





Reachability Analysis for Solvable Dynamical Systems

Ting Gan , Mingshuai Chen , Yangjia Li , Bican Xia , and Naijun Zhan 

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. In the literature, only some special families of linear vector fields are proved with decidable reachability problem, let alone nonlinear ones. In this paper, we investigate the reachability problem of nonlinear vector fields by identifying three families of nonlinear vector fields with solvable and prove that their reachability problems are decidable. An n -dimension dynamical system is called *solvable* if its state variables can be partitioned into m groups such that the derivatives of the variables in the i th group are linear in themselves, but possibly nonlinear in the variables from the 1st to $i - 1$ th groups. The three families of nonlinear solvable vector fields under consideration are: the matrices corresponding to the linear parts of any vector field in the first family are nilpotent; the matrices corresponding to the linear parts of any vector in the second family are only with real eigenvalues; the matrices corresponding to the linear parts of any vector field in the third family are only with pure imaginary eigenvalues. The experimental results indicate the efficiency of our approach.

Index Terms—Hybrid systems (HS), reachability analysis, solvable systems (SSs), Tarski's algebra.

I. INTRODUCTION

HYBRID systems (HSs) integrate computation with physical processes: embedded computers and networks monitor and control physical processes and feedback loops con-

Manuscript received May 25, 2017; revised August 28, 2017; accepted September 18, 2017. Date of publication October 19, 2017; date of current version June 26, 2018. The work of T. Gan and B. Xia was supported in part by NSFC under Grant 61732001, Grant 11290141, Grant 11271034, and Grant 61532019. The work of M. Chen, Y. Li, and N. Zhan was supported in part by "973 Program" under Grant 2014CB340701, in part by NSFC under Grant 61625206, Grant 61732001, and Grant 61502467, in part by CDZ Project CAP (GZ 1023), and in part by the CAS/SAFEA International Partnership Program for Creative Research Teams. Recommended by Associate Editor A. Girard. (Corresponding authors: Bican Xia and Naijun Zhan.)

T. Gan is with the State Key Laboratory of Software Engineering, Wuhan University, Wuhan 430072, China (e-mail: ganting@pku.edu.cn).

M. Chen and N. Zhan are with State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China, and also with the University of Chinese Academy of Sciences, Beijing 100049, China (e-mail: chenms@ios.ac.cn; znj@ios.ac.cn).

Y. Li is with the State Key Laboratory of Computer Science, Institute of Software, Beijing 100190, China (e-mail: yangjia@ios.ac.cn).

B. Xia is with the LMAM & School of Mathematical Sciences, Peking University, Beijing 100871, China (e-mail: xbc@math.pku.edu.cn).

Color versions of one or more of the figures in this paper are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/TAC.2017.2763785

tinuously influence computations, which are known as cyber-physical systems (CPSs) nowadays. Applications of CPS span over many safety-critical domains, e.g., communication, health-care, manufacturing, aerospace, transportation, etc. To guarantee the correctness of these systems is vital so that we can bet our lives on them, and challenging [40]. Therefore, formal methods has 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 intangibly interaction between continuous evolutions and discrete transitions, the reachability problem of most of HSs is undecidable [21], except for some simple cases, either their vector fields, i.e., their continuous evolution parts, are quite simple such as timed automata [4] and multirate automata [3], or there are very restrictive constraints on their discrete transitions such as o-minimal HSs [26].

In [27], Lafferriere *et al.* investigated vector fields of the form

$$\dot{\xi} = A\xi + \mathbf{u} \quad (1)$$

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 $\mathbf{u} : \mathbb{R} \rightarrow \mathbb{R}^n$ is a piecewise continuous function, which is called the *input*. They obtained the decidability of the reachability problems of the following three families of vector fields:

- 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_i s are rationals and c_i s are subject to semialgebraic constraints.
- 3) A is *diagonalizable* with purely imaginary eigenvalues, whose imaginary parts are rationals, and each component of \mathbf{u} of the form $\sum_{i=1}^m c_i \sin(\lambda_i t) + d_i \cos(\lambda_i t)$, where λ_i s are rationals and c_i s and d_i s are subject to semialgebraic constraints.

The above results are achieved by reducing the problems into Tarski's algebra [39].

In [5], Anai and Weispfenning presented a systematic approach on how to reduce the reachability problem and control parameter set problem of parametric inhomogeneous linear differential systems, with the form¹

$$\dot{\xi} = A\xi + \mathbf{u}(t, \mathbf{r}) \quad (2)$$

where $A \in \mathbb{R}^{n \times n}$ is an $n \times n$ matrix, $\mathbf{r} = (r_1, \dots, r_k)$ is a vector of parameters, to the transcendental implicitization problem of a fundamental system of solutions of $\dot{\xi} = A\xi$ by quantifier

¹This form can be generalized to $\dot{\xi} = A(t)\xi + \mathbf{u}(t, \mathbf{r})$.

elimination. They further proved (see [5, Corollary 2]) that exact semialgebraic implicitization is possible for a fundamental system of solutions of $\dot{\xi} = A\xi$ if and only if one of the following cases holds:

- 1') All eigenvalues of A are zero, i.e., A is nilpotent.
- 2') All eigenvalues $\lambda_1, \dots, \lambda_n$ of A are nonzero, pairwise distinct reals, and $\dim_{\mathbb{Q}}(\text{span}(\lambda_1, \dots, \lambda_n)) \leq 1$.
- 3') All eigenvalues $\lambda_1, \dots, \lambda_n$ of A are purely imaginary, say of the form $\lambda_i = \mu_i \mathbf{i}$ with nonzero, pairwise distinct reals μ_i s, and $\dim_{\mathbb{Q}}(\text{span}(\mu_1, \dots, \mu_n)) \leq 1$.

Obviously, Anai and Weispfenning's work extended Lafferriere *et al.*'s further, and particularly proved the largest families of linear vector fields whose exact reachable set computations are computable by reduction to Tarski's algebra.

In [16] and [17], we extended the decidability results of reachability problems of linear vector fields due to Lafferriere *et al.* [27] and Anai and Weispfenning [5].

- 1) In [16], we generalized the above cases 2) and 2') to the following:
 - a) 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_i s are reals and c_i s are subject to semialgebraic constraints.

Note that compared with [5, case 2')], we dropped the constraint $\dim_{\mathbb{Q}}(\text{span}(\lambda_1, \dots, \lambda_n)) \leq 1$, which restrict the eigenvalues to be linearly dependent over \mathbb{Q} . Such extension is substantial, since the new family is strictly more expressive, whose reachability problem cannot be essentially reduced to Tarski's algebra any more as in [5] and [27]. To obtain the decidability, we have to resort to the decidability of the extension of Tarski's algebra with functions of the form

$$f(t, \mathbf{x}) = \sum_{i=0}^m f_i(t, \mathbf{x}) e^{\lambda_i t} \quad (3)$$

where $m \in \mathbb{N}$, $f_i(t, \mathbf{x}) \in \mathbb{R}[t, \mathbf{x}]$, $\lambda_i \in \mathbb{R}$, $i = 0, 1, \dots, m$, and e is an irrational and transcendental number approximately equal to 2.718281828459. We denote the extension by \mathcal{T}_e .

- 2) In [17], we generalized the above cases 3) and 3') to the following:
 - a) 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_i s are reals and c_i s and d_i s are subject to semialgebraic constraints.

This is still achieved by reducing the decidability to Tarski's algebra [39] using the density results in number theory [20], rather either by direct replacement such as [27] or by reduction to the transcendental implicitization problem such as [5]. Note that compared to [5, case 3')], we dropped the constraint $\dim_{\mathbb{Q}}(\text{span}(\mu_1, \dots, \mu_n)) \leq 1$.

It is also worth noting that for linear vector fields, some other problems that are quite related to the reachability problem have been investigated and proved to be decidable in the literature, such as the polytope escape problem [32], Recurrent reachability problem [8], and the Skolem problem [9]. But a main restriction on all of the results is that the unsafe set should only be linear and represented as a polyhedra, whereas in our results, the unsafe

set can be nonlinear and represented by a semialgebraic set. For an effective verification method for the reachability problem of the former case, we refer to Yazarel and Pappas's work [43].

