June 2004

Geometric Programming Relaxations for Linear System Reachability

Hakan Yazarel
University of Pennsylvania

George J. Pappas
University of Pennsylvania, pappasg@seas.upenn.edu

Reprinted from *Proceedings of the 2004 American Control Conference*, Volume 1, pages 553-559.

Geometric Programming Relaxations for Linear System Reachability

Abstract
One of the main obstacles in the safety analysis of continuous and hybrid systems has been the computation of the reachable set for continuous systems in high dimensions. In this paper, we present a novel method that exploits the structure of linear dynamical systems, and the monotonicity of the exponential function in order to obtain safety certificates of continuous linear systems. By over-approximating the sets of initial and final states, the safety verification problem is expressed as a series of geometric programs which can be further transformed into linear programs. This provides the ability to verify the safety properties of high dimensional linear systems with realistic computation times. In addition, our optimization based formulation computes time intervals over which the system is safe and unsafe.

Comments
Reprinted from *Proceedings of the 2004 American Control Conference*, Volume 1, pages 553-559.

Proceeding of the 2004 American Control Conference
Boston, Massachusetts June 30 - July 2, 2004

Geometric Programming Relaxations for Linear System Reachability

Hakan Yazarel and George J. Pappas

Abstract— **One of the main obstacles in the safety analysis of continuous and hybrid systems has been the computation of the reachable set for continuous systems in high dimensions. In this paper, we present a novel method that exploits the structure of linear dynamical systems, and the monotonicity of the exponential function in order to obtain safety certificates of continuous linear systems. By over-approximating the sets of initial and final states, the safety verification problem is expressed as a series of geometric programs which can be further transformed into linear programs. This provides the ability to verify the safety properties of high dimensional linear systems with realistic computation times. In addition, our optimization based formulation computes time intervals over which the system is safe and unsafe.**

I. Introduction

The safety (or reachability) problem asks whether a set of unsafe (final) states is reachable from a set of initial states while satisfying the system dynamics. This is a problem that even for linear systems of the form $\dot{x} = Ax$ has clearly escaped analytic solution. Furthermore, exact or approximate computational approaches have been quite expensive, and, therefore, limited to systems of small dimension. This has constrained the verification of hybrid systems to systems that do not exceed three or four continuous variables.

Computing the exact reachable set for linear systems starting in a semi-algebraic set is possible under certain eigen-structure conditions [1], [2], by relying on expensive quantifier elimination techniques [3]. In [4], quantifier elimination techniques coupled with understanding of linear system eigenstructure resulted in over-approximating the reachable set for linear systems with almost arbitrary eigenstructure.

Methods for exact computation of reachable sets should be contrasted with *approximate* methods, which over- or under-approximate reachable sets using a variety of set representations such as polyhedra, level sets, or ellipsoids. Approximate reachability computations rely on numerical methods for Hamilton-Jacobi equations [5], ellipsoidal calculus [6], flow-pipe approximations [7], and polygonal computations [8]. As a result, approximate methods are, in principle, applicable to larger classes of continuous systems. However, the encoding complexity of set representation, and computational complexity of numerical reachability techniques make these approaches very valuable and precise, but for small dimensional systems.

In this paper, we are interested in the following safety (reachability) problems for linear dynamical systems of the form $\dot{x} = Ax$ where state $x \in \mathbb{R}^n$.

Problem 1.1: (Safety verification) Given a linear system and two polyhedral sets X_0 and X_f, determine if system trajectories starting in X_0 can ever reach X_f.

Solutions to the above problem can be used to prove that a certain set can be reached or avoided. They can also be used to provide refutation for counter-example guided predicate abstraction techniques for hybrid systems [9]. The following problem also extracts some timing information regarding reachability.

Problem 1.2: (Timing verification) Given a linear system and two polyhedral sets X_0 and X_f, compute the minimum and maximum amount of time it takes to reach X_f from X_0.

Solutions to the above problem extract timing information that would be critical in abstracting dynamical systems by simple timing intervals. A solution to the above problem would also allow abstracting hybrid systems with linear dynamics by timed automata [10], enabling the verification of temporal properties of hybrid systems.

In order to address the above problems for high dimensional systems, we use a combination of optimization techniques, in particular linear, geometric, quadratic, and fractional programming which are known to be very scalable. By over-approximating polyhedral initial and final states in modal or polar coordinates, the safety verification problem is written as a series of geometric programs which can be further transformed into linear programs. This provides the ability to address the above problems for high-dimensional linear systems with realistic computation times.

II. Safety Analysis of Linear Systems

We consider linear systems of the form,

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

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

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

In this paper, we are considering *polyhedral* sets of initial and final states X_0 and X_f, defined as,

$$X_0 = \{x_0 \in \mathbb{R}^n \mid H_0 x_0 \leq h_0\}, \tag{3}$$

$$X_f = \{x_f \in \mathbb{R}^n \mid H_f x_f \leq h_f\}, \tag{4}$$

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

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

0-7803-8335-4/04/$17.00 ©2004 AACC

where $H_0 \in \mathbb{R}^{k\times n}$, $H_f \in \mathbb{R}^{l\times n}$, $h_0 \in \mathbb{R}^k$ and $h_f \in \mathbb{R}^l$. Given a set of initial states X_0, the reach set of the linear system (1) on the time interval $[t_0, t_f]$ is defined as,

$$\begin{aligned}\text{Reach}_{[t_0,t_f]}(A, X_0) = \{x_f \in \mathbb{R}^n \mid \exists t\ \exists x_0 :\\ t_0 \le t \le t_f \ \wedge\ x_0 \in X_0 \wedge x_f = e^{At}x_0\}.\end{aligned} \tag{5}$$

The set of all forward reachable states is simply $\text{Reach}_{[0,+\infty)}(A, X_0)$. Given a set of final or unsafe states X_f, we define the safety predicate on $[t_0, t_f]$ as,

$$\text{Safe}_{[t_0,t_f]}(A, X_0, X_f) = \begin{cases} 1 & \text{if Reach}_{[t_0,t_f]}(A, X_0) \cap X_f = \emptyset \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

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

Problem 2.1: (Safety verification) Given a linear system (A, X_0, X_f), determine if $\text{Safe}_{[0,+\infty)}(A, X_0, X_f) = 1$.

