43rd IEEE Conference on Decision and Control
December 14-17, 2004
Atlantis, Paradise Island, Bahamas

S.O.S. for Safety

Hakan Yazarel, Stephen Prajna and George J. Pappas

Abstract— **Verification of continuous systems remains one of the main obstacles in the safety verification of hybrid systems. In this paper, by exploiting the structure of linear dynamical systems, we convert the exact safety verification of linear systems with certain eigen-structure as an emptiness problem for a semi-algebraic set. Sum of squares (SOS) decomposition is then employed to check emptiness of the set defined by polynomial equalities and inequalities which can be effectively computed by semidefinite programming.**

I. Introduction

The safety problem for hybrid systems asks whether trajectories starting from a set of initial states reach a set of unsafe (final) states. Safety verification of purely discrete systems is mature [1]. However, verification of continuous systems remains one of the main obstacles in the safety verification of hybrid systems. This is a difficult problem that even for linear systems of the form $\dot{x} = Ax$ has escaped analytic solution.

For safety verification, *approximate* methods over- or under-approximate the reachable set by using polyhedral, level-sets, or ellipsoid representations. Given a set of initial states, reachable sets are computed which rely on optimization techniques combined with numerical methods for flow-pipe approximations [2], polygonal computations [3], ellipsoidal calculus [4], and Hamilton-Jacobi equations [5]. A scalable verification method, which provides safety certificates in realistic computation times, has been developed for linear systems with polytopic sets of initial and final states by exploiting linear dynamical system structure and using geometric programming relaxations [6].

Exact safety verification of linear systems starting in a semi-algebraic set is possible under certain eigen-structure conditions [7], [8]. In [9], quantifier elimination techniques coupled with understanding of linear system eigen-structure resulted in over-approximating the reachable set for linear systems with almost arbitrary eigen-structure. In [8], exact reachable set of linear systems with certain eigen-structure is computed. Unfortunately, such symbolic computations rely on expensive quantifier elimination techniques [10].

In this paper, we are interested in *exact* safety verification of linear systems. We do not compute the reachable set as in [8], but we simply provide safety certificates. The set of initial and final (unsafe) states are considered to be semialgebraic sets. We convert the exact safety verification of linear systems with certain eigen-structure to an emptiness of a set defined by polynomial equalities and inequalities. We use recent advances in algebraic optimization, in particular the sum of squares (SOS) decomposition [11] for which software tools are available [12]. Using sum of squares decomposition, *Positivstellensatz* [13] provides a characterization of *infeasibility certificates* for systems of polynomial equalities and inequalities. Also, it has been recently shown [11] that Positivstellensatz refutations can be computed using hierarchies of semidefinite programming, which promises to be a scalable solution to the exact safety verification problem. For more general nonlinear system verification, the method in [14] provides sufficient conditions, whereas the method in this paper provides sufficient and necessary conditions for more restricted linear systems. Also, it is shown that the polynomial sets derived in this paper are good seeds for the discrete abstraction of hybrid systems [15] with linear dynamics.

II. Problem Formulation

In this paper, we consider linear systems of the form,

$$\dot{x} = Ax, \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the state at t, and $A \in \mathbb{Q}^{n\times n}$ is the system matrix. Given an initial state $x_0 = x(0)$, the solution to the differential equation (1) for $t \geq 0$ is,

$$x(t) = e^{At}x_0. \tag{2}$$

We shall consider sets of initial and final states X_0 and X_f as semialgebraic sets defined as,

$$X_0 = \{x_0 \in \mathbb{R}^n \mid \bigwedge_{i=1}^{m} p_i(x_0) \geq 0\}, \tag{3}$$

$$X_f = \{x_f \in \mathbb{R}^n \mid \bigwedge_{i=m+1}^{m+k} p_i(x_f) \geq 0\}, \tag{4}$$

where $p_i(x)$ are polynomial functions with rational coefficients.

Given a set of initial states X_0, the forward and backward reachable sets of the linear system (1) are defined as,

$$\begin{aligned}\text{Post}(A, X_0) = \{x_f \in \mathbb{R}^n \mid \exists t\ \exists x_0 :\\ t \geq 0\ \wedge\ x_0 \in X_0 \wedge x_f = e^{At}x_0\}\end{aligned} \tag{5}$$

$$\begin{aligned}\text{Pre}(A, X_0) = \{x_f \in \mathbb{R}^n \mid \exists t\ \exists x_0 :\\ t \leq 0\ \wedge\ x_0 \in X_0 \wedge x_f = e^{At}x_0\}\end{aligned} \tag{6}$$

Given a set of final or unsafe states X_f, we define the forward and backward safety predicates as,

$$\text{Safe}_+(A, X_0, X_f) = \begin{cases} 1 & \text{if Post}(A, X_0) \cap X_f = \emptyset \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

This research is partially supported by the National Science Foundation Information Technology Research grant CCR01-21431.

