ is a rational matrix, the eigenvalue $-r^2$ is clearly algebraic (since it is a zero of the characteristic polynomial of A^2). It follows that r^2 is algebraic, and hence r is algebraic. Now, it follows that the components of the vector $\boldsymbol{c}$ are algebraic as well since they satisfy the simultaneous homogeneous system of equations $(A^T)^2\boldsymbol{c} = -r^2\boldsymbol{c}$.

2.2 Linear Systems with Complex Eigenvalues

Suppose $p(y)$ is the characteristic polynomial of matrix A^T. Since A is a rational matrix, the polynomial $p(y)$ has rational coefficients. In general, the polynomial p can be factored as

$$p \;=\; \Pi_i(y - \lambda_i).\Pi_j(y^2 + r_j^2).\Pi_k(y^2 + a_ky + b_k),$$

where $\lambda_i, r_j, a, b \in \mathbb{R}$, $a \neq 0$ and $4b > a^2$. In Section 2 we extracted reachability information out of factors of the first kind, in Section 2.1 we did the same for factors of the second kind. Now, let $y^2 + ay + b$ be a factor of the third kind, where $a, b \in \mathbb{R}$ and $a \neq 0, 4b > a^2$.

There exist vectors $\boldsymbol{c}$ such that $((A^T)^2 + aA^T + bI)\boldsymbol{c} = 0$, for instance, the eigenvectors of A^T corresponding to the roots of the polynomial $y^2 + ay + b$ are such vectors. In a sense, the vector $\boldsymbol{c}$ is a generalized eigenvector of A^T corresponding to the factor $y^2 + ay + b$. Since $A^T \in \mathbb{Q}^{n\times n}$, $a \in \mathbb{R}$, and $b \in \mathbb{R}$, it follows that there exists such a vector $\boldsymbol{c} \in \mathbb{R}^n$.

Theorem 3. *Let $CS = (X, Init, A)$ be a linear dynamical system with $A \in \mathbb{Q}^{n\times n}$. Let y^2+ay+b be a factor of the characteristic polynomial of A with $a, b \in \mathbb{R}$, $a^2 < 4b$. Let $\boldsymbol{c} = [c_1, c_2, \ldots, c_n]^T$ be a corresponding generalized eigenvector (of A^T, as defined above), and $p = c_1x_1 + c_2x_2 + \cdots + c_nx_n = \boldsymbol{c}^T x$ be the corresponding polynomial. Then, the components c_i of the eigenvector $\boldsymbol{c}$ are all real and if $a > 0$ then*

$$-(d_1^2 + d_3^2)^{1/2} \leq p \leq (d_1^2 + d_3^2)^{1/2}$$

where $d_1 = max\{|\boldsymbol{c}^T\boldsymbol{x_0}| : x_0 \in Init\}$ and $d_3 = (max\{2|\boldsymbol{c}^T\dot{\boldsymbol{x}}_{\boldsymbol{0}}| : x_0 \in Init\} + d_1a)/(4b - a^2)^{1/2}$.

Finally, we note that the real numbers a and b are both algebraic. This is because if λ_1 and λ_2 are the two (complex) roots of $y^2 + ay + b$, then $a = \lambda_1 + \lambda_2$ and $b = \lambda_1\lambda_2$. But λ_1 and λ_2 are algebraic (roots of the characteristic polynomial) and hence, a and b are algebraic too (using Proposition 1).

Example 3. Consider the linear system from Example 1. In Example 2, we used the real root of the characteristic polynomial $y^3 + 3y^2 + 4y + 1$. The other two roots of the characteristic polynomial are the roots of the polynomial $y^2 + (3 + \lambda)y + (\lambda^2 + 3\lambda + 4)$, or equivalently $y^2 + (3+\lambda)y - 1/\lambda$, where λ is the real root. The equation $((A^T)^2 + (\lambda + 3)A^T - (1/\lambda)I)\boldsymbol{c} = 0$ has two solutions $\boldsymbol{c} = [-\lambda, \lambda, 1, 0]^T$ and $\boldsymbol{c} = [1/\lambda, -(1 + \lambda)/\lambda, 0, 1]^T$. Since $\lambda + 3 > 0$, Theorem 3 is applicable. Consider the polynomial $p_2 = 1/\lambda v - ((1 + \lambda)/\lambda)v_f + rgap$ corresponding to the latter solution. For simplicity, assume that the initial conditions are given by $1/\lambda(v - v_f) - v_f + rgap = 0$, so that $d_1 = 0$. Now, assuming $|a| < 1 \wedge |rgap| < 4 \wedge |v_f| < 20$ initially, we get $B < 12$. Thus, we get the following over-approximation of the reach set: $-12 < p_2 < 12$. This can be used to prove collision avoidance under the assumption that v_f is at least 10.