Tarski's algebra is the first-order theory of reals over the structure $\langle \mathbb{R}; +, -, \cdot, 0, 1 \rangle$, which is also called the elementary algebra and geometry. In [39], Tarski showed the decidability of Tarski's algebra. But whether the extension of Tarski's algebra with exponentiation over real closed fields is decidable (so-called "Tarski's conjecture") is still open. In [2] and [30], Weispfenning *et al.* gave a partial solution to Tarski's conjecture by showing the decidability of the extension of Tarski's algebra by allowing terms of the form $f(t, \mathbf{x}, e^t)$, where $f(t, \mathbf{x}, y) \in \mathbb{R}[t, \mathbf{x}, y]$. In [41], Xu *et al.* considered how to generalize Weispfenning *et al.*'s approach by allowing functions of the form (3), but with the restriction that all the λ_i s are nonnegative integers. Obviously, \mathcal{T}_e is strictly more expressive than the ones considered in [2], [30], and [41].

In the literature, there is very little decidability results on the reachability problems of nonlinear vector fields. The first decidability results are given in [42] on the reachability problems for some specific solvable nonlinear vector fields, which are proper subsets of the second family below we consider, by exploiting Weispfenning *et al.*'s result on Tarski's conjecture [2]. In this paper, we investigate this issue by identifying three families of solvable vector fields and proving their reachability problems are decidable by exploiting the techniques developed in our previous work [16], [17], which are the three largest nonlinear vector fields with decidable reachability to the best of our knowledge.

The notion of *solvability* was first proposed in [35] for a class of polynomial programs, and was extended to dynamical and HSs in [42]. Formally, a dynamical system

$$\dot{\xi} = F(\xi, \mathbf{u}(t))$$

is called *solvable system* (SS) if the variable vector $\xi = (\xi_1, \dots, \xi_n)$ can be classified into m groups ($m \leq n$)

$$\zeta_1 = (\xi_{11}, \dots, \xi_{1n_1}), \dots, \zeta_m = (\xi_{m1}, \dots, \xi_{mn_m})$$

and the dynamical system can be represented as the form:

$$\dot{\xi} = \begin{bmatrix} \dot{\zeta}_1 \\ \dot{\zeta}_2 \\ \vdots \\ \dot{\zeta}_m \end{bmatrix} = \begin{bmatrix} A_1 \zeta_1 + \mathbf{u}_1(t) \\ A_2 \zeta_2 + \mathbf{u}_2(t, \zeta_1) \\ \vdots \\ A_m \zeta_m + \mathbf{u}_m(t, \zeta_1, \dots, \zeta_{m-1}) \end{bmatrix} \quad (4)$$

where $0 < n_1 < \dots < n_m = n$ are integers, $m \in \mathbb{N}$, A_1, \dots, A_m are real matrices with corresponding dimensions, $\mathbf{u}_1, \dots, \mathbf{u}_m$ are *polynomial-exponential-trigonometric functions* (PETFs, the definition will be given later). For example

$$\begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \end{bmatrix} = \begin{bmatrix} x + e^{-t} \\ 2y + x^2 - e^{-\sqrt{2}t} \\ \sqrt{3}z + xy + 2e^{-t} \end{bmatrix} \quad (5)$$

is a SS, which is beyond the expression of the linear system. Obviously, all linear dynamical systems (LDSs) are also SSs.

Thus, the main contributions of this paper can be summarized as follows:

- 1") If A_1, \dots, A_m in (4) are *nilpotent*, i.e., $A_1^{k_1} = 0, \dots, A_m^{k_m} = 0$, for some $k_1, \dots, k_m \in \mathbb{N}$, and each

component of \mathbf{u}_i is a polynomial, then the reachability problem of (4) is decidable. This is achieved by reduction to Tarski's algebra similarly to [27].

- 2") If each A_i is *diagonalizable* with real eigenvalues, and each component of \mathbf{u}_i is of the form $\sum_{j=1}^{m_i} c_{ij} e^{\lambda_{ij} t}$, where λ_{ij} s are reals and c_{ij} s are subject to semialgebraic constraints, then the reachability problem of (4) is decidable, where $i = 1, \dots, m$. The technique adopted for this case is adapted from [16]. In [16], it is assumed that any expression of \mathcal{T}_e has no multiple real roots, we will drop such restriction in this paper.
- 3") If each A_i is *diagonalizable* with purely imaginary eigenvalues, whose imaginary parts are reals, and each component of \mathbf{u}_i of the form $\sum_{j=1}^{m_i} c_{ij} \sin(\lambda_{ij} t) + d_{ij} \cos(\lambda_{ij} t)$, where λ_{ij} s are reals and c_{ij} s and d_{ij} s are subject to semialgebraic constraints, the reachability problem of (4) is decidable, where $i = 1, \dots, m$. The technique adopted for this case is essentially same as what we used in [17], but the reduction procedure is more complicated for the nonlinear case.

Additionally, similar to [5] and [17], we present an abstraction of general solvable dynamical systems of the form (4). That is,

- 1) each A_i is a real matrix, and each component of \mathbf{u}_i is of the form $\sum_{k=0}^{r_i} p_{ik}(t) \exp^{\alpha_{ik} t} \cos(\beta_{ik} t + \gamma_{ik})$, where $i = 1, \dots, m$, $r_i \in \mathbb{N}$, $\alpha_{ik}, \beta_{ik}, \gamma_{ik} \in \mathbb{R}$, and $p_{ik}(t) \in \mathbb{R}[t]$.

The basic idea of our approach is as follows: For each eigenvalue $\alpha \pm \beta i$ of A_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 (4) can be essentially represented as the form

$$f(t, \mathbf{x}, \mathbf{a}, \mathbf{b}) = \sum_{i=0}^m \sum_{j=0}^{n_i} f_{ij}(t, \mathbf{x}, \mathbf{a}, \mathbf{b}) e^{\alpha_{ij} t}.$$

Clearly, constraints over such expressions together with all the derived constraints fall into the decidable theory \mathcal{T}_e .

We implement a prototypical tool of our approach, and some case studies are conducted. To demonstrate the efficiency of our approach, first, we compare our tool with CT1D [38], a generalized CAD implementation of Mathematica's Reduce command, which can cope with quantifier elimination of \mathcal{T}_e . For \mathcal{T}_e formulas only with strict inequalities, our tool outperforms CT1D, and for the rest cases, their efficiencies are nearly same. As other state-of-the-art tools for quantifier elimination, e.g., REDLOG [14], QEPCAD, and SyNRAC [24] cannot handle the decidability problems we considered in this paper in general, it is thus not comparable. Second, we also compare our tool with several well-known reachability computation tools based on approximation and numeric computation, e.g., HSolver [33], FLOW* [7], dReach [25], etc., although such comparisons are not fairly as they deal with different problems in general. After necessary preprocessing in order to make the comparison reasonable, our tool is more efficient.

II. PRELIMINARIES

In this section, we first introduce some basic notions and theories, then explain the problem we consider. We use \mathbf{x} to stand for a vector variable (x_1, \dots, x_n) , $\mathbb{N}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ for natural, rational, real, and complex numbers, respectively, $\mathbb{R}[\mathbf{x}]$ for the

polynomial ring in \mathbf{x} with coefficients in \mathbb{R} in what follows. We denote by $\Lambda(M)$ the set of all the eigenvalues of matrix M . For any $c \in \mathbb{C}$, denote by $\mathbf{Im}(c)$ the imaginary part of c .

A. Basic Notions

A term $f(t, \mathbf{x})$ is called *polynomial-exponential function* (PEF) w.r.t. t if it can be written in the form of (3).

A term $f(t, \mathbf{x})$ is called *trigonometric function* (TMF) w.r.t. t if it can be written with the following form:

$$f(t, \mathbf{x}) = \sum_{l=1}^r c_l(\mathbf{x}) \cos(\mu_l t) + d_l(\mathbf{x}) \sin(\mu_l t) \quad (6)$$

where $r \in \mathbb{N}$, $c_l(\mathbf{x}), d_l(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$, and $\mu_l \in \mathbb{R}$, $l = 1, \dots, r$. Denote by $\Gamma(f(t, \mathbf{x}))$ the set $\{\mu_1, \mu_2, \dots, \mu_r\}$ in the sequel.