Hakan Yazarel and George J. Pappas are with GRASP Laboratory, Department of Electrical and Systems Engineering, University of Pennsylvania, 200 South 33rd Street, Philadelphia, PA 19104, USA {hakan,pappasg}@seas.upenn.edu

Stephen Prajna is with Control and Dynamical Systems, California Institute of Technology, Pasadena, CA 91125, USA prajna@cds.caltech.edu

$$\text{Safe}_-(A, X_0, X_f) = \begin{cases} 1 & \text{if Pre}(A, X_0) \cap X_f = \emptyset \\ 0 & \text{otherwise} \end{cases} \quad (8)$$

We say $\text{Safe}(A, X_0, X_f) = 1$ if $\text{Safe}_+(A, X_0, X_f) = 1 \wedge \text{Safe}_-(A, X_0, X_f) = 1$.

In this paper, we are interested in the following problem,

Problem 2.1: Given a linear system (A, X_0, X_f), determine if $\text{Safe}_+(A, X_0, X_f) = 1$ and $\text{Safe}_-(A, X_0, X_f) = 1$.

III. Reachability of Linear System with Rational Eigenvalues

In this section, we consider linear systems with rational eigenvalues. We first transform the system in modal or eigen-coordinates.

Assuming the matrix A is diagonalizable, we have $A = T^{-1}\Lambda T$ or $\Lambda = TAT^{-1}$ where $\Lambda \in \mathbb{Q}^{n\times n}$ is a diagonal matrix whose diagonal entries are eigenvalues of matrix A and $T \in \mathbb{Q}^{n\times n}$ is an invertible transformation matrix defined as $T = [\eta_1|\eta_2|\cdots|\eta_n]^T$ where η_i are left eigenvectors of A. If we define a new state vector

$$z = Tx,\ z \in \mathbb{R}^n \quad (9)$$

and substitute $x = T^{-1}z$ into the differential equation (1), then we obtain the following equivalent differential equation,

$$\dot{z} = \Lambda z, \quad (10)$$

Note that, this is actually transforming the state space into eigenspace by the transformation (9). The differential equation (10) in eigenspace has the following solution,

$$z_i = e^{\lambda_i t} z_{0i}, \quad i = 1, \ldots, n, \quad (11)$$

where λ_i are the eigenvalues of the system matrix A and $z_0 = Tx_0$ is the initial state vector. The transformed states and the sets of initial states and final states in eigen-coordinates are as follows,

$$z_0 = Tx_0, \quad Z_0 = \{z_0 \mid z_0 = Tx_0,\ x_0 \in X_0\}, \quad (12)$$
$$z_f = Tx_f, \quad Z_f = \{z_f \mid z_f = Tx_f,\ x_f \in X_f\}, \quad (13)$$

where z_0 and z_f are the initial and final states in eigenspace, Z_0 and Z_f are the sets of initial and final states in eigenspace, x_0 and x_f are the states in the sets X_0 and X_f. Note that, since the transformation matrix T is invertible, given semialgebraic sets X_0 and X_f in state space, the transformed set of initial states Z_0 and set of final states Z_f in eigenspace are also semialgebraic in the form,

$$Z_0 = \{z_0 \in \mathbb{R}^n \mid \bigwedge_{i=1}^{m} p_{zi}(z_0) \geq 0\}, \quad (14)$$

$$Z_f = \{z_f \in \mathbb{R}^n \mid \bigwedge_{i=m+1}^{m+k} p_{zi}(z_f) \geq 0\}, \quad (15)$$

where $p_{zi}(z)$ are polynomial functions with rational coefficients. Therefore, we verify the system (Λ, Z_0, Z_f) in modal coordinates which is equivalent to verifying the system (A, X_0, X_f) in original coordinates.

Theorem 3.1: Given a diagonalizable linear system (A, X_0, X_f) with rational eigenvalues, the following statements are equivalent,

1) $\text{Safe}_+(A, X_0, X_f) = 1$
2) $\text{Safe}_+(\Lambda, Z_0, Z_f) = 1$
3) The set defined by the following set of polynomial equalities and inequalities is empty for the system in modal coordinates,

$$\begin{aligned} z_{f1}^{a_{12}} z_{02}^{a_{11}} - z_{f2}^{a_{11}} z_{01}^{a_{12}} &= 0 \\ z_{f2}^{a_{22}} z_{03}^{a_{21}} - z_{f3}^{a_{21}} z_{02}^{a_{22}} &= 0 \\ &\vdots \quad (16) \\ z_{f,(n-1)}^{a_{(n-1),2}} z_{0n}^{a_{(n-1),1}} - z_{fn}^{a_{(n-1),1}} z_{0,(n-1)}^{a_{(n-1),2}} &= 0 \\ p_{tf}(z_f) - p_{tf}(z_0) &\geq 0 \quad (17) \end{aligned}$$

$$p_{zi}(z_0) \geq 0 \quad i = 1, \ldots, m \quad (18)$$

$$p_{zi}(z_f) \geq 0 \quad i = m+1, \ldots, m+k \quad (19)$$

where $p_{tf}(z) = \lambda_1 z_1^2 + \lambda_2 z_2^2 + \cdots + \lambda_n z_n^2$,

$$a_{i1} = \frac{s_i}{c_i}, a_{i2} = \frac{s_{i+1}}{c_i}, i = 1, \ldots, n-1 \quad (20)$$

$\lambda_i = \frac{n_i}{d_i}$ are rationals in reduced form, $n_i \in \mathbb{Z}$, $d_i \in \mathbb{Z}^+$, $d = \prod_{i=1}^{n} d_i$, $d \in \mathbb{Z}^+$, $s_i = \lambda_i d$, $s_i \in \mathbb{Z}$, $c_i = \gcd(s_i, s_{i+1})$ and gcd denotes the greatest common divisor.