Problem 2.2: (Timing verification) Given a linear system (A, X_0, X_f), if $\text{Safe}_{[0,+\infty)}(A, X_0, X_f) = 0$, then compute a time interval $[T_{\min}, T_{\max}]$ so that

$$\begin{aligned}\text{Safe}_{[0,T_{\min}]}(A, X_0, X_f) &= 1\\ \text{Safe}_{[T_{\min},T_{\max}]}(A, X_0, X_f) &= 0\\ \text{Safe}_{[T_{\max},+\infty)}(A, X_0, X_f) &= 1\end{aligned}$$

Computing such a time interval $[T_{\min}, T_{\max}]$ exactly is possible if the linear system (A, X_0, X_f) has a certain structure [1], [2]. Approximate answers rely on the following straightforward proposition.

Proposition 2.3: Given linear system and sets (A, X_0, X_f), consider $(A, \hat{X}_0, \hat{X}_f)$ where $X_0 \subseteq \hat{X}_0$ and $X_f \subseteq \hat{X}_f$. Then,

$$\begin{aligned}&\text{Safe}_{[T^*_{\min},T^*_{\max}]}(A, \hat{X}_0, \hat{X}_f) = 1\\ &\quad \Rightarrow \text{Safe}_{[T^*_{\min},T^*_{\max}]}(A, X_0, X_f) = 1\end{aligned} \tag{7}$$

$$\begin{aligned}&\text{Safe}_{[0,+\infty)}(A, \hat{X}_0, \hat{X}_f) = 1\\ &\quad \Rightarrow \text{Safe}_{[0,+\infty)}(A, X_0, X_f) = 1\end{aligned} \tag{8}$$

where $[T^*_{\min}, T^*_{\max}]$ is an over-approximate time interval such that $T^*_{\min} \le T_{\min} \le T_{\max} \le T^*_{\max}$.

A. System decomposition

Our solutions to the above problems rely on the well-known decomposition of linear systems in modal coordinates. Throughout the paper, it is assumed that system matrix A is diagonalizable, therefore A can be written as,

$$A = T^{-1}\Lambda T, \tag{9}$$

where $\Lambda \in \mathbb{C}^{n\times n}$ is a diagonal matrix whose diagonal entries are eigenvalues of matrix A, and $T \in \mathbb{C}^{n\times n}$ is an invertible transformation matrix. By the complex conjugate symmetry property of matrices with real entries, eigenvalues of the system matrix A can be written as,

$$\lambda_i = a_i + jw_i, \quad i = 1, \ldots, m, \tag{10}$$

$$\bar{\lambda}_i = a_i - jw_i, \quad i = 1, \ldots, m, \tag{11}$$

$$\lambda_i = a_i, \quad i = 2m+1, \ldots n, \tag{12}$$

where a_i are the real and w_i are the imaginary parts of the eigenvalues λ_i. Since the matrix A is diagonalizable, the linear system (1) can be decomposed as,

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \tag{13}$$

so that eigenvalues of $A_1 \in \mathbb{R}^{(n-2m)\times(n-2m)}$ are the real eigenvalues in (12) and eigenvalues of $A_2 \in \mathbb{R}^{2m\times 2m}$ are the complex conjugate pairs in (10) and (11).

III. Linear Systems with Real Eigenvalues

In this section, we consider linear systems with real eigenvalues. We first transform the system in modal or eigen-coordinates. Note that, throughout the paper, we use the notation $\min / \max f(x)$ to express that the minimum and maximum values of the function $f(x)$ are computed subject to the same constraints.

A. Transforming the system in eigen-coordinates

Assuming the matrix A is diagonalizable, we have, $A = T^{-1}\Lambda T$ where $T \in \mathbb{R}^{n\times n}$ is an invertible transformation matrix whose columns are left eigenvectors of A and $\Lambda \in \mathbb{R}^{n\times n}$ is a diagonal matrix whose diagonal entries are eigenvalues of matrix A. If we define a new state vector $z \in \mathbb{R}^n$, $z = Tx$, then we obtain the following equivalent differential equation and its solution,

$$\dot{z} = \Lambda z, \qquad z_i(t) = e^{\lambda_i t} z_{0i}, \quad i = 1, \ldots, n, \tag{14}$$

where λ_i are the eigenvalues of the system matrix A and $z_0 = Tx_0$ is the initial state vector. Hence, by the transformation $z = Tx$, we break the verification problem of the linear system $\dot{x} = Ax$ into verification problems of multiple 1-dimensional linear systems.

The transformed states and the sets in eigen-coordinates are as follows,

$$z_0 = Tx_0,\ Z_0 = \{z_0 : z_0 = Tx_0,\ x_0 \in X_0\}, \tag{15}$$

$$z_f = Tx_f,\ Z_f = \{z_f : z_f = Tx_f,\ x_f \in X_f\}, \tag{16}$$

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 defined in (3) and (4) respectively.