2.3 Unifying the Results

Let matrix A be such that (a) there are k polynomials $p_1, p_2, \ldots, p_k$, as in Section 2, corresponding to real eigenvalues $\lambda_1, \ldots, \lambda_k$; (b) there are l polynomials $q_1, q_2, \ldots, q_l$, as in Section 2.1, corresponding to purely imaginary eigenvalues $i\lambda'_1, \ldots, i\lambda'_l$; and (c) there are m polynomials $r_1, r_2, \ldots, r_m$, as in Section 2.2, corresponding to complex eigenvalues $a_1 \pm ib_1, \ldots, a_m \pm ib_m$. Putting the results in Sections 2, 2.1, and 2.2 together, we get the following expression for (an over-approximation of) the set of reachable states,

$$\begin{aligned}\exists t \geq 0.\ & (\bigwedge_{i=1}^{k} p_i(t) = p_i(0)e^{\lambda_i t}) \ \wedge \ (\bigwedge_{i=1}^{l} q_i(t) = q_i(0)cos(\lambda'_i t) + \frac{\dot{q}_i(0)}{\lambda'_i} sin(\lambda'_i t)) \ \wedge \\ & (\bigwedge_{i=1}^{m} r_i(t) = e^{a_i t}(r_i(0)cos(b_i t) + \frac{\dot{r}_i(0) - r_i(0)a_i}{b_i} sin(b_i t))) \qquad (1)\end{aligned}$$

Instead of approximating the above expression by distributing the existential quantifier over the conjunctions (and thus, obtaining results in previous sections), we can perform other simplifications to extract new and different upper-bounds on the set of reachable states. As a simple example, if polynomials p_1 and p_2 correspond to the same real eigenvalue λ_i, then we can deduce the invariant $p_2(0)p_1 = p_1(0)p_2$ for the system. This can be used to further strengthen the approximate reachable set produced using Theorems 1, 2, and 3. The efficient extraction and use of these optimizations will be further studied in the future. Note that if λ_i's (and a_i and b_i's) are rational, then the representation of the eigenvalues and computation with the eigenvectors becomes much easier.

3 Related Work

Consider the case when A is diagonalizable with rational eigenvalues $\lambda_1, \ldots, \lambda_n$, that is, $A = UDU^{-1}$, where D is a diagonal matrix with entries $\lambda_1, \ldots, \lambda_n$ on its diagonal and U is the matrix with eigenvectors of A as its columns. Now, the solution to the differential equation $\dot{\boldsymbol{x}} = A\boldsymbol{x}$ is $\boldsymbol{x}(t) = Ue^{Dt}U^{-1}\boldsymbol{x}(0)$ where $\boldsymbol{x}(0) \in \mathit{Init}$ is an initial state of the system. Therefore, the *exact* reach set is given by

$$\begin{aligned}& \exists t \geq 0.\ \boldsymbol{x}(t) = Ue^{Dt}U^{-1}\boldsymbol{x}(0) \ \wedge \ \boldsymbol{x}(0) \in \mathit{Init} \\ \Leftrightarrow\ & \exists t \geq 0.\ U^{-1}\boldsymbol{x}(t) = e^{Dt}U^{-1}\boldsymbol{x}(0) \ \wedge \ \boldsymbol{x}(0) \in \mathit{Init} \\ \Leftrightarrow\ & \exists t \geq 0.\ \boldsymbol{P}(t) = e^{Dt}\boldsymbol{P}(0) \ \wedge \ \boldsymbol{P}(0) \in U^{-1}\mathit{Init} \\ \Leftrightarrow\ & \exists t \geq 0.\ \boldsymbol{P}(t) = [e^{\lambda_1 t}p_1(0),\ e^{\lambda_2 t}p_2(0), \ldots, e^{\lambda_n t}p_n(0)]^T \ \wedge \ \boldsymbol{P}(0) \in U^{-1}\mathit{Init}\end{aligned}$$

Here we have assumed that $p_1, \ldots, p_n$ are polynomials defined by $p_i(t) = \boldsymbol{w_i}^T\boldsymbol{x}(t)$, where $\boldsymbol{w_i}^T$ is the i-th row of matrix U^{-1} and $\boldsymbol{P}$ is the vector $[p_1,\ p_2,\ \ldots,\ p_n]^T$. The notation $U^{-1}\mathit{Init}$ denotes the set of all vectors obtained by transforming vectors in Init by U^{-1}.

Note that the polynomials P are exactly the polynomials that are computed in our approach. This is because

$$A^T = (U^{-1})^T D^T U^T = (U^{-1})^T D U^T$$

and therefore, since $\boldsymbol{w_i}^T$ is the i-th row of U^{-1}, $\boldsymbol{w_i}$ is the i-th column of $(U^{-1})^T$, or the eigenvector of A^T corresponding to the eigenvalue λ_i. Thus, the difference between [7] and our approach for this restricted class of systems is (i) we work in the space obtained by applying the transformation U^{-1}, and (ii) we use the following logical inference rule to *simplify* the quantifier elimination problem,

$$\exists t.(\phi_1(t) \ \wedge \ \phi_2(t)) \Rightarrow \exists t.\phi_1(t) \ \wedge \ \exists t.\phi_2(t)$$

Clearly, the right-hand side formula is *weaker* than the left-hand side formula, and hence applying this results in an *over-approximation* of the reach set. Thus, the exact reach set formula above is approximated in our approach to

$$\bigwedge_{i=1}^{n} (\exists t \geq 0.\ p_i(t) = e^{\lambda_i t} p_i(0) \ \wedge \ p_i(0) \in (U^{-1} \mathit{Init})|_i)$$

and then we apply even further approximations to *completely eliminate* the need for quantifier elimination (as in the proofs of Theorems 1, 2, and 3). The significance of our results is for the cases when the result of [7] are either not applicable or impractical.