A term $f(t, \mathbf{x})$ is called a *polynomial-exponential-trigonometric function* (PETF) w.r.t. t , if it can be written with the following form:

$$f(t, \mathbf{x}) = \sum_{k=0}^r p_k(t, \mathbf{x}) e^{\alpha_k t} \cos(\beta_k t + \gamma_k) \quad (7)$$

where $r \in \mathbb{N}$, $\alpha_k, \beta_k, \gamma_k \in \mathbb{R}$, and $p_k(t, \mathbf{x}) \in \mathbb{R}[t, \mathbf{x}]$. Obviously, PEFs and TMFs are PETFs as $\sin(\alpha)$ can be seen as $\cos(\frac{\pi}{2} + \alpha)$.

A function vector is said to be PEF (TMF or PETF) if every component is a PEF (TMF or PETF).

A set $X \subset \mathbb{R}^n$ is said to be *semialgebraic* if it is defined as

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

for some polynomials $p_1(\mathbf{x}), \dots, p_j(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$, where $\triangleright \in \{>, >\}$ and $j \in \mathbb{N}$. X is called *open semialgebraic* if there is a ball $b_\delta(\mathbf{x})$ such that $b_\delta(\mathbf{x}) \subseteq X$, where δ is the radius and \mathbf{x} is the center of the ball, for any $\mathbf{x} \in X$.

B. Density Results in Number Theory

In this part, we introduce some theoretical results on density in number theory.

Definition 1 (Rational linear independent): Let a_1, \dots, a_k are some real numbers. We say a_1, \dots, a_k are *rational linear independent* if $\sum_{i=1}^k c_i a_i = 0$ implies $\bigwedge_{i=1}^k c_i = 0$, for all $c_1, \dots, c_k \in \mathbb{Q}$.

Definition 2 (Basis): Let $A \subset \mathbb{R}$ with $\#(A) \leq +\infty$ be a set of real numbers, where $\#(A)$ means the number of elements in 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 $a \in A \setminus B$, where $A \setminus B$ denotes the set of all the elements in A but not in B , then the elements in $\{a\} \cup B$ are not rational linear independent.

Let $A = \{a_1, \dots, a_k\}$ be a set of real number, $B = \{b_1, \dots, b_j\} \subseteq A$ be a basis of A . It is easy to see that for any $a_i \in A$, there exists $c = (c_{i1}, \dots, c_{ij}) \in \mathbb{Q}$ such that $a_i = c_{i1} b_1 + \dots + c_{ij} b_j$. For $1 \leq l \leq j$, let $d_l = \text{lcm}(\text{denom}(c_{1l}), \dots, \text{denom}(c_{kl}))$ where $\text{denom}(c)$ is the denominator of rational number c and lcm means the least common multiple. Let $\bar{B} = \{\frac{b_1}{d_1}, \dots, \frac{b_j}{d_j}\}$ be a basis of A , then for any $a \in A$, a can be written as an integer linear combination of the elements in \bar{B} . We call such basis \bar{B} an *integer-basis* of A .

The following Kronecker Theorem gives a nice density property of a rational or integer linear independent set [20].

Theorem 1 (Kronecker): The set $\{(\{\xi_1 t\}_1, \dots, \{\xi_k t\}_1) \mid t \in \mathbb{N}\}$ is dense in $[0, 1]^k$, if $1, \xi_1, \dots, \xi_k$ are integer linear

independent, where $\{\xi\}_1 \in [0, 1)$ is the decimal part of the real number ξ .

Corollary 1: The set $\{(\{\xi_1 t\}_{2\pi}, \dots, \{\xi_k t\}_{2\pi}) \mid t \geq 0\}$ is dense in $[0, 2\pi]^k$, if ξ_1, \dots, ξ_k are integer linear independent, where $\{\xi\}_{2\pi} \in [0, 2\pi)$ is the remainder of ξ by 2π .

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

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

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

Since ξ_1, \dots, ξ_k are integer linear independent, ξ'_1, \dots, ξ'_k are also integer linear independent. Thus, it is easy to see that there exists $\xi_0 > 0$ such that $1, \xi_0 \xi'_1, \dots, \xi_0 \xi'_k$ are integer linear independent. By Theorem 1, it follows

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

is dense in $[0, 1]^k$. As $\xi_0 > 0$ implies $\{\xi_0 n \mid n \in \mathbb{N}\} \subset \{t \mid t \geq 0\}$, we have that the set in (9) is a subset of the set in (8). Thus, the set in (8) is dense in $[0, 1]^k$. ■

Theorem 2: Let a_1, \dots, a_k be rational linear independent, and

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

$$\bar{S} = \left\{ (\alpha_1, \beta_1, \dots, \alpha_k, \beta_k) \in \mathbb{R}^{2k} \mid \bigwedge_{i=1}^k \alpha_i^2 + \beta_i^2 = 1 \right\} \quad (11)$$

then S is dense in \bar{S} .

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

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

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

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

C. Problem

Given an SS of the form (4) and an initial state $\xi(0) = \mathbf{x}$, the solution of this system at time $t \geq 0$ is denoted by $\xi(t) = \Phi(\mathbf{x}, t)$. Then, the *forward reachable set* $Post(X)$ of (4) from a given set X is defined as follows:

$$Post(X) = \{\mathbf{y} \in \mathbb{R}^n \mid \exists \mathbf{x} \exists t : \mathbf{x} \in X \wedge t \geq 0 \wedge \Phi(\mathbf{x}, t) = \mathbf{y}\}. \quad (12)$$

The safety problem is: given an initial set X and an unsafe set Y , verify whether any unsafe state in Y is not reachable by some trajectory starting from X , i.e., whether $Post(X) \cap Y = \emptyset$. Let

$$\mathcal{F}(X, Y) = \exists \mathbf{x} \exists \mathbf{y} \exists t : \mathbf{x} \in X \wedge \mathbf{y} \in Y \wedge t \geq 0 \wedge \Phi(\mathbf{x}, t) = \mathbf{y}. \quad (13)$$

That is, the safety problem is to verify whether the formula $\mathcal{F}(X, Y)$ is true or false. If it is false then the safety property holds, otherwise the safety property does not hold.

III. NILPOTENT

In this section, we compute the solution form of an SS of (4) in which all the matrices A_1, \dots, A_m are nilpotent and all u_1, u_2, \dots, u_m are polynomials, and show the solution is a polynomial in $\mathbb{R}[\mathbf{x}, t]$ by induction on the number of blocks of variables.

We first prove it when $m = 1$, i.e., the linear case.

Lemma 1: Given a linear system $\dot{\xi} = A\xi + \mathbf{u}(t)$ satisfying $A \in \mathbb{R}^{n_1 \times n_1}$ is a nilpotent matrix, and $\mathbf{u}(t) \in \mathbb{R}[t]^{n_1}$, a given initial point $\mathbf{x} \in \mathbb{R}^{n_1}$, the solution $\Phi(\mathbf{x}, t)$ of the linear system is a polynomial in $\mathbb{R}[\mathbf{x}, t]$.

Proof: Clearly, in this case

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

Since $A \in \mathbb{R}^{d \times d}$ is a nilpotent matrix, $A^k = 0$ for any $k \geq d$. Thus, $e^{At} = \sum_{k=0}^{d-1} \frac{t^k}{k!} A^k$. Moreover,

$$\Phi(\mathbf{x}, t) = \sum_{k=0}^{d-1} \frac{t^k}{k!} A^k \mathbf{x} + \int_0^t \left(\sum_{k=0}^{d-1} \frac{(t-\tau)^k}{k!} A^k \mathbf{u}(\tau) \right) d\tau.$$

As A, \dots, A^{d-1} are all real matrices in $\mathbb{R}^{n_1 \times n_1}$, it is easy to see that $\sum_{k=0}^{d-1} \frac{t^k}{k!} A^k \mathbf{x}$ is a polynomial vector in \mathbf{x} and t , and $\sum_{k=0}^{d-1} \frac{(t-\tau)^k}{k!} A^k \mathbf{u}(\tau)$ is a polynomial vector in \mathbf{x}, t and τ . Hence

$$\int_0^t \left(\sum_{k=0}^{d-1} \frac{(t-\tau)^k}{k!} A^k \mathbf{u}(\tau) \right) d\tau$$

is a polynomial in \mathbf{x} and t . Thus

$$\sum_{k=0}^{d-1} \frac{t^k}{k!} A^k \mathbf{x} + \int_0^t \left(\sum_{k=0}^{d-1} \frac{(t-\tau)^k}{k!} A^k \mathbf{u}(\tau) \right) d\tau$$

is a polynomial vector in \mathbf{x} and t , i.e., $\Phi(\mathbf{x}, t) \in \mathbb{R}[\mathbf{x}, t]^{n_1}$. ■

Theorem 3: Given an SS as (4) in which all the matrices A_1, \dots, A_m are nilpotent and all $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_m$ are polynomial vectors, then for a given initial point \mathbf{x} , the solution $\Phi(\mathbf{x}, t)$ is a polynomial vector in $\mathbb{R}[\mathbf{x}, t]^n$, where $n = n_1 + \dots + n_m$.

