2016 European Control Conference (ECC)
June 29 - July 1, 2016. Aalborg, Denmark

Computing Reachable Sets of Linear Vector Fields Revisited

Ting Gan[1], Mingshuai Chen[2], Yangjia Li[2], Bican Xia[1] and Naijun Zhan[2]

[1] LMAM & School of Mathematical Sciences, Peking University
[2] State Key Lab. of Computer Science, Institute of Software, Chinese Academy of Sciences

Abstract— **The reachability problem is one of the most important issues in the verification of hybrid systems. But unfortunately the reachable sets for most of hybrid systems are not computable except for some special families. In our previous work, we identified a family of vector fields, whose state parts are linear with real eigenvalues, while input parts are exponential functions, and proved its reachability problem is decidable. In this paper, we investigate another family of vector fields, whose state parts are linear, but with pure imagine eigenvalues, while input parts are trigonometric functions, and prove its reachability problem is decidable also. To the best of our knowledge, the two families are the largest families of linear vector fields with a decidable reachability problem. In addition, we present an approach on how to abstract general linear dynamical systems to the first family. Comparing with existing abstractions for linear dynamical systems, experimental results indicate that our abstraction is more precise.**

I. Introduction

Hybrid systems (HSs) integrate discrete and continuous dynamical systems. HSs span over multiple domains, *e.g.*, communication, healthcare, manufacturing, aerospace, transportation, etc., many of which are safety-critical. To guarantee the correctness of these systems is vital and challenging. Therefore, formal methods have been widely used in the verification of HSs. The reachability problem of HSs is to verify that unsafe states are not reachable from the set of the initial states for a given HS, which is one of most important issues in the verification of HSs.

As HSs consist of deep interaction between continuous evolutions and discrete transitions, the reachability problem of most of HSs is undecidable [14], except for some simple cases, either their vector fields are quite simple such as timed automata [3] and multi-rate automata [2], or there are very restrictive constraints on their discrete transitions like o-minimal HSs [18].

In [19], Lafferriere et al. investigated vector fields of the form

$$\dot{\xi} = A\xi + \mathbf{u}, \tag{1}$$

where $\xi(t) \in \mathbb{R}^n$ is the state of the system at time t, $A \in \mathbb{R}^{n\times n}$ is the system matrix, and $\mathbf{u} : \mathbb{R} \to \mathbb{R}^n$ is a piecewise continuous function which is called the *input*. By reducing them into Tarski's algebra [26], they proved that the reachability problems of the following three families of vector fields are decidable.

1) A is *nilpotent*, *i.e.* $A^n = 0$, and each component of $\mathbf{u}$ is a polynomial;
2) A is *diagonalizable* with rational eigenvalues, and each component of $\mathbf{u}$ is of the form $\sum_{i=1}^{m} c_i e^{\lambda_i t}$, where λ_is are rationals and c_is are subject to semi-algebraic constraints;
3) A is *diagonalizable* with purely imaginary eigenvalues, whose imaginary parts are rationals, and each component of $\mathbf{u}$ is of the form $\sum_{i=1}^{m} c_i \sin(\lambda_i t) + d_i \cos(\lambda_i t)$, where λ_is are rationals and c_is and d_is are subject to semi-algebraic constraints.

In our previous work [10], by exploiting the decidability of a theory of specific *polynomial-exponential functions* [1], [24], [25], we generalized the case 2) above to

- A is *diagonalizable* with *real* eigenvalues, and each component of $\mathbf{u}$ is of the form $\sum_{i=1}^{m} c_i e^{\lambda_i t}$, where λ_is are *reals* and c_is are subject to semi-algebraic constraints.

In this paper, we first generalize the case 3) above to

- A is *diagonalizable* with purely imaginary eigenvalues, whose imaginary parts are reals, and each component of $\mathbf{u}$ is of the form $\sum_{i=1}^{m} c_i \sin(\lambda_i t) + d_i \cos(\lambda_i t)$, where λ_is are reals and c_is and d_is are subject to semi-algebraic constraints.

This is achieved also by reducing the decidability to Tarski's algebra [26] using the density results in number theory [13].

Another contribution of this paper is to present an abstraction of general dynamical systems of the form (1). The basic idea of our approach is as follows: for each eigenvalue $\alpha \pm \beta i$, we introduce two fresh variables a and b, and let $a = \sin\beta t$ and $b = \cos\beta t$. So, it derives a new constraint $a^2 + b^2 = 1$. Using such replacement, the reachable set of (1) can be essentially represented as the form

$$f(t, \mathbf{x}, \mathbf{a}, \mathbf{b}) = \sum_{i=0}^{m} f_i(t, \mathbf{x}, \mathbf{a}, \mathbf{b}) e^{\alpha_i t}.$$

Obviously, constraints over such expressions together with all the derived constraints are fallen within the decidable theory of the specific *polynomial-exponential functions* that we considered in [10]. Experimental results indicate that our approach provides more precise abstraction for linear dynamical systems of (1) than Tiwari et al's approach based on the eigenvalues of A [9], [21].

II. Preliminaries

In this section, we first briefly review some basic notions and theoretical results, based on which our approach is

978-1-5090-2591-6 ©2016 EUCA

developed, and then explain the problem we consider. We use $\mathbf{x}$ to stand for a vector variable $(x_1, \ldots, x_n)$, $\mathbb{N}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ for natural, rational, real and complex numbers respectively, and $\mathbb{R}[\mathbf{x}]$ for the polynomial ring in $\mathbf{x}$ with coefficients in $\mathbb{R}$.

A. Some Notions

A term is called a *trigonometric function* (TMF) w.r.t. t if it can be represented as

$$\sum_{l=1}^{r} c_l cos(\mu_l t) + d_l sin(\mu_l t), \tag{2}$$

where $r \in \mathbb{N}, c_l, d_l, \mu_l \in \mathbb{R}$.

A *linear dynamical system* (LDS) is of the form (1). We say an LDS is a *linear dynamical system with trigonometric function input* ($\mathrm{LDS}_{\mathrm{TMF}}$) if every component of $\mathbf{u}$ is a TMF.

A set $\mathrm{X} \subseteq \mathbb{R}^n$ is said *open semi-algebraic* if

$$\mathrm{X} = \{\mathbf{x} \in \mathbb{R}^n \mid p_1(\mathbf{x}) > 0, \cdots, p_j(\mathbf{x}) > 0\},$$

for some polynomials $p_1(\mathbf{x}), \cdots, p_j(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$, where $j \in \mathbb{N}$.

Given an initial state $\xi(0) = \mathbf{x}$, the solution of (1) at time $t \geq 0$ is denoted by $\xi(t) = \Phi(\mathbf{x}, t)$[1]. Then the *backward reachable set* $Pre(\mathrm{X})$ and the *forward reachable set* $Post(\mathrm{X})$ of the LDS (1) from a given set X are defined as follow:

$$Pre(\mathrm{X}) = \{\mathbf{y} \in \mathbb{R}^n \mid \exists \mathbf{x} \exists t : \mathbf{x} \in \mathrm{X} \wedge t \geq 0 \wedge \Phi(\mathbf{y}, t) = \mathbf{x}\}, \tag{3}$$

$$Post(\mathrm{X}) = \{\mathbf{y} \in \mathbb{R}^n \mid \exists \mathbf{x} \exists t : \mathbf{x} \in \mathrm{X} \wedge t \geq 0 \wedge \Phi(\mathbf{x}, t) = \mathbf{y}\}. \tag{4}$$

B. Problem Description

Given an $\mathrm{LDS}_{\mathrm{TMF}}$ described in (1) in which A is diagonalizable with purely imaginary eigenvalues, the i^{th} component u_i of $\mathbf{u}$ is of the following form:

$$u_i = \sum_{l=1}^{r_i} c_{il} cos(\mu_{il} t) + d_{il} sin(\mu_{il} t),$$

where $r_i \in \mathbb{N}, c_{il}, d_{il}, \mu_{il} \in \mathbb{R}$. In addition, we also assume that for all $1 \leq i \leq n$, $1 \leq l \leq r_i$, $\mu_{il}\mathbf{i}$ is not an eigenvalue.