In order to compute time intervals for safety certificates, we project the sets Z_0 and Z_f on each eigendirection. This is easily performed by the following linear programs,

$$\begin{array}{llll} \text{min/max} & z_{0i} & \text{min/max} & z_{fi}, \\ \text{s.t.} & z_0 = Tx_0 & \text{s.t.} & z_f = Tx_f \\ & H_0x_0 \le h_0 & & H_fx_f \le h_f \end{array} \tag{17}$$

This projection yields the over-approximated sets in eigenspace as,

$$\hat{Z}_0 = \{z_0 | z_0^L \le z_0 \le z_0^U\}, \tag{18}$$

$$\hat{Z}_f = \{z_f | z_f^L \le z_f \le z_f^U\}, \tag{19}$$

where z_0^L, z_f^L are the lower bound vectors and z_0^U, z_f^U are the upper bound vectors of initial state vector z_0 and

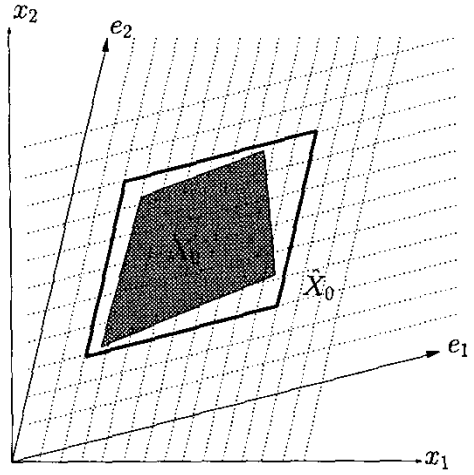

Fig. 1. Over-approximation in state space

final state vector z_f in eigenspace respectively. For a 2-dimensional system, the over-approximation in state space is illustrated in Figure 1 where x_1 and x_2 are the original coordinates, e_1 and e_2 are the eigenvectors, X_0 is the original set and $\hat{X}_0$ is the over-approximated set such that $X_0 \subseteq \hat{X}_0$.

Therefore, we have the over-approximation of the system (Λ, Z_0, Z_f) as $(\Lambda, \hat{Z}_0, \hat{Z}_f)$ which is n 1-dimensional linear systems,

$$z_{fi} = e^{\lambda_i t} z_{0i}, \quad i = 1, \ldots, n, \tag{20}$$

$$z_0^L \leq z_0 \leq z_0^U, \tag{21}$$

$$z_f^L \leq z_f \leq z_f^U. \tag{22}$$

We compute time intervals for each 1-dimensional subsystem and intersect the results to obtain the general solution. For the verification of each 1-dimensional subsystem, we have three cases in the analysis,

Case 1: $z_{0i}^L, z_{0i}^U, z_{fi}^L, z_{fi}^U > 0$ or $z_{0i}^L, z_{0i}^U, z_{fi}^L, z_{fi}^U < 0$: We compute the time interval $[t^i_{\min}, t^i_{\max}]$ for the 1-dimensional subsystem i as

$$t^i_{\min} = \min\{\frac{1}{\lambda_i}\log(\frac{z_{fi}^L}{z_{0i}^U}), \frac{1}{\lambda_i}\log(\frac{z_{fi}^U}{z_{0i}^L})\} \tag{23}$$

$$t^i_{\max} = \max\{\frac{1}{\lambda_i}\log(\frac{z_{fi}^L}{z_{0i}^U}), \frac{1}{\lambda_i}\log(\frac{z_{fi}^U}{z_{0i}^L})\} \tag{24}$$

If $t^i_{\max} < 0$ then we can conclude that the set of final states of subsystem i is not forward reachable from the set of initial states and therefore $\text{Safe}_{[0,+\infty)}(A, X_0, X_f) = 1$.

Case 2: $z_{0i}^L, z_{0i}^U < 0, z_{fi}^L, z_{fi}^U > 0$ or $z_{0i}^L, z_{0i}^U > 0, z_{fi}^L, z_{fi}^U < 0$: Since, when the eigenvalue is real, a final state in negative (positive) orthant is not reachable from an initial state in positive (negative) orthant, we can immediately conclude that 1-dimensional subsystem i is safe and therefore $\text{Safe}_{[0,+\infty)}(A, X_0, X_f) = 1$.

Case 3: *Otherwise:* We explain this case by an example. Consider the case where $z_{0i}^L \leq 0 < z_{0i}^U$ and $z_{fi}^L, z_{fi}^U > 0$. We split the initial set of states into two subsets each of which are defined in negative orthant of the eigenspace as $z_{0i}^L \leq z_{0i} < 0$ and positive orthant of the eigenspace as $0 < z_{0i} \leq z_{0i}^U$. Since 1-dimensional final set of states is not reachable from the states that belong to the subset in the negative orthant $z_{0i}^L \leq z_{0i} < 0$, it's sufficient to verify the subsystem i for the subset $0 < z_{0i} \leq z_{0i}^U$. The rest of the verification can be done as in case 1.

Remark: Note that, a safety certificate for any 1-dimensional subsystem i is a sufficient safety certificate for the overall system.

B. Illustrative Example

Consider the 2-dimensional system matrix,

$$A = \begin{bmatrix} -2 & -2 \\ -1 & -3 \end{bmatrix} \tag{25}$$

with real eigenvalues $\lambda_1 = -1$ and $\lambda_2 = -4$. Consider the polyhedral sets of initial and final states defined in positive orthant defined as in (3) and (4) where

$$H_f, H_0 = \begin{bmatrix} -1 & 1 \\ 1 & -1 \\ -1 & -1 \\ 1 & 1 \end{bmatrix}, h_f = \begin{bmatrix} -1 \\ 2 \\ -16 \\ 18 \end{bmatrix}, h_0 = \begin{bmatrix} -1 \\ 2 \\ -4 \\ 6 \end{bmatrix}.$$

Performing the linear programs defined in (17) yields the following bounds for the states in eigenspace z_0 and z_f,

$$0.6667 \leq z_{01} \leq 1.3334, \quad 0.6667 \leq z_{f1} \leq 1.3334$$
$$7.6667 \leq z_{02} \leq 8.8333, \quad 1.6667 \leq z_{f2} \leq 2.8333$$

For the first 1-dimensional subsystem $z_{f1} = e^{-t} z_{01}$, the time interval is calculated as $[0, 0.6931]$. For the second 1-dimensional subsystem $z_{f2} = e^{-4t} z_{02}$, the time interval is calculated as $[0.2488, 0.4169]$. The intersection of two time intervals is $[T^*_{\min}, T^*_{\max}] = [0.2488, 0.4169]$. Therefore,

$$\begin{aligned} \text{Safe}_{[0, T^*_{\min}]}(A, X_0, X_f) &= 1 \\ \text{Safe}_{[T^*_{\min}, T^*_{\max}]}(A, X_0, X_f) &= 0 \\ \text{Safe}_{[T^*_{\max}, +\infty)}(A, X_0, X_f) &= 1 \end{aligned}$$

by Proposition 2.3. The required CPU time for the computation is 0.13 seconds.