Proof: Let $\mathbf{x} = (\mathbf{z}_1, \dots, \mathbf{z}_m)$ correspond to $(\zeta_1, \dots, \zeta_m)$ in (4). For ζ_1 , by Lemma 1, we know $\zeta_1(t, \mathbf{x}) \in \mathbb{R}[\mathbf{x}, t]^{n_1}$.

Now, suppose that $\zeta_1(t, \mathbf{x}), \dots, \zeta_{k-1}(t, \mathbf{x})$ are all polynomial vectors in $\mathbb{R}[\mathbf{x}, t]^{n_1}, \dots, \mathbb{R}[\mathbf{x}, t]^{n_{k-1}}$, respectively, for $k \leq m$. We prove that $\zeta_k \in \mathbb{R}[\mathbf{x}, t]^{n_k}$. Since $\mathbf{u}_k(t, \zeta_1, \dots, \zeta_{k-1})$ is a polynomial vector, substituting $\zeta_1(t, \mathbf{x}), \dots, \zeta_{k-1}(t, \mathbf{x})$ for $\zeta_1, \dots, \zeta_{k-1}$ in $\mathbf{u}_k(t, \zeta_1, \dots, \zeta_{k-1})$, it follows $\mathbf{u}_k(t, \zeta_1, \dots, \zeta_{k-1}) = \mathbf{u}_k(t, \mathbf{x}) \in \mathbb{R}[\mathbf{x}, t]^{n_k}$. Thus, the subdynamical system w.r.t. ζ_k is reduced to $\dot{\zeta}_k = A_k \zeta_k + \mathbf{u}_k(t, \mathbf{x})$. By Lemma 1, this implies that $\zeta_k(t, \mathbf{x})$ is a polynomial vector. All in all, the solution $\Phi(\mathbf{x}, t) \in \mathbb{R}[\mathbf{x}, t]^n$. ■

Thus, (13) becomes decidable according to the decidability of Tarski algebra [39]. That is

Theorem 4: The problem (13) is decidable.

IV. REAL EIGENVALUES

In this section, we give a decision procedure to the problem (13) when all A_i s are only with real eigenvalues and all \mathbf{u}_i s are PEF vectors in (4).

A. Reduction to the Decision Problem of \mathcal{T}_e

In this part, we prove that the reachability problem above can be reduced to the decision problem of \mathcal{T}_e , therefore is decidable under the assumption of *Schanuel's conjecture* according to Strzeboński's result in [38].

Before proving the solution of (4) in this case can be represented as PEFs, we first show some properties on PEFs.

Lemma 2: The set of PEFs is closed under *add, subtract, multiply, and integral operations*.

Proof: It is easy to see that the set of PEFs is closed under add, subtract, and multiply operations. For the integral operation, since

$$\begin{aligned} \int e^{\lambda t} dt &= \frac{1}{\lambda} e^{\lambda t}, \quad \text{and} \\ \int t^n e^{\lambda t} dt &= \frac{t^n}{\lambda} e^{\lambda t} - \frac{nt^{n-1}}{\lambda^2} e^{\lambda t} + \dots + (-1)^n \\ &\quad \times \frac{n(n-1)\dots 1t}{\lambda^{n+1}} e^{\lambda t} \end{aligned}$$

the integral of a PEF is still PEF. ■

Lemma 3: Let $A \in \mathbb{R}^{n \times n}$ has real eigenvalues only, then e^{At} is a matrix with dimension $n \times n$, and all entries of e^{At} are PEFs.

Proof: Let J be the Jordan normal form of A , so there exist an invertible matrix Q such that $A = QJQ^{-1}$. Then, it follows $e^{At} = Qe^{Jt}Q^{-1}$. Let $J = \text{diag}(J_1, J_2, \dots, J_m)$, where J_1, J_2, \dots, J_m are the corresponding Jordan blocks. Then

$$e^{At} = Qe^{Jt}Q^{-1} = Q \begin{bmatrix} e^{J_1 t} & & & \\ & e^{J_2 t} & & \\ & & \ddots & \\ & & & e^{J_m t} \end{bmatrix} Q^{-1}.$$

Without loss of generality, we just need to prove that all the elements of $e^{J_1 t}$ are PEFs. Suppose that the dimension of J_1 is $d \times d$ and the diagonal entry is λ , i.e.

$$J_1 = \lambda I + \begin{bmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix}.$$

Denote the second summand of J_1 by M , obviously $M^d = 0$. So, we have

$$\begin{aligned} e^{J_1 t} &= e^{\lambda t I} \cdot e^{Mt} \\ &= e^{\lambda t I} \cdot \left(I + tM + \frac{t^2}{2} M^2 + \dots + \frac{t^{d-1}}{(d-1)!} M^{d-1} \right) \\ &= \begin{bmatrix} e^{\lambda t} & & & \\ & e^{\lambda t} & & \\ & & \ddots & \\ & & & e^{\lambda t} \end{bmatrix} \cdot \begin{bmatrix} 1 & t & \dots & \frac{t^{d-1}}{(d-1)!} \\ & 1 & t & \dots \\ & & \ddots & \\ & & & 1 \end{bmatrix}. \end{aligned}$$

Hence, all the entries of $e^{J_1 t}$ are PEFs, and so are all entries of e^{At} . ■

Theorem 5: Given an SS of (4) in which all A_i s are only with real eigenvalues and all \mathbf{u}_i s are PEF vectors, and an initial $\mathbf{x} \in \mathbb{R}^n$, then its solution $\Phi(\mathbf{x}, t)$ can be represented as of the

following form

$$(\Phi(\mathbf{x}, t))_i = \sum_{j=1}^{s_i} \phi_{ij}(\mathbf{x}, t) e^{\nu_{ij} t} \quad (14)$$

for $i = 1, \dots, n$, where $\phi_{ij}(\mathbf{x}, t) \in \mathbb{R}[\mathbf{x}, t]$, $J_i \in \mathbb{N}$ and $\nu_{ij} \in \mathbb{R}$ for $i = 1, \dots, n, j = 1, \dots, s_i$.

Proof: Let $\mathbf{x} = (\mathbf{z}_1, \dots, \mathbf{z}_m)$ corresponding to $(\zeta_1, \dots, \zeta_m)$ in (4).

We proceed the proof by induction on m .

When $m = 1$, thus the SS (4) becomes a linear system. Whence, the solution is

$$\zeta_1(t, \mathbf{x}) = e^{A_1 t} z_1 + \int_0^t e^{A_1(t-\tau)} u_1(\tau) d\tau.$$

By Lemma 3, it follows that all entries in $e^{A_1 t}$ and $e^{A_1(t-\tau)}$ are PEFs. Moreover, using Lemma 2, we have $e^{A_1 t} z_1 + \int_0^t e^{A_1(t-\tau)} u_1(\tau) d\tau$ is a PEF. Hence, $\zeta_1(t, \mathbf{x})$ is a PEF vector.

Now, suppose that $\zeta_1(t, \mathbf{x}), \dots, \zeta_{k-1}(t, \mathbf{x})$, $k < m$, are all PEF vectors, we prove that $\zeta_k(t, \mathbf{x})$ is also a PEF vector. Since $\mathbf{u}_k(t, \zeta_1, \dots, \zeta_{k-1})$ and $\zeta_1, \dots, \zeta_{k-1}$ are all PEF vectors, substituting $\zeta_1(t, \mathbf{x}), \dots, \zeta_{k-1}(t, \mathbf{x})$ for $\zeta_1, \dots, \zeta_{k-1}$ in $\mathbf{u}_k(t, \zeta_1, \dots, \zeta_{k-1})$, it follows $\mathbf{u}_k(t, \zeta_1, \dots, \zeta_{k-1}) = \mathbf{u}_k(t, \mathbf{x})$ is a PEF vector. Thus, the sub-dynamical system w.r.t. ζ_k is reduced to $\dot{\zeta}_k = A_k \zeta_k + \mathbf{u}_k(t, \mathbf{x})$. From the basis case, this implies that $\zeta_k(t, \mathbf{x})$ is a PEF vector.