4 Integrating with the Abstraction tool

The current version of our abstraction tool makes no assumption that the dynamics are linear and does not implement any specific optimizations for this case. However, it can still deduce the facts given in Theorem 1 if it is given the correct set of seed polynomials. The polynomial $c_1 v - (c_1 + 1)v_f + c_3 a + \mathit{rgap}$ can be given to the system by adding c_1 and c_3 as (dummy) parameters and specifying, as invariant *Inv*, the two equations satisfied by c_1 and c_3, see Example 2. In the experiments that we carried out, we also added, as additional invariants *Inv*, the facts that $-1/3 < \lambda < -1/4, -8/9 < c_1 < -11/16$ and $a > -2$ (thus limiting the maximum deceleration of the rear car). Now, given this information, the abstraction tool automatically identifies that for the given dynamical system,

$$d/dt(\mathit{rgap} - c_1 v_f + c_1 v - v_f + c_3 a) = \lambda(\mathit{rgap} - c_1 v_f + c_1 v - v_f + c_3 a)$$

for some *negative* real number λ. Though the generation of the eigenvectors is not currently automated in our tool, it can easily be done and is left for future development.

If the initial condition of the system are specified as

$$(\mathit{rgap} - c_1 v_f + c_1 v - v_f + c_3 a > 0) \ \wedge \ \mathit{rgap} > -10$$

or any other expression which is *stronger* than this (that is, entails a subset of the initial states specified by the above formula), and the invariants are specified as described above, then the tool automatically constructs a finite state discrete transition system abstraction of the dynamical system against which the collision avoidance property is validated. This proves collision avoidance for the original dynamical system and in fact, it gives a condition that should be true of the initial states for which we are guaranteed to not collide with the car in front. Thus, if the initial state region was a subset of the more general one described here, our tool would still successfully prove collision avoidance.

5 Conclusion

In this paper we have presented new techniques to compute over-approximations of the reach set for linear dynamical systems. Our techniques can handle systems with mixed (reals and imaginary) eigenvalues unlike results by Laferriere et. al. [3, 7]. The approximate reachability is, in many cases, sufficient to establish safety properties of the system. Our method integrates naturally with the qualitative abstraction tool we have developed. The tool uses a decision procedure for the quantifier-free theory of reals in a failure-tolerant mode. This means that even if the decision procedure fails (due to a lack of sufficient memory or time), the procedure can still be used (without compromising soundness).

In this work, we have used eigenvectors to generate seed polynomials for qualitatively abstracting linear dynamical system. Finding a good set of initial seed polynomials for other classes of systems would be a topic for future research. Extending to hybrid systems can be done along the lines of [6], where the concept of o-minimality is used to extend reachability algorithms for dynamical systems to those for hybrid systems. In the future, we wish to investigate more intelligent heuristics for eliminating quantifiers from Formula 1 and using them for synthesizing switching laws.

References

[1] R. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P.-H. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. The algorithmic analysis of hybrid systems. *Theoretical Computer Science*, 138(3):3–34, 1995.

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

[3] Rajeev Alur, Tom Henzinger, Gerardo Lafferriere, and George J. Pappas. Discrete abstractions of hybrid systems. *Proceedings of the IEEE*, 88(2):971–984, July 2000.

[4] D. Godbole and J. Lygeros. Longitudinal control of the lead car of a platoon. *IEEE Transactions on Vehicular Technology*, 43(4):1125–35, 1994.

[5] Thomas A. Henzinger, Peter W. Kopke, Anuj Puri, and Pravin Varaiya. What's decidable about hybrid automata? *Journal of Computer and System Sciences*, 57:94–124, 1998. A preliminary version appeared in the Proceedings of the 27th Annual ACM Symposium on Theory of Computing (STOC 1995), pp. 373-382.

[6] 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, *Hybrid Systems: Computation and Control HSCC*, *LNCS* 1569:137–151. Springer Verlag, 1999.

[7] 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.

[8] A. Puri and P. Varaiya. Decidability of hybrid systems with rectangular differential inclusions. In D. L. Dill, editor, *Computer Aided Verification, CAV*, *LNCS* 818:95–104. Springer Verlag, 1994.

[9] A. Puri and P. Varaiya. Driving safely in smart cars. In *Proceedings of the 1995 American Control Conference*, 1995.

[10] A. Tiwari and G. Khanna. Series of abstractions for hybrid automata. In C. J. Tomlin and M. R. Greenstreet, editors, *Hybrid Systems: Computation and Control HSCC*, *LNCS* 2289:465–478. Springer, March 2002.