Given an initial set X and an unsafe set Y, where X and Y both are open semi-algebraic sets, the problem is to verify whether any unsafe state in Y is not reachable by some trajectory starting from X, *i.e.*, whether $Post(\mathrm{X}) \cap \mathrm{Y} = \emptyset$, or dually $Pre(\mathrm{Y}) \cap \mathrm{X} = \emptyset$, or

$$\mathscr{F}(\mathrm{X}, \mathrm{Y}) = \exists \mathbf{x} \exists \mathbf{y} \exists t : \mathbf{x} \in \mathrm{X} \wedge \mathbf{y} \in \mathrm{Y} \wedge t \geq 0 \wedge \Phi(\mathbf{x}, t) = \mathbf{y}. \tag{5}$$

C. Theoretical Results on Number Theory

Definition 1 (Rational Linear Independent): Let $a_1, \ldots, a_k$ be some real numbers. We say $a_1, \ldots, a_k$ are *rational linear independent* if the following formula holds:

$$\bigwedge_{i=1}^{k} c_i \in \mathbb{Q} \wedge \sum_{i=1}^{k} c_i a_i = 0 \Rightarrow \bigwedge_{i=1}^{k} c_i = 0.$$

Definition 2 (Basis): Let $A \subset \mathbb{R}$ with $\#(A) \leq +\infty$ be a set of real numbers, where $\#(A)$ stands for the cardinality of A. A set $B \subseteq A$ is said to be a *basis* of A, if the elements in B are rational linear independent, and for any element $a \in A \backslash B$, where $A \backslash B$ is the set of all the elements in A but not in B, then the elements of $\{a\} \cup B$ are not rational linear independent any more.

Thus, suppose $A = \{a_1, \ldots, a_k\}$ is a set of real numbers, $B = \{b_1, \ldots, b_j\} \subseteq A$ is a basis of A, then for any $a_i \in A$ there exists $c = (c_{i1}, \ldots, c_{ij}) \in \mathbb{Q}$ such that

$$a_i = c_{i1} b_1 + \ldots + c_{ij} b_j. \tag{6}$$

For $1 \leq l \leq j$, let

$$d_l = \mathrm{lcm}(\mathrm{denom}(c_{1l}), \ldots, \mathrm{denom}(c_{kl})), \tag{7}$$

where $\mathrm{denom}(c)$ denotes the denominator of c and lcm means the least common multiple. Then $\overline{B} = \{\frac{b_1}{d_1}, \ldots, \frac{b_j}{d_j}\}$ is a basis of A, and for any $a \in A$, a can be written as a linear combination of $\overline{B}$ with integer coefficients, we call such basis $\overline{B}$ an *integer basis* of A.

Theorem 1 (Kronecker Theorem [13]): The set

$$\{(\{\xi_1 t\}_1, \ldots, \{\xi_k t\}_1) \mid t \in \mathbb{N}\}$$

is dense in $[0,1]^k$, if $1, \xi_1, \ldots, \xi_k$ are integer linear independent, where $\{\xi\}_1 \in [0,1)$ is the decimal part of the real number ξ.

Corollary 1: The set $\{(\{\xi_1 t\}_{2\pi}, \ldots, \{\xi_k t\}_{2\pi}) \mid t \geq 0\}$ is dense in $[0,2\pi]^k$, if $\xi_1, \ldots, \xi_k$ are integer linear independent, where $\{\xi\}_{2\pi} \in [0,2\pi)$ is the remainder of ξ modulo 2π.

Proof: Let $\xi'_i = \frac{\xi_i}{2\pi}$, for $i = 1, \ldots, k$. It is easy to see that we just need to prove that

$$\{(\{\xi'_1 t\}_1, \ldots, \{\xi'_k t\}_1) \mid t \geq 0\} \tag{8}$$

is dense in $[0,1]^k$.

Since $\xi_1, \ldots, \xi_k$ are integer linear independent, $\xi'_1, \ldots, \xi'_k$ are also integer linear independent. It therefore follows that there exists $\xi_0 > 0$ such that $1, \xi_0\xi'_1, \ldots, \xi_0\xi'_k$ are integer linear independent. From Theorem 1 we have that

$$\{(\{\xi_0\xi'_1 n\}_1, \ldots, \{\xi_0\xi'_k n\}_1) \mid n \in \mathbb{N}\} \tag{9}$$

is dense in $[0,1]^k$. Since $\xi_0 > 0$, it follows

$$\{\xi_0 n \mid n \in \mathbb{N}\} \subset \{t \mid t \geq 0\}.$$

Thus, we have that the set in (9) is a subset of the set in (8). Whence, the set in (8) is dense in $[0,1]^k$. ■

Theorem 2: Let $a_1, \ldots, a_k$ be rational linear independent, S and $\overline{S}$ be two sets defined as

$$S = \{(\sin(a_1 t), \cos(a_1 t), \ldots, \sin(a_k t), \cos(a_k t)) \mid t \geq 0\}, \tag{10}$$

$$\overline{S} = \{(\alpha_1, \beta_1, \ldots, \alpha_k, \beta_k) \in \mathbb{R}^{2k} \mid \bigwedge_{i=1}^{k} \alpha_i^2 + \beta_i^2 = 1\}, \tag{11}$$

then S is dense in $\overline{S}$.

Proof: $a_1, \ldots, a_k$ are rational linear independent, then also integer linear independent. By Corollary 1, we have that

$$D_0 = \{(\{a_1 t\}_{2\pi}, \ldots, \{a_k t\}_{2\pi}) \mid t \geq 0\}$$

is dense in $D = [0,2\pi]^k$. On the other hand, obviously, $(\sin, \cos) : D_0 \mapsto S$, and $(\sin, \cos) : D \mapsto \overline{S}$, and $(\sin, \cos)$ is continuous, hence $f(S)$ is dense in $f(\overline{S})$. ■

[1] Here, we assume A and $\mathbf{u}$ in (1) are fixed.

Corollary 2: Let $f(\alpha_1, \beta_1, \dots, \alpha_k, \beta_k)$ be a polynomial in $\alpha_1, \beta_1, \dots, \alpha_k, \beta_k$. Suppose $a_1, \dots, a_k$ are real numbers that are rational linear independent, and S and $\overline{S}$ are defined as (10), (11), then $f(S)$ is dense in $f(\overline{S})$.

Proof: By Theorem 2, it follows that S is dense in $\overline{S}$, and S and $\overline{S}$ are bounded. Since f is polynomial, thus f is continuous, hence $f(S)$ is dense in $f(\overline{S})$. ■

III. Decidability

Given an `LDS` (1) and an initial state $\mathbf{x}$, the solution of the `LDS` starting from $\mathbf{x}$ can be represented by

$$\xi(t) = \Phi(\mathbf{x}, t) = e^{At}\mathbf{x} + \int_0^t e^{A(t-\tau)}\mathbf{u}(\tau)d\tau, \qquad (12)$$

where the matrix exponential e^{At} is defined by $\sum_{k=0}^{\infty} \frac{t^k}{k!} A^k$.