In a word, the solution $\Phi(\mathbf{x}, t)$ is a PEF vector, i.e., each of its component is of the form $(\Phi(\mathbf{x}, t))_i = \sum_{j=1}^{s_i} \phi_{ij}(\mathbf{x}, t) e^{\nu_{ij} t}$ for $i = 1, \dots, n$, where $\phi_{ij}(\mathbf{x}, t) \in \mathbb{R}[\mathbf{x}, t]$, $J_i \in \mathbb{N}$, and $\nu_{ij} \in \mathbb{R}$ for $i = 1, \dots, n, j = 1, \dots, s_i$. ■

Example 1:

$$\begin{bmatrix} \dot{\xi}_1 \\ \dot{\xi}_2 \\ \dot{\xi}_3 \end{bmatrix} = \begin{bmatrix} \xi_1 \\ \xi_1 - \xi_2 + e^t \\ -\xi_3 + \xi_1^2 \end{bmatrix}$$

with an initial state $\mathbf{x} = (x_1, x_2, x_3) \in \mathbb{R}^3$, the corresponding solution is

$$\begin{aligned} \xi_1(t, \mathbf{x}) &= e^t x_1 \\ \xi_2(t, \mathbf{x}) &= \left(\frac{x_1}{2} + \frac{1}{2} \right) e^t - \left(\frac{x_1}{2} + \frac{1}{2} - x_2 \right) e^{-t} \\ \xi_3(t, \mathbf{x}) &= \frac{x_1^2}{3} e^{2t} - \left(\frac{x_1^2}{3} - x_3 \right) e^{-t} \end{aligned}$$

which are PEFs.

Since X and Y are two semialgebraic sets, there exist polynomials $p_1(\mathbf{x}), \dots, p_J(\mathbf{x})$ such that

$$X = \{ \mathbf{x} \in \mathbb{R}^n \mid p_1(\mathbf{x}) \triangleright 0, \dots, p_{J_1}(\mathbf{x}) \triangleright 0 \}$$

$$Y = \{ \mathbf{x} \in \mathbb{R}^n \mid p_{J_1+1}(\mathbf{x}) \triangleright 0, \dots, p_J(\mathbf{x}) \triangleright 0 \}$$

where $\triangleright \in \{ \geq, > \}$. Then, (13) can be reduced to verify whether

$$\mathcal{F}(X, Y) = \exists \mathbf{x} \exists \mathbf{y} \exists t : \Omega \quad (15)$$

holds, where

$$\begin{aligned} \Omega &= p_1(\mathbf{x}) \triangleright 0 \wedge \cdots \wedge p_{J_1}(\mathbf{x}) \triangleright 0 \wedge p_{J_1+1} \\ &\quad \times (\mathbf{y}) \triangleright 0 \wedge \cdots \wedge p_J(\mathbf{y}) \triangleright 0 \wedge t \geq 0 \wedge \bigwedge_{i=1}^n y_i \\ &= \sum_{j=1}^{s_i} \phi_{ij}(\mathbf{x}, t) e^{\nu_{ij} t}. \end{aligned}$$

B. Decision Procedure for \mathcal{T}_e

In this part, we give a decision procedure for \mathcal{T}_e based on *cylindrical algebraic decomposition* (CAD), due to Collins [10].

The basic idea of CAD is: Given a set S of polynomials in $\mathbb{R}[\mathbf{x}]$, CAD is used to partition \mathbb{R}^n into connected semialgebraic sets, called *cells*, such that each polynomial in S keeps constant *sign* (either +, - or 0) on each *cell*. As CAD plays a fundamental role in computer algebra and real algebraic geometry, in the literature, a numerous works are done on improvement of CAD, e.g., [6], [11], [13], [19], [22], [29]. When constraints are open sets, GCAD [36] or openCAD [19] is enough, which partitions the space \mathbb{R}^n into a set of *open cells* instead of *cells* (i.e., takes sample points from open cells only), such that on each of which every polynomial in S keeps constant nonzero *sign* (either + or -). For example, suppose $f_1 = y - x$, $f_2 = y + x$. The graphs of $f_1 = 0$ and $f_2 = 0$ decompose \mathbb{R}^2 into 9 cells with different dimensions: Four of which are two-dimensional (open) cells (i.e., $f_1 \sim 0 \wedge f_2 \sim 0$, where $\sim \in \{>, <\}$); four of which are one-dimensional cells (i.e., $f_1 \sim 0 \wedge f_2 = 0$, $f_1 = 0 \wedge f_2 \sim 0$, where $\sim \in \{>, <\}$); and one of which is zero-dimensional cell (i.e., $f_1 = 0 \wedge f_2 = 0$). Complete CAD takes at least one sample point from each of the nine cells, while GCAD or openCAD takes at least one sample point only from each of the four two-dimensional (open) cells. Formally

Definition 3: For a polynomial $f(x_1, \dots, x_n) \in \mathbb{R}[x_1, \dots, x_n]$, a CAD (openCAD) defined by f under the order $x_1 < x_2 < \cdots < x_n$ is a set of sample points in \mathbb{R}^n obtained through the following three phases:

Projection: Apply CAD (openCAD) projection operator on f to get a set of projection polynomials $\{f_n = f(x_1, \dots, x_n), f_{n-1}(x_1, \dots, x_{n-1}), \dots, f_1(x_1)\}$.

Base: Choose a rational point in each of the (open) intervals defined by the real roots of f_1 .

Lifting: Substitute each sample point in \mathbb{R}^{i-1} for (x_1, \dots, x_{i-1}) in f_i to get a univariate polynomial $f'_i(x_i)$, and then, as in Base phase, choose sample points for $f'_i(x_i)$. Repeat this process for i from 2 to n .

Using CAD (openCAD), we develop a decision procedure for \mathcal{T}_e as follows:

Step 1: Check whether $X \cap Y = \emptyset$, if not, it is easy to see that (15) holds.

Step 2: Translate the problem to an openCAD solvable problem if X and Y are open sets, otherwise a CAD solvable problem. By (14), $y_i(\mathbf{x}, t) = \sum_{j=1}^{s_i} \phi_{ij}(\mathbf{x}, t) e^{\nu_{ij} t}$. So, we can replace $p_j(\mathbf{y})$ with $p_j(y(\mathbf{x}, t))$, which is polynomial in \mathbf{x} and polynomial-exponential in t , abbreviated as $p_j(\mathbf{x}, t)$, for $j = J_1 + 1, \dots, J$. Simply, we define $p_j(\mathbf{x}, t)$ as $p_j(\mathbf{x})$, for $j = 1, \dots, J_1$. Thus, $\mathcal{F}(X, Y)$ in (15) can be reformulated as $\mathcal{F} = \exists \mathbf{x} \exists t \bigwedge_{j=1}^J p_j(\mathbf{x}, t) \triangleright 0 \wedge t \geq 0$.

Step 3: Eliminate x_1, \dots, x_n one by one using CAD (openCAD) projection operator on $\prod_{j=1}^J p_j$ and obtain a set of projection polynomials $\{q_n(x_1, \dots, x_n, t) = \prod_{j=1}^J p_j, q_{n-1}(x_2, \dots, x_n, t), \dots, q_0(t)\}$.

Step 4: Isolate the real roots of the resulted PEF q_0 based on *Rolle's theorem*, which will be elaborated in the next section.

Step 5: Lift the solution using openCAD or CAD lifting procedure corresponding to Step 2 according to the order t, x_n, \dots, x_1 based on $\{q_0, \dots, q_n\}$, and obtain a set S of *sample points*.

Step 6: Check if \mathcal{F} holds by testing if there exists α in S such that $\bigwedge_{j=1}^J p_j(\alpha) \triangleright 0$.