C. High Dimensional Verification

We implemented our method presented in Section III using MATLAB. The results, performed on a laptop which has an Intel Pentium-4 2.4GHz processor and 512 MB RAM, are given in the following table.

System Dimension	*System Safe?*	*Compute Time (sec)*	$T^*_{\min}$ *(sec)*	$T^*_{\max}$ *(sec)*
5	No	0.35	0.6453	1.4232
5	Yes	0.29		
10	No	0.86	0.3278	1.2924
10	Yes	0.8		
100	Yes	351.73		

Table 1 - Safety computation results

Note that the majority of the computation is done in computing over-approximations of the initial and final states in modal coordinates using linear programs.

IV. Linear Systems with Complex Eigenvalues

In this section, we consider linear systems with complex eigenvalues. In this case, we shall transform the systems in polar coordinates.

A. Transforming the optimization in polar coordinates

The matrix $A \in \mathbb{R}^{2m\times 2m}$ can be decomposed into block diagonal form by an invertible transformation matrix $T \in \mathbb{R}^{2m\times 2m}$. If we define a new state vector $z \in \mathbb{R}^{2m}$, $z = Tx$, then we obtain the equivalent linear system $\dot{z} = \Lambda z$ where $A = T^{-1}\Lambda T$, and $\Lambda \in \mathbb{R}^{2m\times 2m}$ is a matrix of the form,

$$\begin{bmatrix} \begin{bmatrix} a_1 & -w_1 \\ w_1 & a_1 \end{bmatrix} & & 0 \\ & \ddots & \\ 0 & & \begin{bmatrix} a_m & -w_m \\ w_m & a_m \end{bmatrix} \end{bmatrix} \tag{26}$$

where a_i and w_i are real and imaginary parts of the eigenvalues λ_i defined in (10) and (11). Therefore, for any complex conjugate eigenvalue pair $(\lambda_i, \overline{\lambda_i})$ there exists a 2-dimensional subspace of the state space. The differential equations in each 2-dimensional subspace take the form,

$$\begin{bmatrix} \dot{z}_{2i-1} \\ \dot{z}_{2i} \end{bmatrix} = \begin{bmatrix} a_i & -w_i \\ w_i & a_i \end{bmatrix} \begin{bmatrix} z_{2i-1} \\ z_{2i} \end{bmatrix}, \quad i = 1,\ldots,m, \tag{27}$$

which can be transformed (and solved) in polar coordinates[1],

$$\dot{\rho}_i = a_i\rho_i \quad \rho_i(t) = e^{a_i t}\rho_{0i}, \quad i = 1,\ldots,m, \tag{28}$$

$$\dot{\theta}_i = w_i, \quad \theta_i(t) = \theta_{0i} + w_i t, \quad i = 1,\ldots,m, \tag{29}$$

where ρ_i is the radial coordinate, and θ_i is the angular coordinate of polar space. Hence, by the transformation $z = Tx$ and further transformation to polar coordinates, we break the verification problem of the linear system $\dot{x} = Ax$ into verification problems of multiple 2-dimensional linear systems.

Transformed sets of initial and final states in polar coordinates are as follows,

$$P_0 = \{\rho_0 \mid \rho_{0i} = z_{0,(2i-1)}^2 + z_{0,(2i)}^2,\ i = 1,\ldots,m, \quad z_0 = Tx_0,\ x_0 \in X_0\}, \tag{30}$$

$$P_f = \{\rho_f \mid \rho_{fi} = z_{f,(2i-1)}^2 + z_{f,(2i)}^2,\ i = 1,\ldots,m, \quad z_f = Tx_f,\ x_f \in X_f\}, \tag{31}$$

$$\Theta_0 = \{\theta_0 \mid \theta_{0i} = \tan^{-1}\frac{z_{0,(2i)}}{z_{0,(2i-1)}},\ 0 \le \theta_{0i} \le 2\pi, \quad i = 1,\ldots,m,\ z_0 = Tx_0,\ x_0 \in X_0\}, \tag{32}$$

$$\Theta_f = \{\theta_f \mid \theta_{fi} = \tan^{-1}\frac{z_{f,(2i)}}{z_{f,(2i-1)}},\ 0 \le \theta_{fi} \le 2\pi, \quad i = 1,\ldots,m,\ z_f = Tx_f,\ x_f \in X_f\}, \tag{33}$$

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

where X_0 and X_f are the polyhedral sets defined in (3), and (4), x_0 and x_f are the states in X_0 and X_f.