A. First Part

Suppose all the eigenvalues of the real matrix A are purely imaginary numbers, then there exists a block diagonal matrix $D \in \mathbb{R}^{n\times n}$ and an invertible matrix $Q \in \mathbb{R}^{n\times n}$ such that $A = QDQ^{-1}$, where

$$D = \begin{bmatrix} D_1 & & \\ & \ddots & \\ & & D_m \end{bmatrix},$$

with blocks $D_1, \dots, D_m$ of the form:

$$D_k = \begin{bmatrix} 0 & -\lambda_k \\ \lambda_k & 0 \end{bmatrix},$$

$n = 2m$ and $\pm\lambda_1\mathbf{i}, \dots, \pm\lambda_m\mathbf{i}$ are the eigenvalues of A. Denote

$$\Lambda = \{\pm\lambda_1\mathbf{i}, \dots, \pm\lambda_m\mathbf{i}\}. \qquad (13)$$

Since $e^{D_k t} = \begin{bmatrix} \cos(\lambda_k t) & -\sin(\lambda_k t) \\ \sin(\lambda_k t) & \cos(\lambda_k t) \end{bmatrix}$, we have

$$\begin{aligned} e^{At} &= Q \begin{bmatrix} e^{D_1 t} & & \\ & \ddots & \\ & & e^{D_m t} \end{bmatrix} Q^{-1} \\ &= Q \begin{bmatrix} \cos(\lambda_1 t) & -\sin(\lambda_1 t) & & & \\ \sin(\lambda_1 t) & \cos(\lambda_1 t) & & & \\ & & \ddots & & \\ & & & \cos(\lambda_m t) & -\sin(\lambda_m t) \\ & & & \sin(\lambda_m t) & \cos(\lambda_m t) \end{bmatrix} Q^{-1}. \end{aligned}$$

Then it is straightforward that $(e^{At})_{ij}$ has the following form:

$$(e^{At})_{ij} = \sum_{k=1}^{m} a_{ijk}\cos(\lambda_k t) + b_{ijk}\sin(\lambda_k t), \qquad (14)$$

where $a_{ijk}, b_{ijk} \in \mathbb{R}$, and $1 \le i, j \le n$. So we have that

$$\begin{aligned} (e^{At}\mathbf{x})_i &= \sum_{j=1}^{n} (\sum_{k=1}^{m} a_{ijk}\cos(\lambda_k t) + b_{ijk}\sin(\lambda_k t)) x_j \\ &= \sum_{k=1}^{m} (\sum_{j=1}^{n} a_{ijk} x_j)\cos(\lambda_k t) + \sum_{k=1}^{m} (\sum_{j=1}^{n} b_{ijk} x_j)\sin(\lambda_k t). \end{aligned}$$

Thus, $(e^{At}\mathbf{x})_i$ should have the following form:

$$(e^{At}\mathbf{x})_i = \sum_{k=1}^{m} \alpha_{ik}(\mathbf{x})\cos(\lambda_k t) + \beta_{ik}(\mathbf{x})\sin(\lambda_k t). \qquad (15)$$

B. Second Part

Now, we consider the other part of the solution $\int_0^t e^{A(t-\tau)}\mathbf{u}(\tau)d\tau$, in which each u_j of $\mathbf{u}(t)$ is of the form

$$u_j(t) = \sum_{l=1}^{r_j} c_{jl}\cos(\mu_{jl} t) + d_{jl}\sin(\mu_{jl} t), \qquad (16)$$

where $r_j \in \mathbb{N}$, $c_{jl}, d_{jl}, \mu_{jl} \in \mathbb{R}$ for $1 \le j \le n$, $1 \le l \le r_j$, and $\mu_{jl}\mathbf{i}$ is not equal to any eigenvalue of A, *i.e.* $\mu_{jl}\mathbf{i} \notin \Lambda$.

Then, for $1 \le i \le n$, we have

$$\begin{aligned} & (e^{-A\tau}\mathbf{u}(\tau))_i \\ = \; & \sum_{j=1}^{n} (e^{-A\tau})_{ij} u_j(\tau) \\ = \; & \sum_{j=1}^{n} (\sum_{k=1}^{m} a_{ijk}\cos(\lambda_k\tau) + b_{ijk}\sin(\lambda_k\tau))(\sum_{l=1}^{r_j} c_{jl}\cos(\mu_{jl}\tau) \\ & + d_{jl}\sin(\mu_{jl}\tau)) \\ = \; & \sum_{j=1}^{n}\sum_{k=1}^{m}\sum_{l=1}^{r_j} a_{ijk}c_{jl}\cos(\lambda_k\tau)\cos(\mu_{jl}\tau) \\ & \quad + a_{ijk}d_{jl}\cos(\lambda_k\tau)\sin(\mu_{jl}\tau) \\ & \quad + b_{ijk}c_{jl}\sin(\lambda_k\tau)\cos(\mu_{jl}\tau) + b_{ijk}d_{jl}\sin(\lambda_k\tau)\sin(\mu_{jl}\tau). \end{aligned}$$

As the products $\sin\eta\sin\theta$, $\sin\eta\cos\theta$, $\cos\eta\sin\theta$, $\cos\eta\cos\theta$ can be re-written as linear combinations of $\sin(\eta\pm\theta)$ and $\cos(\eta\pm\theta)$, $(e^{-A\tau}\mathbf{u}(\tau))_i$ can be reformulated as the following form:

$$(e^{-A\tau}\mathbf{u}(\tau))_i = \sum_{j=1}^{s_i} f_{ij}\cos(\nu_{ij}\tau) + g_{ij}\sin(\nu_{ij}\tau), \qquad (17)$$

where $s_j \in \mathbb{N}, f_{ij}, g_{ij} \in \mathbb{R}$ and $\nu_{ij} \in \{\lambda_k \pm \mu_{il} \mid 1 \le k \le m, 1 \le j \le n, 1 \le l \le r_j\}$. Additionally, $\nu_{ij} \ne 0$, as $\mu_{jl}\mathbf{i} \notin \Lambda$, for all $1 \le i \le n, 1 \le j \le s_i$.

Thus, we have that

$$\begin{aligned} & (\int_0^t e^{A(t-\tau)}\mathbf{u}(\tau)d\tau)_i \\ &= \sum_{k=1}^{n} (e^{At})_{ik} \int_0^t (e^{-A\tau}\mathbf{u}(\tau))_k d\tau \\ &= \sum_{k=1}^{n} (e^{At})_{ik} \int_0^t (\sum_{j=1}^{s_i} f_{kj}\cos(\nu_{kj}\tau) + g_{kj}\sin(\nu_{kj}\tau))d\tau \\ &= \sum_{k=1}^{n} (e^{At})_{ik} \sum_{j=1}^{s_i} (\frac{f_{kj}}{\nu_{kj}}\sin(\nu_{kj}t) - \frac{g_{kj}}{\nu_{kj}}\cos(\nu_{kj}t) + \frac{g_{kj}}{\nu_{kj}}). \end{aligned}$$

Combining with the formula (14), it is easy to see that $(\int_0^t e^{A(t-\tau)}\mathbf{u}(\tau)d\tau)_i$ should have the form:

$$(\int_0^t e^{A(t-\tau)}\mathbf{u}(\tau)d\tau)_i = \sum_{j=1}^{J_i} f'_{ij}\cos(\omega_{ij}t) + g'_{ij}\sin(\omega_{ij}t), \quad (18)$$

where $J_i \in \mathbb{N}, f'_{ij}, g'_{ij} \in \mathbb{R}$.

By (15) and (18), the solution (12) should be of the form

$$(\xi(t))_i = \sum_{k=1}^{K_i} z^c_{ik}(\mathbf{x})\cos(\gamma_{ik}t) + z^s_{ik}(\mathbf{x})\sin(\gamma_{ik}t), \qquad (19)$$

where $z^c_{ik}(\mathbf{x}), z^s_{ik}(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$ and $\gamma_{ik} \in \mathbb{R}$.

Hence, (5) can be reformulated as

$$\begin{aligned}\mathscr{F}(\mathrm{X},\mathrm{Y}) \; = \; & \exists\mathbf{x}\exists\mathbf{y}\exists t : \mathbf{x}\in\mathrm{X}\wedge\mathbf{y}\in\mathrm{Y}\wedge t\geq 0 \\ & \wedge y_i = \sum_{k=1}^{K_i} z^c_{ik}(\mathbf{x})\cos(\gamma_{ik}t)+z^s_{ik}(\mathbf{x})\sin(\gamma_{ik}t). \end{aligned}\tag{20}$$

C. Reduction to Tarski's Algebra

Whether formula (20) holds is essentially a *quantifier elimination* problem. For the polynomial case, *i.e.* all the functions in the formula are polynomials, it can be well solved by some tools [20], [15], [7], [8], [4], [12], [23], all of which are based on *cylindrical algebraic decomposition* (CAD) [6]. But formula (20) is not in the polynomial case, since it contains trigonometric functions.