Proof: (1) $\Leftrightarrow$ (2): Since the transformation matrix T is invertible, $\text{Safe}_+(A, X_0, X_f) = 1$ if and only if $\text{Safe}_+(\Lambda, Z_0, Z_f) = 1$.

(2) $\Leftrightarrow$ (3): A state z_f is reachable from z_0 at some time if and only if there is a trajectory satisfying the system's model defined by (10) passing from both z_0 and z_f. Now, we find the set of polynomial equalities that uniquely defines all the possible trajectories of the system defined in (10) with the solution in (11). For simplicity, we assume $\lambda_i \geq 0$. For general case, the proof is similar. We assume that $\lambda_i = \frac{n_i}{d_i}$ are in reduced form. We define $d = \prod_{i=1}^{n} d_i$. By eliminating the term $e^{\frac{t}{d}}$ from the solutions in (11), the solutions can be written as,

$$(\frac{z_1}{z_{01}})^{s_2 s_3 \cdots s_n} = (\frac{z_2}{z_{02}})^{s_1 s_3 \cdots s_n} = \cdots = (\frac{z_n}{z_{0n}})^{s_1 s_2 \cdots s_{n-1}} \quad (21)$$

where $s_i = \lambda_i d, s_i \in \mathbb{Z}$. If we consider the leftmost equality, we obtain,

$$(\frac{z_1}{z_{01}})^{s_2} - (\frac{z_2}{z_{02}})^{s_1} = 0 \quad (22)$$

To represent the solutions in (11) equivalently with polynomials, we divide the powers of (22) by $c_1 = \gcd(s_1, s_2)$ which yields,

$$z_{f1}^{a_{12}} z_{02}^{a_{11}} - z_{f2}^{a_{11}} z_{01}^{a_{12}} = 0, \quad (23)$$

where a_{11} and a_{12} are defined as in (20). Similarly, considering all the equalities in (21), we can equivalently represent all the possible trajectories of the system with the $n-1$ polynomial equalities defined by (16). Since these polynomial equalities are obtained from the solution (11) of the differential equation (10) , for an initial state $z_0 \in \mathbb{R}^n$,

$z(t)$ is a trajectory generated by the linear system if and only if z_0 and $z(t)$ satisfy the polynomial equalities (16) for all t. Therefore, given two states z_0 and z_f, the set of polynomial equalities (16) is nonempty if and only if there is a trajectory passing from the states z_0 and z_f.

Note that, in the set of polynomial equalities (16) that defines the system trajectories, we eliminate time t. Therefore, if the set defined by polynomial equalities is nonempty for some z_0 and z_f, we cannot conclude if z_f is forward or backward reachable from z_0. We consider the following polynomial function that is transverse to the trajectories of the system (10),

$$p_{tf}(z) = \frac{1}{2}\lambda_1 z_1^2 + \frac{1}{2}\lambda_2 z_2^2 + \cdots + \frac{1}{2}\lambda_n z_n^2 \qquad (24)$$

The time derivative of the function $p_{tf}(z)$ is,

$$\begin{aligned}\frac{\partial p_{tf}(z)}{\partial t} &= \lambda_1 z_1 \dot{z}_1 + \lambda_2 z_2 \dot{z}_2 + \cdots + \lambda_n z_n \dot{z}_n \\ &= \lambda_1^2 z_1^2 + \lambda_2^2 z_2^2 + \cdots + \lambda_n^2 z_n^2\end{aligned}$$

When we exclude the origin point [1], the time derivative of $p_{tf}(z)$ is always greater than zero which means that $p_{tf}(z)$ always increases with time. In other words, $p_{tf}(t_1) > p_{tf}(t_2)$ if and only if $t_1 > t_2$. We know from the monotonicity of the exponential function that $t_1 > t_2$ if and only if $e^{t_1} > e^{t_2}$. Since the states of the system are also exponential functions of time, $p_{tf}(z(t_1)) > p_{tf}(z(t_2))$ if and only if $t_1 > t_2$. Hence, a state z_f is forward reachable from the initial state z_0 at some time $t \geq 0$ if and only if

$$p_{tf}(z_f) - p_{tf}(z_0) \geq 0. \qquad (25)$$

Therefore, given two states z_0 and z_f, z_f is forward reachable from initial state z_0 if and only if the polynomial inequality (25) is satisfied and the set of polynomial equalities (16) is nonempty. Hence, the set defined by polynomial equalities and inequalities in (16), (17), (18) and (19) is empty if and only if $\mathrm{Safe}_+(\Lambda, Z_0, Z_f) = 1$. ■

Remark 3.2: Using similar arguments in the proof, it is straightforward to show that $\mathrm{Safe}_-(\Lambda, Z_0, Z_f) = 1$ if and only if the set defined by polynomial equalities and inequalities in (16), (18), (19) and $p_{tf}(z_f) - p_{tf}(z_0) \leq 0$ is empty.