We formulate the safety verification problem using the following optimization programs which searches for such $T_{\min}$ and $T_{\max}$ so that the equations (28), (29) and set constraints (30), (31), (32), (33) are satisfied,

$$\begin{array}{lll} \textit{min/max} & t, & \\ \text{s.t.} & \rho_{fi} = e^{a_i t}\rho_{0i}, & i = 1,\ldots,m, \\ & \theta_{fi} = \theta_{0i} + w_i t, & i = 1,\ldots,m, \\ & \rho_{0i} = z_{0,(2i-1)}^2 + z_{0,(2i)}^2, & i = 1,\ldots,m, \\ & \rho_{fi} = z_{f,(2i-1)}^2 + z_{f,(2i)}^2, & i = 1,\ldots,m, \\ & \theta_{0i} = \tan^{-1}\frac{z_{0,(2i)}}{z_{0,(2i-1)}}, & i = 1,\ldots,m, \\ & \theta_{fi} = \tan^{-1}\frac{z_{f,(2i)}}{z_{f,(2i-1)}}, & i = 1,\ldots,m, \\ & z_0 = Tx_0, & \\ & z_f = Tx_f, & \\ & H_0x_0 \le h_0, & \\ & H_fx_f \le h_f, & \\ & t > 0 & \end{array} \tag{34}$$

Optimization program (34) is, in general, a nonconvex nonlinear optimization problem which is computationally expensive and hard to solve globally. By relaxing the set constraints, (34) can be over-approximated by linear programs. We over-approximate the sets P_0, P_f, Θ_0 and Θ_f by computing the lower and upper bounds of the states $\rho_0, \rho_f, \theta_0, \theta_f$ so that the over-approximations are expressed as,

$$\hat{P}_0 = \{\rho_0 \mid \rho_0^L \le \rho_0 \le \rho_0^U\}, \hat{P}_f = \{\rho_f \mid \rho_f^L \le \rho_f \le \rho_f^U\} \tag{35}$$

$$\hat{\Theta}_0 = \{\theta_0 \mid \theta_0^L \le \theta_0 \le \theta_0^U\}, \hat{\Theta}_f = \{\theta_f \mid \theta_f^L \le \theta_f \le \theta_f^U\} \tag{36}$$

where $P_0 \subseteq \hat{P}_0$, $P_f \subseteq \hat{P}_f$, $\Theta_0 \subseteq \hat{\Theta}_0$ and $\Theta_f \subseteq \hat{\Theta}_f$. The lower bounds ρ_0^L and ρ_f^L of the states ρ_0 and ρ_f in each 2-dimensional subspace can be computed by performing the following quadratic programs,

$$\begin{array}{lll} \textit{min} & \rho_{0i}^2 = z_{0,(2i-1)}^2 + z_{0,(2i)}^2, & i = 1,\ldots,m, \\ \text{s.t.} & z_0 = Tx_0, & \\ & H_0x_0 \le h_0, & \\ \text{min} & \rho_{fi}^2 = z_{f,(2i-1)}^2 + z_{f,(2i)}^2, & i = 1,\ldots,m, \\ \text{s.t.} & z_f = Tx_f, & \\ & H_fx_f \le h_f. & \end{array} \tag{37}$$

Since maximization of a quadratic program is not a convex program, we compute the upper bounds ρ_0^U and ρ_f^U of the states ρ_0 and ρ_f in each 2-dimensional subspace as,

$$\rho_{0i}^U = \sqrt{(z_{0,(2i-1)}^U)^2 + (z_{0,(2i)}^U)^2},\ i = 1,\ldots,m, \tag{38}$$

$$\rho_{fi}^U = \sqrt{(z_{f,(2i-1)}^U)^2 + (z_{f,(2i)}^U)^2},\ i = 1,\ldots,m \tag{39}$$

where z_0^U and z_f^U can be computed by the linear programs (17).

In order to find the lower and upper bounds θ_0^L and θ_0^U of the state θ_0 in each 2-dimensional subspace, we divide the set θ_0 into four subsets so that each subset is defined in one of the orthants of the 2-dimensional subspace. Then for each

orthant we perform fractional programs to find the minimum and maximum θ_0 for the portion of the set defined in that orthant. Note that splitting is performed in order to express the over-approximation of the set Θ_0 as fractional programs [11] which can be further transformed in linear programs. In the first orthant where $z_{0,(2i-1)} \geq 0, z_{0,(2i)} \geq 0$, the following fractional programs are performed,

$$\begin{aligned} &\text{min/max} && \frac{z_{0,(2i)}}{z_{0,(2i-1)}}, && i = 1, \ldots, m, \\ &\text{s.t.} && z_0 = Tx_0, \\ & && H_0 x_0 \leq h_0, \\ & && z_{0,(2i-1)} \geq 0,\ z_{0,(2i)} \geq 0 \\ &\Rightarrow \alpha_{i1}^L = \tan^{-1}(\min\{\frac{z_{0,(2i)}}{z_{0,(2i-1)}}\}) \\ & \quad \alpha_{i1}^U = \tan^{-1}(\max\{\frac{z_{0,(2i)}}{z_{0,(2i-1)}}\}) \end{aligned} \tag{40}$$

For the second orthant where $z_{0,(2i-1)} \leq 0, z_{0,(2i)} \geq 0$, by the change of variables $\bar{z}_{0,(2i-1)} = -z_{0,(2i-1)}$, the following fractional programs are performed,

$$\begin{aligned} &\text{min/max} && \frac{z_{0,(2i)}}{\bar{z}_{0,(2i-1)}}, && i = 1, \ldots, m, \\ &\text{s.t.} && z_0 = Tx_0, \\ & && H_0 x_0 \leq h_0, \\ & && \bar{z}_{0,(2i-1)} \geq 0,\ z_{0,(2i)} \geq 0 \\ &\Rightarrow \alpha_{i2}^L = \pi - \tan^{-1}(\min\{\frac{z_{0,(2i)}}{\bar{z}_{0,(2i-1)}}\}) \\ & \quad \alpha_{i2}^U = \pi - \tan^{-1}(\max\{\frac{z_{0,(2i)}}{\bar{z}_{0,(2i-1)}}\}) \end{aligned} \tag{41}$$