From now on, we will focus on how to transform formula (20) to Tarski's algebra equivalently, under the conditions described in section II-B.

Let Ω be the quantifier-free part of formula (20), *i.e.*

$$\begin{aligned}\Omega \; = \; & \mathbf{x}\in\mathrm{X}\wedge\mathbf{y}\in\mathrm{Y}\wedge t\geq 0\wedge \\ & \bigwedge_{i=1}^{n} y_i = \sum_{k=1}^{K_i} z^c_{ik}(\mathbf{x})\cos(\gamma_{ik}t)+z^s_{ik}(\mathbf{x})\sin(\gamma_{ik}t),\end{aligned}$$

$\Gamma=\{\gamma_{ik}\mid 1\leq i\leq n, 1\leq k\leq K_i\}$, where γ_{ik}s are the real numbers appearing in the above formula, and $\Delta=\{\delta_1,\dots,\delta_N\}$ be an integer-basis of Γ, *i.e.*, for any $\gamma\in\Gamma$, γ can be written as a linear combination of Δ with integer coefficients. So, obviously, $\cos(\gamma t)$ and $\sin(\gamma t)$ both are polynomials in $\sin(\delta_1 t),\cos(\delta_1 t),\dots,\sin(\delta_N t),\cos(\delta_N t)$, for $1\leq i\leq n, 1\leq k\leq K_i$. Formally,

$$\cos(\gamma_{ik}t) = f^c_{ik}(\sin(\delta_1 t),\cos(\delta_1 t),\dots,\sin(\delta_N t),\cos(\delta_N t)), \tag{21}$$

$$\sin(\gamma_{ik}t) = f^s_{ik}(\sin(\delta_1 t),\cos(\delta_1 t),\dots,\sin(\delta_N t),\cos(\delta_N t)), \tag{22}$$

where f^c_{ik}, f^S_{ik} are polynomials.

Now, we denote the following formula by Ξ, *i.e.*,

$$\begin{aligned}\Xi \,\hat{=}\; & \mathbf{x}\in\mathrm{X}\wedge\mathbf{y}\in\mathrm{Y}\wedge\bigwedge_{j=1}^{N} u_j^2+v_j^2=1\wedge \\ & \bigwedge_{i=1}^{n} y_i = \sum_{k=1}^{K_i}\left(\begin{array}{c} z^c_{ik}(\mathbf{x})f^c_{ik}(u_1,v_1,\dots,u_N,v_N) \\ +z^s_{ik}(\mathbf{x})f^s_{ik}(u_1,v_1,\dots,u_N,v_N)\end{array}\right).\end{aligned}$$

Theorem 3: Suppose X, Y both are open semi-algebraic sets, Γ is defined as above, which is a set of real numbers, Δ is an integer-basis of Γ, f^c_{ik} and f^s_{ik} are defined as (21), (22), and Ω and Ξ are two formulas defined as above, then

$$\exists x\exists y\exists t\Omega \Leftrightarrow \exists x\exists y\exists_{j=1}^{N}u_j\exists_{j=1}^{N}v_j\Xi. \tag{23}$$

Proof: It is evident to see that

$$\exists x\exists y\exists t\Omega \Rightarrow \exists x\exists y\exists_{j=1}^{N}u_j\exists_{j=1}^{N}v_j\Xi, \tag{24}$$

since if there exist x,y,t satisfying Ω, let $u_j=\sin(\delta_j t), v_j=\cos(\delta_j t)$, then Ξ is satisfied. We just need to prove that

$$\exists x\exists y\exists t\Omega \Leftarrow \exists x\exists y\exists_{j=1}^{N}u_j\exists_{j=1}^{N}v_j\Xi. \tag{25}$$

Let

$$S=\{(\sin(\delta_1 t),\cos(\delta_1 t),\dots,\sin(\delta_N t),\cos(\delta_N t))\mid t\geq 0\},$$

$$\overline{S}=\{(u_1,v_1,\dots,u_N,v_N)\in\mathbb{R}^{2N}\mid \bigwedge_{i=1}^{N}u_i^2+v_i^2=1\}.$$

From Theorem 2, it derives that S is dense in $\overline{S}$. Denote $w=(u_1,v_1,\dots,u_N,v_N)$. Let x',y',u'_i,v'_i satisfy Ξ, *i.e.*,

$$\begin{aligned}& x'\in\mathrm{X}\wedge y'\in\mathrm{Y}\wedge w'\in\overline{S}\wedge \\ & \bigwedge_{i=1}^{n} y'_i = \sum_{k=1}^{K_i} z^c_{ik}(x')f^c_{ik}(w')+z^s_{ik}(x')f^s_{ik}(w'),\end{aligned}$$

where $w'=(u'_1,v'_1,\dots,u'_N,v'_N)$. Since Y is an open set, $y'\in\mathrm{Y}$, there exists an open ball $B_\varepsilon(y')\subset\mathrm{Y}$, where $B_\varepsilon(y')$ is the ball with center y' and radius $\varepsilon>0$. Moreover,

$$y_i=\sum_{k=1}^{K_i} z^c_{ik}(x')f^c_{ik}(w)+z^s_{ik}(x')f^s_{ik}(w),$$

is a continuous function w.r.t. w (denote $y=y(w)$), thus, there must exists an open ball $B_\sigma(w')$ such that $y(B_\sigma(w'))\subset B_\varepsilon(y')\subset\mathrm{Y}$, where $\sigma>0$. Besides, as $w'\in\overline{S}$ and S is dense in $\overline{S}$, there must exists $w_0\in B_\sigma(w')$, *i.e.*, there exists $t_0>0$ with $(a_1t_0,\dots,a_Nt_0)\in B_\sigma(w')$ and $y_0=y(w_0)\in B_\varepsilon(y')\subset\mathrm{Y}$. Hence, x',y_0,t_0 satisfy Ω. This completes the proof. ■

Until now, the problem described in section II-B has been equivalently reduced to Tarski's algebra, therefore, its decidability is obtained by [26]. That is,

Theorem 4: The problem described in (5) is decidable.

Remark 1: i) As *openness* of X and Y plays an important role in the proof of Theorem 3, our approach cannot be extended to the case when X and Y are arbitrary semi-algebraic sets.
ii) Additionally, as the density of S in $\overline{S}$ is guaranteed only if time goes infinity, our approach is not applicable to bounded reachability analysis.

Example 1: Given an LDS as

$$\begin{pmatrix}\dot{\xi_1}\\ \dot{\xi_2}\end{pmatrix}=\begin{pmatrix}2 & 2\\ -3 & -2\end{pmatrix}\begin{pmatrix}\xi_1\\ \xi_2\end{pmatrix}+\begin{pmatrix}cos(t)\\ sin(t)\end{pmatrix},$$

for an initial point $\xi(0)=(x_1,x_2)$, the solution is

$$\begin{aligned}&\Phi((x_1,x_2),t)= \\ &\begin{pmatrix}(x_1+2)\alpha_1+\sqrt{2}(x_1+x_2)\beta_1-2\alpha_2-\beta_2\\ (x_2-2)\alpha_1-\sqrt{2}(\frac{3}{2}x_1+x_2+1)\beta_1+2\alpha_2+2\beta_2\end{pmatrix},\end{aligned}$$

where $\alpha_1=cos(\sqrt{2}t)$, $\beta_1=sin(\sqrt{2}t)$, $\alpha_2=cos(t)$, $\beta_2=sin(t)$. Given initial set X and unsafe set Y as follows:

$$\mathrm{X}=\{(x_1,x_2)\mid x_1^2+x_2^2<1\}, \mathrm{Y}=\{(y_1,y_2)\mid y_1+y_2>4\},$$

we want to check whether this system is safe. From Theorem 3, we just need to check whether the following formula is satisfiable,

$$\begin{aligned}\mathscr{F}\;\hat{=}\; & x_1^2+x_2^2<1\wedge\alpha_1^2+\beta_1^2=1\wedge\alpha_2^2+\beta_2^2=1 \\ & \wedge(x_1+x_2)\alpha_1-\sqrt{2}(\frac{1}{2}x_1+1)\beta_1+\beta_2>4.\end{aligned}$$

It is easy to prove that there does not exist any x_1, x_2, α_1, α_2, β_1, $\beta_2 \in \mathbb{R}$ such that the above formula holds. Thus, the system is safe.