Remark 3.3: In [15], a qualitative discrete abstraction method is proposed for hybrid systems whose success crucially depends on the choice of seed polynomial set which is used to construct abstraction. Abstraction is done by starting from a set of polynomials and adding the time derivatives of the polynomials in this set until the set saturates. This procedure is not guaranteed to terminate. In this sense, the polynomials in (16) provide useful polynomial seeds for the abstraction. If we consider the polynomial defined in (23), $p(z) = z_{f1}^{a_{12}} z_{02}^{a_{11}} - z_{f2}^{a_{11}} z_{01}^{a_{12}}$, and take the derivative, we get,

$$\frac{dp(z(t))}{dt} = \frac{\lambda_1 \lambda_2 d}{\gcd(\lambda_1, \lambda_2)} p(z(t))$$

Similar analysis can be performed to remaining polynomials in (16). Adding higher order time derivatives of the polynomials does not produce new polynomials and the seed polynomial set saturates. Therefore, the set of polynomials in (16) form a good seed polynomial set for the abstraction.

[1]We exclude the origin in the computations since if initial state is at the origin, then the state will remain at the origin for all time. Conversely, the origin is not reachable from any nonzero state in finite time.

IV. Linear Systems with Purely Imaginary Eigenvalues

In this section, we consider linear systems with purely imaginary eigenvalues which have rational imaginary parts. In this case, we shall transform the systems in modal coordinates. Assuming the matrix A is diagonalizable, the matrix $A \in \mathbb{Q}^{2m\times 2m}$ can be decomposed into block diagonal form by an invertible transformation matrix $T \in \mathbb{Q}^{2m\times 2m}$. If we define a new state vector $z \in \mathbb{R}^n,\ z = Tx$, then we obtain the equivalent linear system

$$\dot{z} = \Lambda z \qquad (26)$$

where $A = T^{-1}\Lambda T$, and $\Lambda \in \mathbb{Q}^{2m\times 2m}$ is a matrix of the form,

$$\begin{bmatrix} \begin{bmatrix} 0 & -\lambda_1 \\ \lambda_1 & 0 \end{bmatrix} & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & \begin{bmatrix} 0 & -\lambda_m \\ \lambda_m & 0 \end{bmatrix} \end{bmatrix} \qquad (27)$$

where eigenvalues of A are $\pm \mathbf{i}\lambda_\mathbf{i}$ and $\lambda_i \in \mathbb{Q}$. Therefore, to any complex conjugate eigenvalue pair there exists a 2-dimensional subspace of the state space.

The differential equations in each 2-dimensional subspace take the form,

$$\begin{bmatrix} \dot{z}_{2i-1} \\ \dot{z}_{2i} \end{bmatrix} = \begin{bmatrix} 0 & -\lambda_i \\ \lambda_i & 0 \end{bmatrix} \begin{bmatrix} z_{2i-1} \\ z_{2i} \end{bmatrix}, \quad i = 1, \ldots, m, \qquad (28)$$

which has the following solution,

$$\begin{aligned} z_{2i-1} &= \cos(\lambda_i t) z_{0,2i-1} - \sin(\lambda_i t) z_{0,2i} \\ z_{2i} &= \sin(\lambda_i t) z_{0,2i-1} + \cos(\lambda_i t) z_{0,2i} \end{aligned} \qquad (29)$$

Theorem 4.1: Given a diagonalizable linear system (A, X_0, X_f) with purely imaginary eigenvalues which have rational imaginary parts, the following statements are equivalent,

1) $\mathrm{Safe}(A, X_0, X_f) = 1$
2) $\mathrm{Safe}(\Lambda, Z_0, Z_f) = 1$
3) The following set defined by polynomial equalities and inequalities is empty for the system in modal coordinates,

$$\begin{aligned} &-z_{f,2i} + y_i z_{0,2i-1} + w_i z_{0,2i} = 0, i = 1, \ldots, m \\ &-z_{f,2i-1} + w_i z_{0,2i-1} - y_i z_{0,2i} = 0, \\ &w_i - f_{\frac{s_i}{c}}(w, y) = 0, i = 1, \ldots, m \\ &y_i - g_{\frac{s_i}{c}}(w, y) = 0, \end{aligned} \qquad (30)$$

$$w^2 + y^2 - 1 = 0,$$
$$p_{zi}(z_0) \geq 0, \quad i = 1, \ldots, m \tag{31}$$
$$p_{zi}(z_f) \geq 0, \quad i = m+1, \ldots, m+k \tag{32}$$

where $\lambda_i = \frac{n_i}{d_i}$ are rationals in reduced form, $n_i \in \mathbb{Z}$, $d_i \in \mathbb{Z}^+$, $d = \prod_{i=1}^n d_i$, $d \in \mathbb{Z}^+$, $s_i = \lambda_i d$, $s_i \in \mathbb{Z}$, $c = \gcd(s_1, \ldots, s_n)$ where gcd denotes the greatest common divisor and $f_\alpha(x, y)$ and $g_\alpha(x, y)$ are polynomial functions defined as [8]

$$\cos(\alpha t) = f_\alpha(\cos t, \sin t), \ \alpha \geq 1 \tag{33}$$
$$\sin(\alpha t) = g_\alpha(\cos t, \sin t), \ \alpha \geq 1 \tag{34}$$

Proof: (1) $\Leftrightarrow$ (2): Since the transformation matrix T is invertible, $\text{Safe}(A, X_0, X_f) = 1$ if and only if $\text{Safe}(\Lambda, Z_0, Z_f) = 1$.