For the third orthant where $z_{0,(2i-1)} \leq 0, z_{0,(2i)} \leq 0$, by the change of variables $\bar{z}_{0,(2i-1)} = -z_{0,(2i-1)}$ and $\bar{z}_{0,(2i)} = -z_{0,(2i)}$, the following fractional programs are performed,

$$\begin{aligned} &\text{min/max} && \frac{\bar{z}_{0,(2i)}}{\bar{z}_{0,(2i-1)}}, && i = 1, \ldots, m, \\ &\text{s.t.} && z_0 = Tx_0, \\ & && H_0 x_0 \leq h_0, \\ & && \bar{z}_{0,(2i-1)} \geq 0,\ \bar{z}_{0,(2i)} \geq 0 \\ &\Rightarrow \alpha_{i3}^L = \pi + \tan^{-1}(\min\{\frac{\bar{z}_{0,(2i)}}{\bar{z}_{0,(2i-1)}}\}) \\ & \quad \alpha_{i3}^U = \pi + \tan^{-1}(\max\{\frac{\bar{z}_{0,(2i)}}{\bar{z}_{0,(2i-1)}}\}) \end{aligned} \tag{42}$$

For the fourth orthant where $z_{0,(2i-1)} \geq 0, z_{0,(2i)} \leq 0$, by the change of variables $\bar{z}_{0,(2i)} = -z_{0,(2i)}$, the following fractional programs are performed,

$$\begin{aligned} &\text{min/max} && \frac{\bar{z}_{0,(2i)}}{z_{0,(2i-1)}}, && i = 1, \ldots, m, \\ &\text{s.t.} && z_0 = Tx_0, \\ & && H_0 x_0 \leq h_0, \\ & && z_{0,(2i-1)} \geq 0,\ \bar{z}_{0,(2i)} \geq 0 \\ &\Rightarrow \alpha_{i4}^L = 2\pi - \tan^{-1} \frac{\bar{z}_{0,(2i)}}{z_{0,(2i-1)}} \\ & \quad \alpha_{i4}^U = 2\pi - \tan^{-1} \frac{\bar{z}_{0,(2i)}}{z_{0,(2i-1)}} \end{aligned} \tag{43}$$

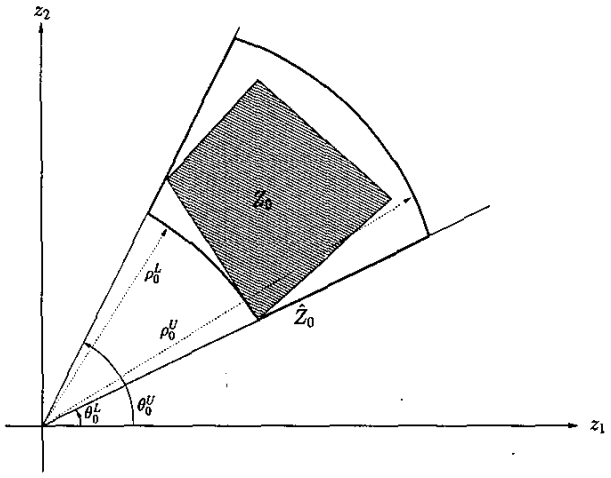

Fig. 2. Over-approximation of Z_0 in polar coordinates

Then θ_0^L and θ_0^U can be calculated by the following,

$$\theta_{0i}^L = \min(\alpha_{i1}^L, \alpha_{i2}^L, \alpha_{i3}^L, \alpha_{i4}^L), \tag{44}$$

$$\theta_{0i}^U = \max(\alpha_{i1}^U, \alpha_{i2}^U, \alpha_{i3}^U, \alpha_{i4}^U). \tag{45}$$

The lower and upper bounds θ_f^L and θ_f^U of the state θ_f can be computed for each subspace by the method above where the computed values are in the interval $[0, 2\pi]$. However, we need to identify angles whose difference is an integer multiple of 2π. Therefore, in the optimization programs, $\theta_{fi}^L + 2k_i\pi$ and $\theta_{fi}^L + 2k_i\pi$ for $k_i \in \mathbb{Z}$ should be used as the lower and upper bounds of θ_f.

For a 2-dimensional subspace, the over-approximation in polar space is illustrated in Figure 2 where z_1 and z_2 are the states, Z_0 is the original set and $\hat{Z}_0$ is the over-approximated set such that $Z_0 \subseteq \hat{Z}_0$.

Subsituting the over-approximated sets (35) and (36) into (34) and writing the constraints $\rho_{fi} = e^{a_i t}\rho_{0i}$ as $\rho_{fi}^{-1} e^{a_i t}\rho_{0i} = 1$ yield the following relaxed optimization programs,

$$\begin{aligned} &\text{min/max} && t, \\ &\text{s.t.} && \rho_{fi}^{-1} e^{a_i t}\rho_{0i} = 1, && i = 1, \ldots, m, \\ & && \theta_{fi} = \theta_{0i} + w_i t, && i = 1, \ldots, m, \\ & && \rho_0^L \leq \rho_0 \leq \rho_0^U \\ & && \rho_f^L \leq \rho_f \leq \rho_f^U \\ & && \theta_0^L \leq \theta_0 \leq \theta_0^U \\ & && \theta_{fi}^L + 2k_i\pi \leq \theta_{fi} \leq \theta_{fi}^U + 2k_i\pi, && i = 1, \ldots, m, \\ & && k_i \in \mathbb{Z}, && i = 1, \ldots, m, \\ & && t > 0 \end{aligned} \tag{46}$$

There are infinite number of optimization programs (46) in the grid of the integer variable k_i. However, the optimization programs (46) can be written equivalently as a series of finite number of linear programs by finding lower and upper bounds $\underline{k}_i$ and $\overline{k}_i$ of the integer variable k_i. For this purpose, we split the optimization programs (46) into two:

optimization in ρ space and optimization in θ space. Then the results of two cases can be intersected to obtain the general result.