On the other hand, if replace the unsafe set Y by $\mathrm{Y}' = \{(y_1,y_2) \mid y_1+y_2 > 3\}$, then

$$\begin{aligned}\mathscr{F}' \ \hat{=}\ & x_1^2+x_2^2 < 1 \wedge \alpha_1^2+\beta_1^2 = 1 \wedge \alpha_2^2+\beta_2^2 = 1 \\ & \wedge (x_1+x_2)\alpha_1 - \sqrt{2}(\frac{1}{2}x_1+1)\beta_1+\beta_2 > 3.\end{aligned}$$

Let $x_1 = 0.99$, $x_2 = 0$, $\alpha_1 = \frac{\sqrt{5}}{5}$, $\beta_1 = -\frac{2\sqrt{5}}{5}$, $\alpha_2 = 0$, $\beta_2 = 1$, then $(x_1+x_2)\alpha_1 - \sqrt{2}(\frac{1}{2}x_1+1)\beta_1+\beta_2 \approx 3.334 > 3$. Thus, the system becomes unsafe.

IV. Abstraction of the General Case

In this section we deal with the most general case of LDS (1) and propose a verification method by abstraction. To this end, we introduce some basic notions first. A term is called a *polynomial-exponential-trigonometric function* (PETF) w.r.t. t, if it can be written as

$$\sum_{k=0}^{r} p_k(t)\mathrm{e}^{\alpha_k t}\cos(\beta_k t+\gamma_k),$$

where $r \in \mathbb{N}$, $\alpha_k, \beta_k, \gamma_k \in \mathbb{R}$ and $p_k(t) \in \mathbb{R}[t]$. In the rest of this paper, we assume that every component of the input $\mathbf{u}(t)$ of an LDS is a PETF.

The Jordan decomposition of a matrix $A \in \mathbb{R}^{n\times n}$ is as follows:

$$A = Q\begin{bmatrix} J_{n_1}(\lambda_1) & & \\ & \ddots & \\ & & J_{n_d}(\lambda_d)\end{bmatrix}Q^{-1}, \qquad (26)$$

where $Q \in \mathbb{C}^{n\times n}$ is an invertible matrix and $J_d(\lambda)$ represents the $d\times d$ Jordan block:

$$J_d(\lambda) = \begin{bmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & \lambda \end{bmatrix}.$$

A. Solution of General Case

Given an LDS of form (1), we shall reduce its solution of form (12) to a PETF vector. To this end, we first calculate the term $\mathrm{e}^{At}\mathbf{x}$. Let the Jordan decomposition of A be as in equation (26), and denote by $\lambda = [\lambda_1,\cdots,\lambda_d]$ the row vector of its eigenvalues. For convenience, we write $\mathbf{e}_\lambda(t) = [\mathrm{e}^{\lambda_1 t},\cdots,\mathrm{e}^{\lambda_d t}]$.

Lemma 1: For each $k \in \{1,2,\cdots,n\}$, we can find a $d\times n$ matrix $P_k(t)$ whose entries are in $\mathbb{R}[t]$, such that the kth row vector of e^{At} is represented as

$$(\mathrm{e}^{At})_{k,-} = \mathbf{e}_\lambda(t)P_k(t). \qquad (27)$$

Proof: Using the Jordan decomposition (26), we have

$$(\mathrm{e}^{At})_{k,-} = q_k\begin{bmatrix} \mathrm{e}^{J_{n_1}(\lambda_1)t} & & \\ & \ddots & \\ & & \mathrm{e}^{J_{n_d}(\lambda_d)t}\end{bmatrix}Q^{-1},$$

where q_k is the kth row vector of Q. Corresponding to the Jordan blocks, we write $q_k = [q_k^{(1)},\cdots,q_k^{(d)}]$ and $Q^{-1} = [R^{(1)},\cdots,R^{(d)}]^{\mathrm{T}}$, then we have

$$\begin{aligned}(\mathrm{e}^{At})_{k,-} &= \sum_{i=1}^{d} q_k^{(i)}\mathrm{e}^{J_{n_i}(\lambda_i)t}R^{(i)} = \sum_{i=1}^{d} q_k^{(i)}\mathrm{e}^{I_{n_i}\lambda_i t+J_{n_i}(0)t}R^{(i)} \\ &= \sum_{i=1}^{d}\mathrm{e}^{\lambda_i t}q_k^{(i)}\mathrm{e}^{J_{n_i}(0)t}R^{(i)} = \mathbf{e}_\lambda(t)P_k(t),\end{aligned}$$

where $P_k(t) = [q_k^{(1)}\mathrm{e}^{J_{n_1}(0)t}R^{(1)},\cdots,q_k^{(d)}\mathrm{e}^{J_{n_d}(0)t}R^{(d)}]^{\mathrm{T}}$ is a $d\times n$ matrix. Now we only need to prove that all entries of $q_k^{(i)}\mathrm{e}^{J_{n_i}(0)t}R^{(i)}$ are polynomials in t, which can be verified as follows:

$$\begin{aligned}\mathbf{v}^{\mathrm{T}}\mathrm{e}^{J_k(0)t}\mathbf{w} &= \mathbf{v}^{\mathrm{T}}\sum_{l=0}^{\infty}\frac{t^l}{l!}{J_k}^l(0)\mathbf{w} \\ &= \sum_{l=0}^{\infty}\frac{\mathbf{v}^{\mathrm{T}}{J_d}^k(0)\mathbf{w}}{l!}t^l = \sum_{l=0}^{k-1}\frac{\sum_{i=1}^{k-l}u_i v_{i+l}}{l!}t^l\end{aligned}$$

for any natural number k and two column vectors $\mathbf{v},\mathbf{w}$. ■

Note that the decomposition of form (27) can be computed by linear programming instead of by Jordan decomposition. In fact, defining an $n\times n$ matrix $Q_l(t)$ by $(Q_l(t))_{k,-} = (P_k(t))_{l,-}$ for all $k = 1,\cdots,n$ and $l = 1,\cdots,d$, it is equivalent to compute $Q_l(t)$ such that:

$$\mathrm{e}^{At} = \sum_l Q_l(t)\mathrm{e}^{\lambda_l t}. \qquad (28)$$

Now, let $\lambda_1,\cdots,\lambda_d$ be all of distinct eigenvalues of A, we choose $Q_l(t)$ to be an $n\times n$ matrix whose entries are polynomials in t of degree less than the algebraic multiplicity of λ_l, and solve all coefficients subject to the constraints

$$\begin{aligned}& Q_l'(t) = (A-\lambda_l I_d)Q_l(t),\ \forall l = 1,\cdots,d, \\ & \sum_{l=1}^{d} Q_l(0) = I_d.\end{aligned}$$

Note that the existence of the solution is guaranteed by Lemma 1 and the uniqueness is from Eq. (28). Then we obtain the decomposition of e^{At}.