(2) $\Leftrightarrow$ (3): As in Section III, we find the set defined by polynomial equalities that uniquely defines the possible trajectories of the system defined by (26). For simplicity, we assume $\lambda_i \geq 0$. For general case, the proof is similar. We assume that $\lambda_i = \frac{n_i}{d_i}$ are in reduced form with positive denominators. We define $d = \prod_{i=1}^n d_i$ and $s_i = \lambda_i d$. If we consider the equalities in (29) for $i = 1, 2$, we will have terms $\cos(\lambda_1 t), \cos(\lambda_2 t), \sin(\lambda_1 t), \sin(\lambda_2 t)$ in the equalities. Using the change of variables $\tau = \frac{t}{d}$, these terms can be equivalently written as $\cos(s_1\tau), \cos(s_2\tau), \sin(s_1\tau), \sin(s_2\tau)$. If we define $w_i = \cos(\frac{s_i}{c}\tau)$ and $y_i = \sin(\frac{s_i}{c}\tau)$, by denoting $w = \cos(\tau)$ and $y = \sin(\tau)$ we have,

$$w_i = f_{\frac{s_i}{c}}(w, y) \tag{35}$$
$$y_i = g_{\frac{s_i}{c}}(w, y) \tag{36}$$

Note that, we divide the s_i terms by $c = \gcd(s_1, \ldots, s_n)$ to represent the solutions in (29) equivalently with polynomials. By the change of variables $w = \cos(\tau)$ and $y = \sin(\tau)$, using the trigonometric identity $w^2 + y^2 = 1$ and substituting (35) and (36) into (29), we can equivalently express the possible trajectories of the system with the set defined by polynomial equalities in (30).

Since, trajectories of the linear system with purely imaginary eigenvalues are periodic, there is no notion of backward and forward reachability, in fact they are equivalent. Hence, the set defined by polynomial equalities and inequalities in (30), (31) and (32) is empty if and only if $\text{Safe}(\Lambda, Z_0, Z_f) = 1$. ■

Remark 4.2: If we consider the first polynomial defined in (30) and take the second derivative, we obtain,

$$\frac{d^2 p(z(t))}{dt^2} = -\lambda_1^2 p(z(t))$$

Similar to the conclusion in Remark 3.3, the set of polynomials in (30) also form a good seed polynomial set for the abstraction.

V. Linear Systems with Nilpotent System Matrix

In this section, we consider linear systems with nilpotent system matrices. Consider nilpotent system matrix $A \in \mathbb{Q}^{n\times n}$ where $A^n = 0$. Using the series for the matrix exponential, we can write $x(t) = e^{At}x_0$ which is the solution of the differential equation (1) as,

$$\begin{aligned} x_i(t) &= \sum_{j=1}^{n} (\sum_{k=0}^{n-1} \frac{t^k}{k!} A^k)_{ij} x_{0j} \\ &= \sum_{k=0}^{n-1} f_{ik}(x_0) t^k \end{aligned} \tag{37}$$

where $f \in \mathbb{Q}^{n\times n}$ is the matrix whose entry ik is the coefficient of the polynomial term t^k of the state x_i.

We consider the sets of initial and final states as semialgebraic sets defined in (3) and (4).

Theorem 5.1: Given a linear system (A, X_0, X_f) with nilpotent system matrix A, $\text{Safe}_+(A, X_0, X_f) = 1$ if and only if the following set is empty,

$$\begin{aligned} -x_{fi} + \textstyle\sum_{k=0}^{n-1} f_{ik}(x_0) t^k &= 0 \\ p_i(x_0) &\geq 0 \qquad i = 1, \ldots, m \\ p_i(x_f) &\geq 0 \qquad i = m+1, \ldots, m+k \\ t &\geq 0 \end{aligned} \tag{38}$$

where $f \in \mathbb{Q}^{n\times n}$ is the matrix whose entry ik is the coefficient of the polynomial term t^k of the state x_{fi}.

Proof: Trajectories of the system can be written as a set defined by polynomial equalities in (37). Therefore, given two states x_0 and x_f, the set in (37) is nonempty if and only if there is a trajectory passing from the states z_0 and z_f. Moreover, x_f is forward reachable from initial state x_0 if and only if $t \geq 0$. Hence, the set in (38) is empty if and only if $\text{Safe}_+(A, X_0, X_f) = 1$. ■

Remark 5.2: It is straightforward to show that $\text{Safe}_-(A, X_0, X_f) = 1$ if and only if the set defined in (38) is empty when the time constraint is $-t \geq 0$.