B. Verification in ρ coordinates

The optimization programs in ρ coordinates are,

$$\begin{array}{ll} \text{min/max} & t, \\ \text{s.t.} & \rho_{fi}^{-1} e^{a_i t} \rho_{0i} = 1, \quad i = 1, \ldots, m, \\ & \rho_0^L \leq \rho_0 \leq \rho_0^U \\ & \rho_f^L \leq \rho_f \leq \rho_f^U \\ & t > 0. \end{array} \tag{47}$$

Since $\rho_f, \rho_0, \rho_f^L, \rho_f^U, \rho_0^L, \rho_0^U, t > 0$, optimization programs (47) are geometric programs [11] consisting of only monomial equality constraint, by the change of variables $\rho_f = e^{\bar{\rho}_f}, \rho_0 = e^{\bar{\rho}_0}$ they can be written equivalently as linear programs,

$$\begin{array}{ll} \text{min/max} & t, \\ \text{s.t.} & -\bar{\rho}_{fi} + a_i t + \bar{\rho}_{0i} = 0, \quad i = 1, \ldots, m, \\ & \bar{\rho}_0^L \leq \bar{\rho}_0 \leq \bar{\rho}_0^U, \\ & \bar{\rho}_f^L \leq \bar{\rho}_f \leq \bar{\rho}_f^U, \\ & t > 0, \end{array} \tag{LPr}$$

where $\bar{\rho}_0^L = \log(\rho_0^L)$, $\bar{\rho}_0^U = \log(\rho_0^U)$, $\bar{\rho}_f^L = \log(\rho_f^L)$ and $\bar{\rho}_f^U = \log(\rho_f^U)$. Hence, if the sets of initial and final states X_0 and $X_f$are given in state space as in (3), and (4), they can be transformed into polar space where the ρ coordinate of the sets is defined in (30) and (31). The ρ coordinate of the sets can be over-approximated by performing the quadratic programs (37) and (39). After over-approximation, the predicate $\text{Safe}_{[0,+\infty)}(A, X_0, X_f) = 1$ can be verified by solving the linear programs (LPr). If the linear programs (LPr) return a time interval $[T^*_{\min}, T^*_{\max}]$, we can conclude,

$$\begin{aligned} \text{Safe}_{[0,T^*_{\min}]}(A, X_0, X_f) &= 1 \\ \text{Safe}_{[T^*_{\min}, T^*_{\max}]}(A, X_0, X_f) &= 0 \\ \text{Safe}_{[T^*_{\max}, +\infty)}(A, X_0, X_f) &= 1 \end{aligned}$$

by Proposition 2.3. Note that, only two linear programs are required for the verification in ρ coordinates. If a more precise time interval is required or safety analysis in ρ coordinates failed to show $\text{Safe}_{[0,+\infty)}(A, X_0, X_f) = 1$, verification in θ coordinates focusing only on the critical time interval $[T^*_{\min}, T^*_{\max}]$ can be done.

C. Verification in θ coordinates

The optimization programs in θ coordinates are,

$$\begin{array}{ll} \text{min/max} & t, \\ \text{s.t.} & \theta_{fi} = \theta_{0i} + w_i t, \qquad i = 1, \ldots, m, \\ & \theta_{fi}^L + 2k_i\pi \leq \theta_{fi} \leq \theta_{fi}^U + 2k_i\pi, i = 1, \ldots, m, \\ & \theta_0^L \leq \theta_0 \leq \theta_0^U, \\ & k_i \in \mathbb{Z}, \qquad i = 1, \ldots, m, \\ & T^*_{\min} \leq t \leq T^*_{\max}, \end{array} \tag{48}$$

where $[T^*_{\min}, T^*_{\max}]$ is the time interval computed by the linear programs (LPr).

Since, we are only focusing on the critical time interval $[t^*_{\min}, t^*_{\max}]$, we can find the lower and upper bounds $\underline{k}_i$ and $\overline{k}_i$ of k_i in each subspace by,

$$\underline{k}_i = \lfloor \frac{w_i T^*_{\min}}{2\pi} \rfloor, \quad \overline{k}_i = \lceil \frac{w_i T^*_{\max}}{2\pi} \rceil. \tag{49}$$

In each subspace, for each integer $k_i \in [\underline{k}_i, \overline{k}_i]$, optimization programs (48) become the following linear programs,

$$\begin{array}{ll} \text{min/max} & t, \\ \text{s.t.} & \theta_{fi} = \theta_{0i} + w_i t, \\ & \theta_{fi}^L + 2k_i\pi \leq \theta_{fi} \leq \theta_{fi}^U + 2k_i\pi \\ & \theta_{0i}^L \leq \theta_{0i} \leq \theta_{0i}^U \\ & T^*_{\min} \leq t \leq T^*_{\max}, \end{array} \tag{LPt}$$

Therefore, the verification in θ coordinates can be done by solving linear programs (LPt) for each integer $k_i \in [\underline{k}_i, \overline{k}_i]$ in each 2-dimensional subspace and then intersecting the results obtained by each linear program to obtain the general solution in θ coordinates. The total number of linear programs (LPt) required is $m(\overline{k}_i - \underline{k}_i + 1)$ where m is the number of 2-dimensional subspaces. Note that, finite number of linear programs are required for the verification in θ coordinates.

Hence, if the sets of initial and final states X_0 and X_f are given in state space as in (3), and (4), they can be transformed into polar space where θ coordinate of the sets is defined in (32) and (33). The θ coordinate of the sets can be over-approximated by performing the fractional programs (40),(42),(43),(44) and performing (44) and (45). After over-approximation, the predicate $\text{Safe}_{[0,+\infty)}(A, X_0, X_f) = 1$ can be verified by the method proposed in this section. If the verification method returns a time interval $[T^*_{\min}, T^*_{\max}]$, we can conclude,

$$\begin{aligned} \text{Safe}_{[0,T^*_{\min}]}(A, X_0, X_f) &= 1 \\ \text{Safe}_{[T^*_{\min}, T^*_{\max}]}(A, X_0, X_f) &= 0 \\ \text{Safe}_{[T^*_{\max}, +\infty)}(A, X_0, X_f) &= 1 \end{aligned}$$

by Proposition 2.3.