It follows immediately from Eq. (27) that

$$(\mathrm{e}^{At}\mathbf{x})_k = \mathbf{e}_\lambda(t)P_k(t)\mathbf{x} = \sum_{i=1}^{d}(P_k(t)\mathbf{x})_i\mathrm{e}^{\lambda_i t}. \qquad (29)$$

Now we calculate the other term $\int_0^t \mathrm{e}^{A(t-\tau)}\mathbf{u}(\tau)\mathrm{d}\tau$ in (12). Since $\mathbf{u}(t)$ is a PETF, we can write it as $\mathbf{u}(t) = M(t)\mathbf{e}_\mu(t)$, where $M(t)$ is an $n\times m$ matrix whose entries are in $\mathbb{C}[t]$ and $\mathbf{e}_\mu(t) = [\mathrm{e}^{\mu_1 t},\cdots,\mathrm{e}^{\mu_m t}]^{\mathrm{T}}$ with $\mu = [\mu_1,\cdots,\mu_m]^{\mathrm{T}} \in \mathbb{C}^m$. For convenience, we define a polynomial $\mathrm{Int}_{k,\eta}(t)$ such that

$$\int_0^t \mathrm{e}^{\eta\tau}\tau^k\mathrm{d}\tau = \mathrm{e}^{\eta t}\mathrm{Int}_{k,\eta}(t) - \mathrm{Int}_{k,\eta}(0) \qquad (30)$$

for any $k \in \mathbb{N}$, $t \in \mathbb{R}$ and $\eta \in \mathbb{C}$. In fact, if $\eta = 0$ we can define $\mathrm{Int}_{k,0}(t) = t^{k+1}/(k+1)$. For $\eta \neq 0$, we inductively define a polynomial: $p_0(x) = 1,\ p_k(x) = x^k - kp_{k-1}(x)$. Then it is easy to verify that

$$\int_0^x \mathrm{e}^y y^k\mathrm{d}y = \mathrm{e}^x p_k(x) - p_k(0).$$

Thus we can define $\mathrm{Int}_{k,\eta}(t) = p_k(\eta t)/\eta^{k+1}$.

We have,

$$\begin{aligned}
&(\int_0^t \mathrm{e}^{A(t-\tau)}\mathbf{u}(\tau)\mathrm{d}\tau)_k \\
=&\int_0^t (\mathrm{e}^{A(t-\tau)}\mathbf{u}(\tau))_k\mathrm{d}\tau \quad \text{(Applying Eq. (29))} \\
=&\int_0^t \mathbf{e}_\lambda(t-\tau)P_k(t-\tau)\mathbf{u}(\tau)\mathrm{d}\tau \\
=&\int_0^t \mathbf{e}_\lambda(t-\tau)P_k(t-\tau)M(\tau)\mathbf{e}_\mu(\tau)\mathrm{d}\tau \\
=&\int_0^t \mathbf{e}_\lambda(t-\tau)\sum_{l=0}^{r} F_{k,l}(t)\tau^l\mathbf{e}_\mu(\tau)\mathrm{d}\tau \quad (*) \\
=&\sum_{l=0}^{r}\sum_{i=1}^{d}\sum_{j=1}^{m}\int_0^t \mathrm{e}^{\lambda_i(t-\tau)}(F_{k,l}(t))_{i,j}\mathrm{e}^{\mu_j\tau}\tau^l\mathrm{d}\tau \\
=&\sum_{l=0}^{r}\sum_{i=1}^{d}\sum_{j=1}^{m}\mathrm{e}^{\lambda_i t}(F_{k,l}(t))_{i,j}\int_0^t \mathrm{e}^{(\mu_j-\lambda_i)\tau}\tau^l\mathrm{d}\tau \text{ (Applying Eq.(30))} \\
=&\sum_{l=0}^{r}\sum_{i=1}^{d}\sum_{j=1}^{m}\mathrm{e}^{\lambda_i t}(F_{k,l}(t))_{i,j}(\mathrm{e}^{(\mu_j-\lambda_i)t}\mathrm{Int}_{l,\mu_j-\lambda_i}(t)-\mathrm{Int}_{l,\mu_j-\lambda_i}(0)) \\
=&\sum_{l=0}^{r}\sum_{i=1}^{d}\sum_{j=1}^{m}(F_{k,l}(t))_{i,j}(\mathrm{e}^{\mu_j t}\mathrm{Int}_{l,\mu_j-\lambda_i}(t)-\mathrm{e}^{\lambda_i t}\mathrm{Int}_{l,\mu_j-\lambda_i}(0)).
\end{aligned}$$

Here, we let $P_k(t-\tau)M(\tau) = \sum_{l=0}^{r} F_{k,l}(t)\tau^l$ in equation $(*)$, where $F_{k,l}(t)$ are $d \times m$ matrices whose entries are polynomials in t. Combining with Eq. (29), we have rewritten the solution of LDS (12) as follows:

$$(\xi(t))_k = (\mathrm{e}^{At}\mathbf{x})_k + (\int_0^t \mathrm{e}^{A(t-\tau)}\mathbf{u}(\tau)\mathrm{d}\tau)_k = \sum_{\eta\in\Psi} f_{\eta,k}(\mathbf{x},t)\mathrm{e}^{\eta t}$$

where $\Psi = \{\lambda_1, \cdots, \lambda_d, \mu_1, \cdots, \mu_m\}$, and $f_{\eta,k}(\mathbf{x},t)$ is polynomial in t and linear on $\mathbf{x}$. Note that $\mathrm{e}^{\eta t} = \mathrm{e}^{\alpha t}\cos(\beta t) + \mathbf{i}\sin(\beta t)$ for $\eta = \alpha + \mathbf{i}\beta$, $\alpha, \beta \in \mathbb{R}$. We put $\Gamma = \{\gamma \mid \gamma = \mathrm{Im}(\eta) \text{ for some } \eta \in \Psi\}$. Then it is easy to obtain that

$$(\xi(t))_k = \sum_{\gamma\in\Gamma} g_{\gamma,k}(\mathbf{x},t)\cos(\gamma t) + h_{\gamma,k}(\mathbf{x},t)\sin(\gamma t), \qquad (31)$$

where $g_{\gamma,k}$ and $h_{\gamma,k}$ are linear on $\mathbf{x}$, and are polynomial-exponential functions w.r.t. t.

B. Abstraction of Reachable Sets

Using the solution form (31) of LDS (1), the reachability of Y from X can be formally described as $\exists\mathbf{x}\exists\mathbf{y}\exists t : \Omega$, where

$$\begin{aligned}
\Omega \hat{=}\ & \mathbf{x} \in \mathrm{X} \wedge \mathbf{y} \in \mathrm{Y} \wedge t \geq 0 \wedge \\
& \bigwedge_{k=1}^{n} y_k = \sum_{\gamma\in\Gamma} g_{\gamma,k}(\mathbf{x},t)\cos(\gamma t) + h_{\gamma,k}(\mathbf{x},t)\sin(\gamma t).
\end{aligned}$$

The reachability problem of this form is generally undecidable due to the trigonometric functions in the formula. However, if there are no such functions it becomes decidable, and a decision procedure has been proposed in [10]. This fact hints us to eliminate the trigonometric functions by overapproximation of the reachable set, which is analogous to the procedure used in Section III-C.

We define the following formula:

$$\begin{aligned}
\Xi \hat{=}\ & \mathbf{x} \in \mathrm{X} \wedge \mathbf{y} \in \mathrm{Y} \wedge t \geq 0 \wedge \bigwedge_{\gamma} u_\gamma^2 + v_\gamma^2 = 1 \\
& \wedge \bigwedge_{k=1}^{n} y_k = \sum_{\gamma} g_{\gamma,k}(\mathbf{x},t)u_\gamma + h_{\gamma,k}(\mathbf{x},t)v_\gamma.
\end{aligned}$$

Then it follows immediately that

Theorem 5: $\exists x\exists y\exists t : \Omega \Rightarrow \exists x\exists y\exists t\forall\gamma \in \Gamma\exists u_\gamma\exists v_\gamma : \Xi$.

We can conclude, by Theorem 5, the system to be verified is safe, *i.e.*, Y is not reachable from X, as long as we can prove $\exists x\exists y\forall\gamma \in \Gamma\exists u_\gamma\exists v_\gamma\Xi$ does not hold.

V. Examples

To demonstrate the effectiveness of our technique which uses abstraction for general linear dynamical systems with complex eigenvalues, we have extended our tool called *LinR* [10] in Mathematica, which has been demonstrated more efficient than existing approaches based on approximation and numeric computation in general, *e.g.*, HSolver [22], dReach [17], FLOW* [5], etc. For systems with real or purely imaginary eigenvalues, the tool produces an exact result in finite time declaring the system "SAFE" or "UNSAFE"; while for systems with complex eigenvalues where overapproximation is used, the algorithm is guaranteed to terminate in a finite number of steps, either by finding a real counterexample (sample point) in the concrete system and declaring the system "UNSAFE", or by claiming the system "SAFE" when the abstracted system is safe, *i.e.* no counterexample is detected, or returning an "UNKNOWN" answer when the abstracted system is unsafe but the concrete system is safe, where only spurious counterexamples can be derived. In what follows, we illustrate our approach by several real-world examples.