VI. Sum of Squares Decomposition

The results we have so far indicate clearly the importance of proving set emptiness to verify system safety. Now we will give a brief outline of a method based on sum of squares (SOS) decomposition and semidefinite programming for proving that a basic semialgebraic set is empty. Readers are referred to [11], [12] for more details.

A multivariate polynomial $f(x)$ is a *sum of squares* if it can be written as $f(x) = \sum_{i=1}^m f_i^2(x)$ for some polynomials $f_i(x)$, $i = 1, ..., m$. The condition that $f(x) = \sum_{i=1}^m f_i^2(x)$ is equivalent to the existence of a positive semidefinite matrix Q such that $f(x) = Z^T(x)QZ(x)$ for some vector of monomials $Z(x)$. Here we may choose $Z(x)$ to consist of all monomials whose degrees are at most equal to $\deg(f(x))/2$. Thus, checking if a polynomial is a sum of squares amounts to finding $Q \geq 0$ that at the same time satisfies the equation above, which is a semidefinite programming feasibility problem.

For presenting the method that can prove emptiness of semialgebraic sets, we need the following definitions from polynomial algebra.

Definition 6.1: Given a finite set of polynomials $\{p_i(x)\}$, the *ideal* $I(p_i)$ generated by $\{p_i(x)\}$ is

$$I(p_i) = \left\{ \sum_i a_i p_i \mid a_i \text{ are polynomials for all } i \right\}$$

Definition 6.2: Given a finite set of polynomials $\{p_i(x)\}$, the *multiplicative monoid* generated by $\{p_i(x)\}$, which is denoted by $M(p_i)$, is the set of finite products of elements p_i, including the empty product (the identity).

The following is an equivalent characterization of a *cone* generated by a finite set of polynomials in the polynomial ring.

Definition 6.3: Given a finite set of polynomials $\{p_i(x)\}$, the *cone* generated by $\{p_i(x)\}$, which is denoted by $P(p_i)$, is

$$P(p_i) = \{ \quad a + \sum_{j=1}^{k} b_j q_j \mid a, b_j \text{ are sums of squares}, \\ q_j \in M(p_i) \text{ for } j = 1, ..., k\}$$

All the above definitions are used in the *Positivstellensatz* [13], a central result from real algebraic geometry. The theorem provides a characterization of *infeasibility certificates* for real solutions of systems of polynomial equalities and inequalities.

Theorem 6.4 (Positivstellensatz): Let f_j, g_k be finite sets of polynomials in x. Then the following are equivalent:

1) The following set is empty,

$$\{x \in \mathbb{R}^n \mid f_j(x) \geq 0, g_k(x) = 0, \ \forall j, k\} \tag{39}$$

2) There exist $f \in P(f_j)$, $g \in I(g_k)$ such that

$$f + g + 1 = 0. \tag{40}$$

It has been recently shown [11] that Positivstellensatz refutations (i.e., f, g that satisfy (40)) can be computed using hierarchies of semidefinite programming. The idea is to choose a degree bound for the polynomials, and then affinely parameterize a family of candidate f and g. This converts the problem into a sum of squares feasibility problem. For example, the software SOSTOOLS [12] can be used to compute suitable polynomials f and g which prove that (39) is empty. This provides a hierarchy of safety certificates for the exact safety verification problem.

VII. Illustrative Examples

A. Linear Systems with Rational Eigenvalues

Consider the 2-dimensional linear system (A, X_0, X_f),

$$A = \begin{bmatrix} 2 & 2 \\ 1 & 3 \end{bmatrix}, \ H_f x_f \geq h_f, \ H_0 x_0 \geq h_0, \tag{41}$$

where

$$H_f, H_0 = \begin{bmatrix} -\frac{1}{3} & \frac{4}{3} \\ \frac{1}{3} & -\frac{4}{3} \\ -1 & 0 \\ 1 & 0 \end{bmatrix} \ h_f = \begin{bmatrix} 1 \\ -2 \\ 4 \\ -6 \end{bmatrix} \ h_0 = \begin{bmatrix} -1 \\ 2 \\ 10 \\ -12 \end{bmatrix}$$

and the matrix A has rational eigenvalues $\lambda_1 = 1$ and $\lambda_2 = 4$.

If we transform the linear system (A, X_0, X_f) into eigenspace by the transformation matrix $T = \begin{bmatrix} -\frac{2}{3} & \frac{2}{3} \\ -\frac{1}{3} & -\frac{2}{3} \end{bmatrix}$ we have (Λ, Z_0, Z_f) as,

$$\Lambda = \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix}, \ \bar{H}_f z_f \geq \bar{h}_f, \ \bar{H}_0 z_0 \geq \bar{h}_0, \tag{42}$$

where

$$\bar{H}_f, \bar{H}_0 = \begin{bmatrix} 1 & -1 \\ -1 & 1 \\ 1 & 1 \\ -1 & -1 \end{bmatrix}, \bar{h}_f = \begin{bmatrix} 1 \\ -2 \\ 4 \\ -6 \end{bmatrix}, \bar{h}_0 = \begin{bmatrix} -1 \\ 2 \\ 10 \\ -12 \end{bmatrix}.$$