In [38], Strzeboński presented another decision procedure for \mathcal{T}_e completely based on CAD. Our decision procedure differentiates from Strzeboński's in the following points:

- 1) When all constraints are open sets, our method is based on openCAD, which requires less computation compared to the corresponding complete CAD, as we do not need to consider the cells that are represented as roots of equations involving PEFs, which are extremely difficult, during the base and lifting phases in openCAD. Therefore, as indicated later in the experiments, our decision procedure is more efficient in this case. But the two decision procedures share the same complexity in general case.
- 2) In [38], an algorithm for isolating real roots of a given PEF based on *weak Fourier sequence* [37] is given. It is claimed that the algorithm is *complete* under the assumption of *Schanuel's conjecture* [34]. Whereas, in this paper, we give another algorithm to isolate real roots of the resulted PEF $q_0(t)$ based on *Rolle's theorem*. We prove that our approach is also *complete* under the assumption that $q_0(t)$ does not have any multiple real roots, which can be implied by *Schanuel's conjecture*.

C. Isolating Real Roots of PEFs

In this part, we give an algorithm PEFIsolation to isolate the finitely many real roots of a PEF.

Definition 4: Consider a PEF in t as

$$f(t) = \sum_{i=0}^s f_i(t) e^{\nu_i t} \quad (16)$$

where $s \in \mathbb{N}$, $0 \neq f_i \in \mathbb{R}[t]$ and $\nu_i \in \mathbb{R}$ are pairwise different. *Real root isolation* of the equation $f(t) = 0$ is to obtain a set of intervals $\{I_j = (a_j, b_j) \mid a_j, b_j \in \mathbb{R} \wedge a_j < b_j, j = 1, \dots, J\}$ such that $I_i \cap I_j = \emptyset$ if $i \neq j$, in each I_j there exists only one real root of $f(t)$, and all real roots of $f(t)$ are contained in $\bigcup_{j=1}^J I_j$.

Given an open interval I , *real root isolation* of $f(t)$ over I can be defined similarly.

Without loss of generality, in (16), we can assume

$$0 = \nu_0 < \nu_1 < \nu_2 < \cdots < \nu_s, f_i(t) \neq 0, \text{ for } i = 0, 1, \dots, s \quad (17)$$

since we can always multiply out by $e^{\nu_0 t}$ for the smallest ν_0 to ensure this happens. When $s = 1$ or every ν_i ($0 \leq i \leq s$) is a positive integer, in [2], an algorithm named ISOL was proposed to isolate all real roots of $f(t)$. This algorithm can

be easily extended to the case when all ν_i ($i = 0, \dots, s$) are rationals or there exists a nonzero real number κ such that for every $0 \leq i \leq s$, $\nu_i \kappa$ is a rational.

1) Lower and Upper Bounds on Real Roots: Similar to [2], we can prove the following theorem, which indicates that there is a lower and upper bound on real roots for any given PEF.

Theorem 6 (Upper bound): Let $f(t)$ be a PEF of the form (16). Then, we can obtain an upper bound C on its real roots through the following procedure:

- 1) Find $C_1 \geq 0$, $M > 0$ such that for all $t > C_1$, $|f_s(t)| > \frac{1}{sM}$.
- 2) Find $C_2 \geq 0$ and $k \in \mathbb{N}$ such that for all $t > C_2$ and for all $0 \leq i < s$, $|f_i(t)| < \frac{t^k}{sM}$.
- 3) Find $C_3 \geq 0$ such that for all $t > C_3$, $t^k < e^{(\nu_s - \nu_{s-1})t}$.
- 4) Set $C = \max\{C_1, C_2, C_3\}$.

Proof: Let $t > C$, then we have $|f_s(t)| > \frac{1}{sM}$, $t^k < e^{(\nu_s - \nu_{s-1})t}$, $|f_i(t)| < \frac{t^k}{sM}$, for $i = 0, \dots, s-1$. Whence

$$\begin{aligned} |f_0(t) + \sum_{i=1}^{s-1} f_i(t)e^{\nu_i t}| &\leq |f_0(t)| + \sum_{i=1}^{s-1} |f_i(t)e^{\nu_i t}| < \frac{t^k}{sM} \\ &+ \sum_{i=1}^{s-1} \frac{t^k}{sM} e^{\nu_i t} \\ &< \frac{t^k}{sM} e^{\nu_{s-1} t} + \sum_{i=1}^{s-1} \frac{t^k}{sM} e^{\nu_{s-1} t} = \frac{1}{M} t^k e^{\nu_{s-1} t} < \frac{1}{M} e^{\nu_s t} \\ &< |f_s(t)e^{\nu_s t}|. \end{aligned}$$

Thus, $|f_0(t) + \sum_{i=1}^{s-1} f_i(t)e^{\nu_i t}| < |f_s(t)e^{\nu_s t}|$, and we have $f_0(t) + \sum_{i=1}^{s-1} f_i(t)e^{\nu_i t} + f_s(t)e^{\nu_s t} \neq 0$. This implies $f(t) \neq 0$ for any $t \geq C$. So C is an upper bound on the real roots of $f(t)$. ■

In order to get a lower bound, a commonly used method is to replace $f(t)$ with $g(t) = f(-t)e^{\nu_s t}$. Then, by Theorem 6, there is an upper bound B on the real roots of $g(t) = 0$. It is easy to see that $-B$ is a lower bound on the real roots of $f(t) = 0$. Thus, we see that all roots of $f(t) = 0$ are in the interval $(-B, C)$. In what follows, we denote by $L(f) = -B$, $U(f) = C$, the lower and upper bounds on the real roots of $f(t)$, respectively.

2) Algorithm: In this part, we present our algorithm PE-FISOLATION for isolating all real roots of a given nonzero PEF $f(t)$ of the form (16).

Definition 5: Let $f(t)$ be a nonzero PEF of the form (16), then we define

$$\begin{aligned} \text{coff}(f) &\hat{=} (f_0, f_1, \dots, f_s)^T, \text{nu}(f) \hat{=} (0, \nu_1, \dots, \nu_s)^T \\ \text{deg}(f) &\hat{=} (\text{deg}(f_0), \text{deg}(f_1), \dots, \text{deg}(f_s))^T \end{aligned}$$

where $\text{deg}(g)$ means the degree of g , and as a convention, $\text{deg}(0) = -1$. So, (16) can be shorten as

$$f(t) = \text{coff}(f)^T \cdot e^{\text{nu}(f)t}$$

where $e^{\text{nu}(f)t} = (1, e^{\nu_1 t}, \dots, e^{\nu_s t})^T$, $\mathbf{a} \cdot \mathbf{b}$ stands for the inner product of the two vectors, i.e., $\sum_{i=1}^n a_i b_i$.

From Definition 5, it follows

$$\begin{aligned} \text{coff}(f') &= (f'_0, f'_1 + \nu_1 f_1(t), \dots, f'_s + \nu_s f_s(t))^T, \text{nu}(f') \\ &= (0, \nu_1, \dots, \nu_s)^T \end{aligned}$$

$$\text{deg}(f') = (\max\{\text{deg}(f_0) - 1, -1\}, \text{deg}(f_1), \dots, \text{deg}(f_s))^T$$

where f' denotes the derivative of f w.r.t. t .

In the following, we will explain the basic idea behind PE-FISOLATION through the following simple example.

Example 2: Consider $\hat{f}(t) = t + 1 + e^{\sqrt{2}t} - (t+2)e^{\sqrt{5}t}$.

First, in order to isolate the real roots of $\hat{f}(t) = 0$, we need to calculate the upper and lower bounds on all its real roots according to Theorem 6.

Regarding the upper bound of $\hat{f}(t) = 0$, we have: 1) $C_1 = 0$, $M = 1$, $\forall t \geq 0$, $|t+2| > 1$; 2) $C_2 = 4$, $k = 2$, $\forall t \geq 4$, $|t+1| < \frac{t^2}{2}$, $1 < \frac{t^2}{2}$; 3) $C_3 = 12$, $\forall t \geq 12$, $t^2 < e^{(\sqrt{5}-\sqrt{2})t}$. Thus, we obtain $U(\hat{f}) = 12$.

In order to obtain the lower bound, we have to calculate the upper bound $U(g)$ of $g(t) = \hat{f}(-t)e^{\sqrt{5}t}$, i.e., $g(t) = t - 2 + e^{(\sqrt{5}-\sqrt{2})t} - (t-1)e^{\sqrt{5}t}$. Because 1) $\bar{C}_1 = 3$, $M = 1$, $\forall t \geq 3$, $|t-1| > 1$; 2) $\bar{C}_2 = 4$, $k = 2$, $\forall t \geq 4$, $|t-2| < \frac{t^2}{2}$, and $1 < \frac{t^2}{2}$; 3) $\bar{C}_3 = 1$, $\forall t \geq 1$, and $t^2 < e^{\sqrt{2}t}$, we obtain the upper bound $U(g) = 4$.