A. Pond Pollution

Consider three ponds connected by streams, where the first pond has an external pollution source that spreads via the connecting streams to the other two ponds. Denote $x_1(t), x_2(t), x_3(t)$ as the amount (lbs) of pollutant in ponds 1, 2, 3 respectively, and t as the time in minutes. Assume that the pollutant is well-mixed in each pond, and we plan to verify that the amount of pollutant in pond 2 stays higher than that in pond 3 with an offset, 6 lbs for instance. By using a compartment analysis and instantiating the parameters[2], we obtain the specialized dynamics as

$$\begin{aligned}
\dot{x_1}(t) &= 0.001x_3(t) - 0.001x_1(t) + 0.01, \\
\dot{x_2}(t) &= 0.001x_1(t) - 0.001x_2(t), \\
\dot{x_3}(t) &= 0.001x_2(t) - 0.001x_3(t),
\end{aligned}$$

with the initial set $\mathrm{X} = \{(x_1,x_2,x_3)^T \mid (x_1-1)^2 + (x_2-1)^2 + (x_3-1)^2 < 1\}$ and the unsafe set $\mathrm{Y} = \{(y_1,y_2,y_3)^T \mid y_2 - y_3 + 6 < 0\}$. The safety property we are concerning is to check if some state in Y is reachable from X. Since $\mathrm{X} \cap \mathrm{Y} = \emptyset$, we

[2] For more details, please refer to `http://www.math.utah.edu/~gustafso/s2013/2250/systemsExamplesTheory2008.pdf`

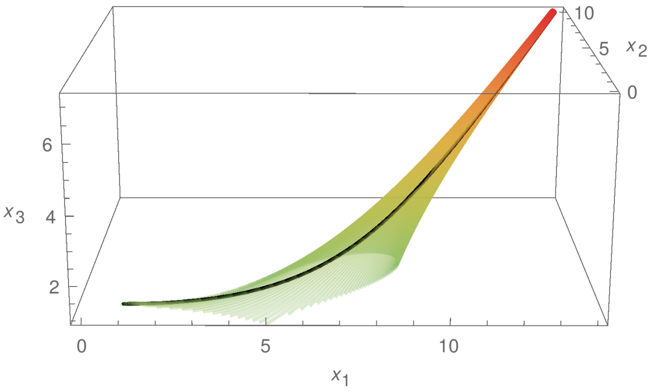

Fig. 1. Overapproximation of the trajectory starting from $(1,1,1)^T$

need further reduce the reachability problem to a quantifier elimination problem.

Observe that the system matrix is diagonalizable with three complex eigenvalues 0, $(-3-\mathbf{i}\sqrt{3})/2000$, and $(-3+\mathbf{i}\sqrt{3})/2000$. By using the solution of this system w.r.t. an initial state $(x_1,x_2,x_3)^T \in \mathrm{X}$, the reachability problem thus becomes

$$\begin{aligned}\mathscr{F} \hat{=} \exists x_1 \exists x_2 \exists x_3 \exists t : &(x_1-1)^2+(x_2-1)^2+(x_3-1)^2-1<0\\ &\wedge a+b\cos\left(\frac{\sqrt{3}t}{2000}\right)+c\sin\left(\frac{\sqrt{3}t}{2000}\right)<0\\ &\wedge t>0,\end{aligned}$$

where the second constraint corresponds to the unsafe set Y, with $a = 28e^{3t/2000}$, $b = 3x_2-3x_3-10$, and $c = \sqrt{3}(2x_1-x_2-x_3-10)$.

To further reduce the above problem to Tarski's algebra with exponentiations, we abstract the second constraint by eliminating trigonometric functions with overapproximation, *i.e.*

$$a+bu+cv<0 \wedge u^2+v^2=1. \tag{32}$$

As a quantifier elimination procedure, we can eliminate u and v in (32) by using the Cauchy-Schwarz inequality and thus get

$$a^2-b^2-c^2<0. \tag{33}$$

The reduced reachability problem is then successfully solved in *LinR* due to its kernel that implements CAD. The original system is verified to be safe inasmuch as no counterexamples of the abstracted system is derived, namely the overapproximation of the original system is safe. In a more intuitive way, Fig. 1 depicts the overapproximation (the tube) of one single trajectory (the curve) starting from $(1,1,1)^T$ initially. Note that the approximation tends to be tighter as the system evolves along with time, which is essentially on account of the intrinsic convergence of the original system. In other words, the system matrix has three eigenvalues whose real parts are all non-positive. This implies the stability property and thus makes our approach more competitive for checking properties in terms of a long span of time.

B. PID Controller

Consider a proportional-integral-derivative (PID) controller (taken from [21]) which is used to control a simple mass, spring, and damper problem. The modelling equation of the mass, spring, and damper system (plant) is

$$M\ddot{x}+b\dot{x}+kx=F$$

where $M=1kg, b=10Ns/m, k=20N/m$ are given parameters of the plant, and F is the controllable force. Suppose the goal is to control the plant to reach a steady state where $x=1$ with some requirements on the overshoot and rise time. Let $r(t)$ denote the desired trajectory for reaching the steady state $x=1$, which follows as a step function: $r(t)=0$ for $t<0$ and $r(t)=1$ for $t>0$.

Given a PID controller, the model describing the composed plant and controller is

$$M\ddot{x}+b\dot{x}+kx \;=\; K_d(r\dot{-}x)+K_p(r-x)+K_i\int(r-x)$$

where K_d, K_p and K_i are parameters indicating gains of the derivative, proportional and integral respectively, while $r-x$ is the error in tracking the desired trajectory r.

We consider the case of using a PI controller, *i.e.* $K_d=0$, and choose $K_p=350$ and $K_i=300$. We will prove the following property of the system using our approach:

$$\mathbf{G}(t>0.5 \Rightarrow x \geq 0.9 \wedge x \leq 1.1). \tag{34}$$

Note that this case has been studied in [21] but unfortunately it cannot be proved by the method proposed there.

Let $\mathbf{x} = [\int x, x, \dot{x}, t]^{\mathrm{T}}$, then $\dot{\mathbf{x}} = A\mathbf{x}+\mathbf{u}$, where

$$A = \begin{bmatrix} 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ -300 & -370 & -10 & 300\\ 0 & 0 & 0 & 0 \end{bmatrix}$$

and $\mathbf{u} = [0,0,350,1]^{\mathrm{T}}$. The initial value is $\mathbf{x}(0) = [0,0,0,0]$ and unsafe set is $Y = \{\mathbf{x} \mid t>0.5 \wedge (x<0.9 \vee x>1.1)\}$. Now the problem has been written in the form of reachability of an LDS. The eigenvalues of A are $0, \lambda_0, \lambda_1$, and λ_2, where λ_i $(i=0,1,2)$ are roots of the characteristic equation $f(\lambda) = \lambda^3+10\lambda^2+370\lambda+300$. Solving the LDS we get

$$x = 1+c_0\lambda_0 \mathrm{e}^{\lambda_0 t}+c_1\lambda_1\mathrm{e}^{\lambda_1 t}+c_2\lambda_2\mathrm{e}^{\lambda_2 t},$$

where

$$\begin{bmatrix} c_0\\ c_1\\ c_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1\\ \lambda_0 & \lambda_1 & \lambda_2\\ \lambda_0^2 & \lambda_1^2 & \lambda_2^2 \end{bmatrix}^{-1} \begin{bmatrix} 1/15\\ -1\\ 0 \end{bmatrix}.$$