Then, the set defined in (16), (17), (18) and (19) becomes,

$$\begin{aligned} z_{f1}^2 + 4z_{f2}^2 - z_{01}^2 - 4z_{02}^2 &\geq 0 \\ z_{f1}^4 z_{02} - z_{f2} z_{01}^4 &= 0 \\ z_{01} - z_{02} + 1 &\geq 0 \\ -z_{01} + z_{02} - 2 &\geq 0 \\ z_{01} + z_{02} - 10 &\geq 0 \\ -z_{01} - z_{02} + 12 &\geq 0 \\ z_{f1} - z_{f2} - 1 &\geq 0 \\ -z_{f1} + z_{f2} + 2 &\geq 0 \\ z_{f1} + z_{f2} - 4 &\geq 0 \\ -z_{f1} - z_{f2} + 6 &\geq 0 \end{aligned}$$

Performing SOS decomposition test returns that the solution to above set is empty. Hence $\text{Safe}_+(A, X_0, X_f) = 1$. The required CPU time for computation is 0.65 seconds.

B. Linear Systems with Purely Imaginary Eigenvalues

Consider the 2-dimensional linear system (A, X_0, X_f),

$$A = \begin{bmatrix} 0 & 1 \\ -9 & 0 \end{bmatrix}, \ H_f x_f \geq h_f, \ H_0 x_0 \geq h_0, \tag{43}$$

where

$$H_f, H_0 = \begin{bmatrix} 3 & -1 \\ -3 & 1 \\ 3 & 1 \\ -3 & -1 \end{bmatrix}, h_f = \begin{bmatrix} -1 \\ 2 \\ 10 \\ -12 \end{bmatrix}, h_0 = \begin{bmatrix} 1 \\ -2 \\ 4 \\ -6 \end{bmatrix},$$

and the matrix A has purely imaginary eigenvalues $\lambda_1 = \mathbf{i}3$ and $\lambda_2 = -\mathbf{i}3$. If we transform the linear system (A, X_0, X_f) into modal coordinates by the transformation matrix $T = \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix}$, we have (Λ, Z_0, Z_f) as,

$$\Lambda = \begin{bmatrix} 0 & -3 \\ 3 & 0 \end{bmatrix}, \ \bar{H}_f z_f \geq \bar{h}_f, \ \bar{H}_0 z_0 \geq \bar{h}_0, \tag{44}$$

where

$$\bar{H}_f, \bar{H}_0 = \begin{bmatrix} 1 & -1 \\ -1 & 1 \\ 1 & 1 \\ -1 & -1 \end{bmatrix}, \bar{h}_f = \begin{bmatrix} -1 \\ 2 \\ 10 \\ -12 \end{bmatrix}, \bar{h}_0 = \begin{bmatrix} 1 \\ -2 \\ 4 \\ -6 \end{bmatrix}.$$

We choose $w = \cos(3t)$ and $y = \sin(3t)$, then the set

defined in (30), (31) and (32) becomes,

$$\begin{aligned} -z_{f1} + wz_{01} - yz_{02} &= 0 \\ -z_{f2} + yz_{01} + wz_{02} &= 0 \\ w^2 + y^2 - 1 &= 0 \\ z_{01} - z_{02} - 1 &\geq 0 \\ -z_{01} + z_{02} + 2 &\geq 0 \\ z_{01} + z_{02} - 4 &\geq 0 \\ -z_{01} - z_{02} + 6 &\geq 0 \\ z_{f1} - z_{f2} + 1 &\geq 0 \\ -z_{f1} + z_{f2} - 2 &\geq 0 \\ z_{f1} + z_{f2} - 10 &\geq 0 \\ -z_{f1} - z_{f2} + 12 &\geq 0 \end{aligned}$$

SOS decomposition test returns that $\mathrm{Safe}_+(A, X_0, X_f) = 1$. The required CPU time for computation is 0.26 seconds.

C. Linear Systems with Nilpotent System Matrices

Consider the 3-dimensional linear system (A, X_0, X_f) where the matrix A is nilpotent,

$$A = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \; H_f x_f \geq h_f, \; H_0 x_0 \geq h_0, \qquad (45)$$

where

$$H_f = \begin{bmatrix} 1 & -1 & 0 \\ -1 & 1 & 0 \\ 1 & 1 & 0 \\ -1 & -1 & 0 \end{bmatrix}, H_0 = \begin{bmatrix} 1 & -1 & 0 \\ -1 & 1 & 0 \\ 1 & 1 & 0 \\ -1 & -1 & 0 \end{bmatrix},$$

$h_f = [2, -6, 10, -12]^T$, $h_0 = [1, -2, 4, -6]^T$. Then the set defined in (38) becomes,

$$\begin{aligned} -x_{f1} + \tfrac{1}{2}x_{03}t^2 + (x_{03} + x_{02})t + x_{01} &= 0 \\ -x_{f2} + x_{03}t + x_{02} &= 0 \\ -x_{f3} + x_{03} &= 0 \\ x_{01} - x_{02} - 2 &\geq 0 \\ -x_{01} + x_{02} + 6 &\geq 0 \\ x_{01} + x_{02} - 10 &\geq 0 \\ -x_{01} - x_{02} + 12 &\geq 0 \\ x_{f1} - x_{f2} - 1 &\geq 0 \\ -x_{f1} + x_{f2} + 2 &\geq 0 \\ x_{f1} + x_{f2} - 4 &\geq 0 \\ -x_{f1} - x_{f2} + 6 &\geq 0 \\ t &\geq 0 \end{aligned}$$

SOS decomposition test returns that $\mathrm{Safe}_+(A, X_0, X_f) = 1$. The required CPU time for computation is 8 seconds.