D. Illustrative Example

Assume the two dimensional system with the system matrix,

$$A = \begin{bmatrix} -3 & 1 \\ -5 & 1 \end{bmatrix}, \tag{50}$$

with eigenvalues $\lambda_{1,2} = -1 \pm 1i$.The set of initial and final (unsafe) states are given as in (3) and (4), where

$$H_f, H_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ -1 & 0 \\ 0 & -1 \end{bmatrix} \quad h_f = \begin{bmatrix} 10 \\ 10 \\ -1 \\ -1 \end{bmatrix} \quad h_0 = \begin{bmatrix} 420 \\ 420 \\ -410 \\ -410 \end{bmatrix}$$

With the following transformation matrix,

$$T = \begin{bmatrix} 5.3284 & -2.2071 \\ 0.3787 & 0.9142 \end{bmatrix}, \tag{51}$$

the system matrix A can be decomposed into,

$$\Lambda = \begin{bmatrix} -1 & 1 \\ -1 & -1 \end{bmatrix}. \quad (52)$$

The solution in polar coordinates to differential equation $\dot{z} = \Lambda z$ is given in (28) and (29). Performing the quadratic programs (37) and (39) to overapproximate the sets in ρ coordinates yield,

$$2.3890 \leq \rho_f < 19.2604,$$
$$1368.3938 \leq \rho_0 \leq 1435.9588 \quad (53)$$

Performing the linear programs (40), (42), (43), and (44) and performing (44) and (45) to overapproximate the sets in θ coordinates yield,

$$0.0918 \leq \theta_f < 2.6245, \quad 0.3809 \leq \theta_0 \leq 0.4050 \quad (54)$$

Verification in ρ coordinates by solving (LPr) with the computed over-approximations in ρ coordinates yields $T^*_{\min} = 4.2633$ and $T^*_{\max} = 6.3987$.

Now we proceed to the verification in θ coordinates by focusing on the critical time interval $[4.2633, 6.3987]$ to obtain a more precise time interval or a safety certificate. Substituting $w = 1$ and computed $T^*_{\min}$ and $T^*_{\max}$ values into (49) yields $\underline{k} = 0$ and $\overline{k} = 2$. For $k = 0$ solving (LPt) yields infeasible solutions which means that the final set is not reachable in the first revolution. For $k = 1$ solving (LPt) yields the time interval $[5.9699, 6.3987]$. For $k = 2$ solving (LPt) yields infeasible solutions which means that the final set is not reachable in the third revolution. Therefore, the intersection of all time intervals computed for each k is $T^*_{\min} = 5.9699$ and $T^*_{\max} = 6.3987$. Hence,

$$\begin{aligned} \text{Safe}_{[0,T^*_{\min}]}(A, X_0, X_f) &= 1 \\ \text{Safe}_{[T^*_{\min}, T^*_{\max}]}(A, X_0, X_f) &= 0 \\ \text{Safe}_{[T^*_{\max}, +\infty)}(A, X_0, X_f) &= 1 \end{aligned}$$

by Proposition 2.3. The elapsed CPU time for computing the above linear programs is 0.27 seconds.

E. High Dimensional Verification

We implemented our method presented in Section IV using MATLAB. The results in different dimensions are given in the following table,

System Dimension	*System Safe?*	*Compute Time (Sec)*	$T^*_{\min}$ *(sec)*	$T^*_{\max}$ *(sec)*
6	No	0.94	113.14	186.88
6	Yes	0.79		
10	No	1.70	81.70	109.86
10	Yes	1.72		
100	Yes	705.60		

Table 2 - Safety computation results

Note that, only two linear programs are sufficient to do verification in ρ coordinates. Therefore, besides the dimension, another factor affecting computational time significantly is the value of $(\overline{k}_i - \underline{k}_i + 1)$ which determines the number of linear programs in the safety analysis in θ coordinates. Depending on the eigenstructure and sets, it is possible to get quick results by only performing safety analysis in ρ coordinates. If more precise time intervals are required, or safety analysis in ρ coordinates failed to show $\text{Safe}_{[0,+\infty)}(A, X_0, X_f) = 1$, then we can proceed to do further analysis in θ coordinates focusing only on the critical time interval provided by the analysis in ρ coordinates.

V. Conclusions

In this paper, we have presented a novel method to obtain safety certificates of continuous linear systems by exploiting the structure of linear systems and the monotonicity of the exponential function. The safety verification problem was written as series of geometric programs and further transformed to equivalent linear programs which provides the ability to verify the safety properties of (high dimensional) linear systems in realistic computation times. Our method provides time intervals over which the system is safe and unsafe.

VI. Acknowledgments

This research would not have been possible without the inspired teaching of Ali Jadbabaie on Convex Optimization course in the Fall 2002 semester at the University of Pennsylvania. We also thank Stephen Prajna for discussions on this paper.

References

[1] 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.

[2] 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.

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

[4] 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.

[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] 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.

[7] 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.

[8] 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.

[9] R. Alur, T. Dang, and F. Ivancic, "Counter-example guided predicate abstraction of hybrid systems," in *Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, ser. Lecture Notes in Computer Science, H. Garavel and J. Hatcliff, Eds. Warsaw, Poland: Springer, April 2003, vol. 2619, pp. 208–223.

[10] R. Alur and D. Dill, "A theory of timed automata," *Theoretical Computer Science*, vol. 126, pp. 183–235, 1994.

[11] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.