Observe that $f(\lambda)$ has only one real root, denoted by λ_0, and by λ_1 and λ_2 the other two conjugate complex roots. Let $\lambda_{1,2} = \alpha \pm \beta\mathbf{i}$, then the solution can be rewritten as

$$x = 1+c_0\lambda_0\mathrm{e}^{\lambda_0 t}+2\mathrm{e}^{\alpha t}(\mathrm{Re}(c_1\lambda_1)\cos(\beta t)-\mathrm{Im}(c_1\lambda_1)\sin(\beta t)).$$

Now by abstraction, we put $u=\cos(\beta t)$, $v=\cos(\beta t)$ and require that $u^2+v^2=1$. Then the reachability of Y becomes

$$\begin{aligned}&\exists u \exists v \exists t : u^2+v^2=1 \wedge t>0.5 \wedge\\ &(\phi(u,v,t)<-0.1 \vee \phi(u,v,t)>0.1),\end{aligned} \tag{35}$$

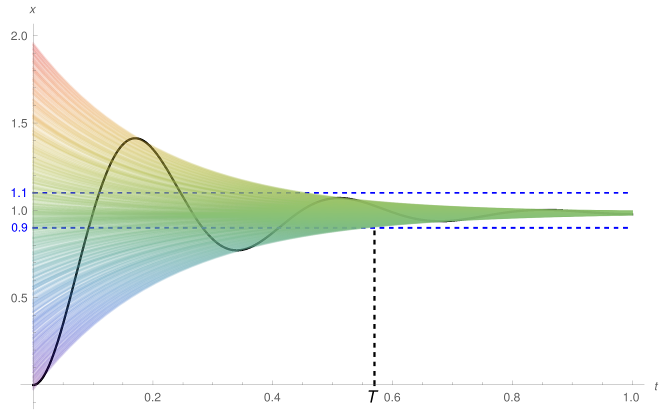

Fig. 2. Overapproximation (the “broom”) of the trajectory of x (the curve) starting from 0. Here the two horizontal dashed lines specify the boundaries of the safe set, while T indicates a point in time, after which the behaviour of the overapproximated system stays within the safe region.

where $\phi(u,v,t) = c_0\lambda_0 \mathrm{e}^{\lambda_0 t} + 2(\mathrm{Re}(c_1\lambda_1)u - \mathrm{Im}(c_1\lambda_1)v)\mathrm{e}^{\alpha t}$. Then using the method proposed in [10], we prove that (i) $\phi(u,v,t) > 0.1$ is invalid, and thus $x \leq 1.1$ in Eq. (34) is verified; and (ii) the interval $(0.5, T]$ covers all t that make $\phi(u,v,t) < -0.1$ satisfiable in Eq. (35). Here T is the unique root of $|c_0\lambda_0|\mathrm{e}^{\lambda_0 t} + 2|c_1\lambda_1|\mathrm{e}^{\alpha t} - 0.1$, which can be approximated by real root isolation with arbitrary precision. We adopt 0.6 as an overapproximation of T here (see Fig. 2).

Using our method it has been shown that Y can only be reached when t is in $(0.5, 0.6]$. Moreover, it can be checked by bounded model checking or simulation based verification [11], [16] that even for $t \in (0.5, 0.6]$ Y can not be reached. Therefore, we have proved the property (34) for the given system.

VI. Conclusions

In this paper, we first identified a family of vector fields, whose state parts are linear, but with pure imagine eigenvalues, while input parts are trigonometric expressions, and proved its reachability problem is decidable. This essentially extends the third case in Lafferriere et al.’s work [19]. Together with our previous work in [10], this advances the state of the art on the decidability of the reachability problems of dynamical and hybrid systems.

In addition, we presented an approach on how to abstract computing the reachable sets of general linear dynamical systems to the decidability of a theory of specific *polynomial-exponential* functions we considered in [10]. Comparing with existing abstractions for linear dynamical systems, experimental results indicate that our abstraction is more precise.

Acknowledgement

The authors would like to thank Dr. Ming Xu for insightful discussions on the density results in number theory. The first and fourth authors are supported partly by NSFC under grants 11290141, 11271034 and 61532019; the second, third and fifth authors are supported partly by “973 Program” under grant No. 2014CB340701, by NSFC under grant 91418204, by CDZ project CAP (GZ 1023), and by the CAS/SAFEA International Partnership Program for Creative Research Teams.

References

[1] M. Achatz, S. McCallum, and V. Weispfenning. Deciding polynomial-exponential problems. In *ISSAC’08*, pages 215–222, 2008.

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

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

[4] C. W. Brown. Improved projection for cylindrical algebraic decomposition. *J. Symb. Comput.*, 32(5):447–465, 2001.

[5] X. Chen, E. Ábrahám, and S. Sankaranarayanan. Flow*: An analyzer for non-linear hybrid systems. In *CAV’13*, volume 8044 of *LNCS*, pages 258–263, 2013.

[6] G. E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decompostion. In *2nd GI Conference on Automata Theory and Formal Languages*, pages 134–183, 1975.

[7] G. E. Collins and H. Hong. Partial cylindrical algebraic decomposition for quantifier elimination. *J. Symb. Comput.*, 12(3):299–328, 1991.

[8] J. H. Davenport and J. Heintz. Real quantifier elimination is doubly exponential. *J. Symb. Comput.*, 5(1):29–35, 1988.

[9] P. S. Duggirala and A. Tiwari. Safety verification for linear systems. In *EMSOFT’13*, pages 7:1–7:10, 2013.

[10] T. Gan, M. Chen, L. Dai, B. Xia, and N. Zhan. Decidability of the reachability for a family of linear vector fields. In *ATVA’15*, volume 9364 of *LNCS*, pages 482–499, 2015.

[11] A. Girard and G. Pappas. Verification using simulation. In *HSCC’06*, volume 3927 of *LNCS*, pages 272–286, 2006.

[12] J. Han, L. Dai, and B. Xia. Constructing fewer open cells by GCD computation in CAD projection. In *ISSAC’14*, pages 240–247, 2014.

[13] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers (5th ed.).* Oxford University Press, Oxford, 1979.

[14] T. A. Henzinger, P. W. Kopke, A. Puri, and P. Varaiya. What’s decidable about hybrid automata? *Journal of Computer and System Sciences*, 57(1):94–124, 1998.

[15] H. Hong. An improvement of the projection operator in cylindrical algebraic decomposition. In *ISSAC’90*, pages 261–264. ACM, 1990.

[16] Z. Huang and S. Mitra. Computing bounded reach sets from sampled simulation traces. In *HSCC’12*, pages 291–294, 2012.

[17] S. Kong, S. Gao, W. Chen, and E. Clarke. dReach: Delta-reachability analysis for hybrid systems. In *TACAS’15*, volume 9035 of *LNCS*, pages 200–205, 2015.

[18] G. Lafferriere, G. J. Pappas, and S. Sastry. O-minimal hybrid systems. *MCSS*, 13(1):1–21, 2000.

[19] G. Lafferriere, G. J. Pappas, and S. Yovine. Symbolic reachability computation for families of linear vector fields. *J. Symb. Comput.*, 32:231–253, 2001.

[20] S. McCallum. An improved projection operation for cylindrical algebraic decomposition of three-dimensional space. *J. Symb. Comput.*, 5(1):141–161, 1988.

[21] S. Mover, A. Cimatti, A. Tiwari, and S. Tonetta. Time-aware relational abstractions for hybrid systems. In *EMSOFT’13*, pages 14:1–14:10, 2013.

[22] S. Ratschan and Z. She. Safety verification of hybrid systems by constraint propagation based abstraction refinement. In *HSCC’05*, volume 3414 of *LNCS*, pages 573–589. 2005.

[23] A. Strzeboński. Solving systems of strict polynomial inequalities. *J. Symb. Comput.*, 29(3):471–480, 2000.

[24] A. Strzeboński. Real root isolation for exp-log functions. In *ISSAC ’08*, pages 303–314. ACM, 2008.

[25] A. Strzeboński. Cylindrical decomposition for systems transcendental in the first variable. *J. Symb. Comput.*, 46:1284–1290, 2011.

[26] A. Tarski. *A Decision Method for Elementary Algebra and Geometry.* University of California Press, Berkeley, 1951.