Remark 7.1: Theorems 3.1, 4.1, and 5.1 provide *theoretical* procedures for exact safety verification. On the other hand, SOS decomposition *theoretically* provides hierarchies of infeasibility certificates. Since, there is no a priori bound on the degree of the certificate, the search may not be computationally feasible. Hence, failure of the SOS test in practice does not mean that the system is not safe.

VIII. Conclusion

In this paper, we converted the exact safety verification of linear dynamical systems with certain eigen-structure to an emptiness of a set defined by polynomial equalities and inequalities. Emptiness of such a set can be checked using SOS decomposition. Such decomposition can effectively be computed by semidefinite programming which promises to be a scalable solution to the exact verification problem. Also, it was shown that such polynomial sets are good seeds for the abstraction of hybrid systems with linear dynamics.

IX. Acknowledgments

We thank Ashish Tiwari for very useful comments on this paper and discussions on safety of hybrid systems.

References

[1] E. M. Clarke and R. P. Kurshan, "Computer-aided verification," *IEEE Spectrum*, vol. 33, no. 6, pp. 61–67, 1996.

[2] A. Chutinan and B. H. Krogh, "Computational techniques for hybrid system verification," *IEEE Transactions on Automatic Control*, vol. 48, no. 1, pp. 64–75, Jan. 2003.

[3] T. Dang and O. Maler, "Reachability analysis via face lifting," in *Hybrid Systems : Computation and Control*, ser. Lecture Notes in Computer Science, T. Henzinger and S. Sastry, Eds. Berlin: Springer Verlag, 1998, vol. 1386, pp. 96–109.

[4] A. Kurzhanski and P. Varaiya, "Ellipsoidal techniques for reachability analysis," in *Hybrid Systems : Computation and Control*, ser. Lecture Notes in Computer Science, B. Krogh and N. Lynch, Eds. Springer Verlag, 2000, vol. 1790, pp. 203–213.

[5] I. Mitchell and C. Tomlin, "Level set methods for computation in hybrid systems," in *Hybrid Systems : Computation and Control*, ser. Lecture Notes in Computer Science, B. Krogh and N. Lynch, Eds. Springer Verlag, 2000, vol. 1790, pp. 310–323.

[6] H. Yazarel and G. J. Pappas, "Geometric programming relaxations for linear system reachability," in *Proceedings of 2004 American Control Conference, ACC'04*, Boston, MA, USA, June 2004.

[7] H. Anai and V. Weispfenning, "Reach set computations using real quantifier elimination," in *Hybrid Systems : Computation and Control*, ser. Lecture Notes in Computer Science, M. D. D. Benedetto and A. L. Sangiovanni-Vincentelli, Eds. Springer Verlag, 2001, vol. 2034, pp. 63–76.

[8] G. Lafferriere, G. J. Pappas, and S. Yovine, "Symbolic reachability computations for families of linear vector fields," *Journal of Symbolic Computation*, vol. 32, no. 3, pp. 231–253, September 2001.

[9] A. Tiwari, "Approximate reachability for linear systems," in *Hybrid Systems: Computation and Control*, ser. Lecture Notes in Computer Science, O. Maler and A. Pnueli, Eds., vol. 2623. Springer-Verlag, Apr. 2003, pp. 514–525.

[10] A. Tarski, *A decision method for elementary algebra and geometry*, 2nd ed. University of California Press, 1951.

[11] P. A. Parrilo, "Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization," Ph.D. dissertation, California Institute of Technology, 2000.

[12] S. Prajna, A. Papachristodoulou, and P. A. Parrilo, "IntroducingSOSTOOLS: A general purpose sum of squares programming solver," in *Proceedings of the 2002 IEEE Conference on Decision and Control*, Las Vegas, Nevada, USA, Dec. 2002. Available at http://www.cds.caltech.edu/sostools and http://www.aut.ee.ethz.ch/˜parrilo/sostools.

[13] G. Stengle, "A nullstellensatz and a positivstellensatz in semialgebraic geometry," Math. Ann., vol. 207, pp. 87–97, 1974.

[14] S. Prajna and A. Jadbabaie, "Safety verification of hybrid systems using barrier certificates," in *Hybrid Systems : Computation and Control*, ser. Lecture Notes in Computer Science, R. Alur and G. J. Pappas, Eds. Philadelphia, PA, USA: Springer Verlag, March 2004.

[15] A. Tiwari and G. Khanna, "Series of abstractions for hybrid automata," in *Hybrid Systems : Computation and Control*, ser. Lecture Notes in Computer Science, C. Tomlin and M. Greenstreet, Eds., vol. 2289. Stanford, CA, USA: Springer Verlag, April 2002.