Therefore, the lower bound $L(\hat{f}) = -U(g) = -4$ is obtained. Obviously, all real roots of $\hat{f}(t) = 0$ should be in the interval $(-4, 12)$, which implies that we just need to isolate all real roots in $(-4, 12)$.

From *differential mean value theorem* (i.e., *Rolle's theorem*), we know there must exist at last one real root of $f'(t) = 0$ between every two real roots of $f(t) = 0$, if $f(t)$ is continuous differentiable. In order to obtain the real roots of $f(t) = 0$, we can try to get the real roots of $f'(t) = 0$ first. Likewise, in order to obtain the real roots of $f'(t) = 0$, we can try to get the real roots of $f''(t) = 0$ first. We can repeat the above procedure until the real solutions of the i th derivative of $f(t)$ for some i can be achieved. Then, we lift the real solutions of the respective derivative in the inverse order until $f(t)$ itself. We illuminate the procedure by continuing the running example.

At the beginning,

$$S_0 = \hat{f}(t) = t + 1 + e^{\sqrt{2}t} - (t+2)e^{\sqrt{5}t}$$

$$\text{coff}(S_0) = (t + 1, 1, -t - 2)^T$$

$$\text{nu}(S_0) = (0, \sqrt{2}, \sqrt{5})^T, \text{deg}(S_0) = (1, 0, 1)^T.$$

Then, we obtain the derivative of \hat{f} is

$$S_1 = \hat{f}'(t) = 1 + \sqrt{2}e^{\sqrt{2}t} - (\sqrt{5}t + 2\sqrt{5} + 1)e^{\sqrt{5}t}$$

$$\text{coff}(S_1) = (1, \sqrt{2}, -\sqrt{5}t - 2\sqrt{5} - 1)^T$$

$$\text{nu}(S_1) = (0, \sqrt{2}, \sqrt{5})^T, \text{deg}(S_1) = (0, 0, 1)^T.$$

Furthermore, the derivative of \hat{f}' is

$$\hat{f}''(t) = 0 + 2e^{\sqrt{2}t} - (5t + 2\sqrt{5} + 10)e^{\sqrt{5}t}$$

$$\text{coff}(\hat{f}'') = (0, 2, -5t - 2\sqrt{5} - 10)^T$$

$$\text{nu}(\hat{f}'') = (0, \sqrt{2}, \sqrt{5})^T, \text{deg}(\hat{f}'') = (-1, 0, 1)^T.$$

Clearly, \hat{f}'' and the following S_2 share the same real roots:

$$S_2 = \hat{f}''(t)e^{-\sqrt{2}t} = 2 - (5t + 2\sqrt{5} + 10)e^{(\sqrt{5}-\sqrt{2})t} \quad (18)$$

$$\text{coeff}(S_2) = (0, 2, -5t - 2\sqrt{5} - 10)^T$$

$$\text{nu}(S_2) = (0, 0, \sqrt{5} - \sqrt{2})^T, \text{deg}(S_2) = (-1, 0, 1)^T. \quad (19)$$

Now, the derivative of S_2 is

$$S_3 = S_2' = 0 + 0 + he^{(\sqrt{5}-\sqrt{2})t}, \text{coeff}(S_3) = (0, 0, h)^T$$

$$\text{nu}(S_3) = (0, 0, \sqrt{5} - \sqrt{2})^T, \text{deg}(S_3) = (-1, -1, 1)^T$$

where $h = -(5(\sqrt{5} - \sqrt{2})t + 15 + 10\sqrt{5} - 2\sqrt{10} - 10\sqrt{2})$. Obviously, $S_3 = 0$ if and only if $h = 0$, while the real zeros of h can be easily achieved by any real root isolation procedure for polynomials [12].

Remark 1: In general, suppose $S_i(t) = f_0(t) + \sum_{j=1}^J f_j(t)e^{\nu_j t}$ with $0 \neq f_j(t) \in \mathbb{R}[t]$, $0 < \nu_1 < \dots < \nu_J$, and $0 < J \in \mathbb{N}$, then we define $S_{i+1}(t) = S_i'(t)$ if $f_0'(t) \neq 0$; otherwise, $S_{i+1}(t) = S_i'(t)e^{-\nu_1 t} = (f_1'(t) + \nu_1 f_1(t)) + \sum_{j=2}^J (f_j'(t) + \nu_j f_j(t))e^{(\nu_j - \nu_1)t}$. It is obvious that $S_{i+1} = 0$ shares the same real roots of $S_i'(t) = 0$. We construct S_{i+1} from S_i , for $i = 0, \dots$. This procedure terminates when S_k is a polynomial for some k .

Theorem 7: Let $f(t)$ be a PEF, $f'(t)$ the derivative of $f(t)$ w.r.t. t , $I = (a, b)$ a nonempty open interval, and $\mathcal{L}_I(f') = \{I_j | j = 1, \dots, J\}$ a real root isolation of f' in I , in which $I_j = (a_j, b_j)$ with $a = b_0 < a_1 < b_1 < \dots < a_J < b_J < a_{J+1} = b$. Furthermore, $f(t)$ has no real roots in any closed interval $[a_j, b_j]$, $1 \leq j \leq J$. Then, $\{(b_j, a_{j+1}) | f(b_j)f(a_{j+1}) < 0, 0 \leq j \leq J\}$ is a real root isolation of $f(t)$ in I .

Proof: Since $f(t)$ has no real roots in any closed interval $[a_j, b_j]$, $1 \leq j \leq J$, all real roots of $f(t)$ are in $\bigcup_{j=0}^J (b_j, a_{j+1})$ and $f(b_j)f(a_{j+1}) \neq 0$. Moreover, $f(t)$ has at most one real root in each (b_j, a_{j+1}) , otherwise, there must be at least one real root of $f'(t) = 0$ on it by *Rolle's theorem*, which is a contradiction with the definition of $\mathcal{L}_I(f')$. So, if $f(b_j)f(a_{j+1}) < 0$, then there exists only one real root of $f(t)$ in (b_j, a_{j+1}) , otherwise no real root of $f(t)$ in (b_j, a_{j+1}) . ■

Now, let us continue the running example. As $e^{(\sqrt{5}-\sqrt{2})t} \neq 0$, by $S_3 = he^{(\sqrt{5}-\sqrt{2})t} = 0$, it follows $h(t) = 0$. Thus, $t = \frac{-15+10\sqrt{5}-2\sqrt{10}-10\sqrt{2}}{5(\sqrt{5}-\sqrt{2})} \in (-5, -4)$. As $(-5, -4) \cap (-4, 12) = \emptyset$, there is no real root of $S_3 = 0$ in $(-4, 12)$. Hence, we have $\mathcal{L}(S_3) = \emptyset$. In addition, from (18), we have

$$S_2(-4) = 2 + (10 - 2\sqrt{5})e^{-4(\sqrt{5}-\sqrt{2})} > 0$$

$$S_2(12) = 2 - (70 + 2\sqrt{5})e^{12(\sqrt{5}-\sqrt{2})} < 0.$$

So, there exists only one real root of S_2 in $(-4, 12)$ by Theorem 7. Clearly, the real root isolation of S_2 in $(-4, 12)$ is same as that of \hat{f}'' .

In order to construct $\mathcal{L}_{(-4,12)}(S_1)$, a real root isolation of S_1 in $(-4, 12)$, from $\mathcal{L}_{(-4,12)}(S_2)$ by Theorem 7, the condition that there is no real root of S_1 in $[a, b]$ for any (a, b) in $\mathcal{L}_{(-4,12)}(S_2)$ should be guaranteed. This means that we have to refine the intervals in $\mathcal{L}_{(-4,12)}(S_2)$ until the condition holds. This is achieved by Algorithm 2 below (see lines 2–13).

The following table is the bisection procedure (line 2–13) in Algorithm 2 to refine the interval $(-4, 12)$, in which “ \exists ” (resp. “ $\neg\exists$ ”) means there exists (no) a real root in the observed interval.

	(-4,12)	(-4,4)	(-4,0)	(-2,0)	(-2,-1)
S_2	\exists	\exists	\exists	\exists	\exists
S_1	\exists	\exists	\exists	\exists	$\neg\exists$

Finally, a refined interval $(a, b) = (-2, -1)$ is obtained, which satisfies the condition of Theorem 7. Thus, $(-4, -2)$ and $(-1, 12)$ are two intervals that may contain at most one real root of $S_1(t) = 0$. In addition, as $S_1(-4)S_1(-2) > 0$ and $S_1(-1)S_1(12) < 0$, $(-1, 12)$ contains a real root of $S_1(t) = 0$, but $(-4, -2)$ does not by Theorem 7. Thus, we get a real root isolation for $S_1(t) = 0$ in $(-4, 12)$, i.e., $\mathcal{L}_{(-4,12)}(S_1) = \{(-1, 12)\}$.

In order to compute $\mathcal{L}_{(-4,12)}(S_0)$, we repeat the above procedure, and obtain $\mathcal{L}_{(-4,12)}(\hat{f}) = \{(-4, -0.59375), (-0.390625, 12)\}$.

Up to now, we have already explained the main idea of our approach how to isolate real roots of a PEF by the running example. This procedure is implemented in Algorithm 1, whose main steps can be understood as follows:

- Step 1: In line 1, compute upper and lower bounds of the real roots of $f(t)$.
- Step 2: In line 1, construct a sequence $S_0(t) = f(t), S_1(t), S_2(t), \dots, S_r(t)$, where S_i is a PEF which has the same real roots as the derivative of S_{i-1} , $i = 1, 2, \dots, r$, $r \in \mathbb{N}$, and $S_r(t)$ is a polynomial in t .
- Step 3: Isolate all real roots of $S_r(t)$ by calling `UPIsolating`($S_r(t)$) in line 1. Note that the problem of isolating real roots of a univariate polynomial is well studied (e.g., in [12]).
- Step 4: In line 1, for $i = r - 1$ down to 0, construct a real root isolation of S_i from that of S_{i+1} using Theorem 7 by calling `PEFI`. Note that during this procedure, we use \mathcal{S}_1 to record all subintervals in which $f(t)$ has no real roots, while \mathcal{S}_2 to record all subintervals in which $f'(t)$ has no real roots. So, we only need to construct a real root isolation of S_i from that of S_{i+1} on the remainder part of the considered interval by excluding all subintervals in \mathcal{S}_1 and \mathcal{S}_2 , and accordingly update \mathcal{S}_1 and \mathcal{S}_2 in each iteration, see the detail in Algorithm 2.

Theorem 8 (Correctness of PEFI): Algorithm PEFI always terminates correctly.

Proof: The termination of PEFI is obvious because $f_1(t) = 0$ and $f_2(t) = 0$ have no common real roots. Then, we prove its correctness.

\mathcal{S}_1' and \mathcal{S}_2' are updated in line 5 and line 7, respectively. Obviously, after every update, the properties of \mathcal{S}_1' and \mathcal{S}_2' still hold, i.e., $f_1(t)$ has no real roots in $\cup \mathcal{S}_1'$, $f_2(t)$ has no real roots in $\cup \mathcal{S}_2'$, and $\cup \mathcal{S}_1' \cap \cup \mathcal{S}_2' = \emptyset$. It is also easy to see that, after the *for loop* at lines 15–18, \mathcal{L}' is a real root isolation of $g_1(t)$ on $(a, b) \setminus \cup(\mathcal{S}_1' \cup \mathcal{S}_2')$. ■

Theorem 9 (Correctness of PEFIsolation): Algorithm PEFIsolation always terminates and returns a real root isolation for a given PEF f , if f does not have multiple real roots.

Proof: Termination is immediately obtained from Theorem 8. Then, we prove its correctness. After the *for*

Algorithm 1: PEFIsolation.

Input: $f(t)$, a PEF of the form (16) with the assumption (17), which has no multiple real roots

Output: \mathcal{L} , a real root isolation of $f(t)$

- 1 Calculate a lower bound a and an upper bound b on real roots of $f(t) = 0$;
- 2 set $\mathcal{S}_1 \leftarrow \emptyset, \mathcal{S}_2 \leftarrow \emptyset$;
/* \mathcal{S}_1 records all closed subintervals of $[a, b]$ in which $f(t)$ has no real roots, while \mathcal{S}_2 records all closed subintervals of $[a, b]$ in which $f'(t)$ has no real roots. */
- 3 Construct a sequence, $S_0(t) = f(t), S_1(t), S_2(t), \dots, S_r(t)$, where S_i is a PEF, which shares the common real roots with the derivative of S_{i-1} , $i = 1, 2, \dots, r$, $r \in \mathbb{N}$, and $S_r(t)$ is a polynomial;
- 4 $\mathcal{L}_{(a,b)}(S_r) := \text{UPIsolving}(S_r(t))$, a real root isolation of $S_r(t)$;
- 5 **for** $i = r - 1; i \geq 0; i --$ **do**
- 6 $\lfloor [\mathcal{S}_1, \mathcal{S}_2, \mathcal{L}] \leftarrow \text{PEFI}(S_0, S_1, S_i, S_{i+1}, (a, b), \mathcal{S}_1, \mathcal{S}_2, \mathcal{L})$;
- 7 **for** $[c, d] \in \mathcal{S}_2$ **do**
- 8 **if** $S_0(c)S_0(d) < 0$ **then**
- 9 $\lfloor \mathcal{L} \leftarrow \mathcal{L} \cup \{(c, d)\}$;
- 10 **return** \mathcal{L} ;

loop in line 2, \mathcal{L} is a real root isolation of $S_0(t) = 0$ (i.e., $f(t) = 0$) on $(a, b) \setminus \cup(\mathcal{S}_1 \cup \mathcal{S}_2)$. Because $f'(t)$ has a constant nonzero sign in each interval of \mathcal{S}_2 , $f(t)$ has at most one real root in each interval of \mathcal{S}_2 and this can be decided by checking the signs of $f(t)$ at two endpoints of the interval. Moreover, since there is no real root of $f(t) = 0$ in $\cup \mathcal{S}_1$, so \mathcal{L}_2 is a real root isolation of $S_0(t)$ in (a, b) . ■

3) Multiple Real Roots of PEFs: Termination of the algorithm PEFIsolation with an input PEF f rely on that f does not have multiple real roots, which is however not obvious to check. In this section, we deal with multiple real roots of PEF based on Schanuel's conjecture.

Definition 6 (Algebraic independence): A set of complex numbers $S = \{a_1, \dots, a_n\}$ is algebraically independent over \mathbb{Q} if the elements of S do not satisfy any nontrivial polynomial equation with coefficients in \mathbb{Q} .

Definition 7 (Transcendence degree): Let L be a field extension of \mathbb{Q} , the transcendence degree of L over \mathbb{Q} is defined as the largest cardinality of an algebraically independent subset of L over \mathbb{Q} .

Conjecture 1 (Schanuel's conjecture): Given any complex numbers z_1, \dots, z_n that are linearly independent over \mathbb{Q} , the extension field $\mathbb{Q}(z_1, \dots, z_n, e^{z_1}, \dots, e^{z_n})$ has transcendence degree of at least n over \mathbb{Q} .

In what follows, we handle the multiple real roots of PEF. Let

$$f(t) = f_0(t) + f_1(t)e^{\lambda_1 t} + \dots + f_r(t)e^{\lambda_r t}$$

where $f_0, \dots, f_r \in \mathbb{Q}[t]$, and $\lambda_1, \dots, \lambda_r$ are different algebraic numbers. Let a_1, \dots, a_n be an integer-basis of $\lambda_1, \dots, \lambda_r$. Then a_1, \dots, a_n are linearly independent over \mathbb{Q} , and $f(t)$ is a polynomial w.r.t. $t, e^{a_1 t}, \dots, e^{a_n t}$, denoted by $f(t, e^{a_1 t}, \dots, e^{a_n t})$.

Since $f(t, y_1, \dots, y_n)$ is a polynomial, by factorization we have

$$f(t, y_1, \dots, y_n) = f_1^{m_1}(t, y_1, \dots, y_n) \cdots f_s^{m_s}(t, y_1, \dots, y_n)$$

Algorithm 2: PEFI.

Input: (1) PEFs $f_1(t), f_2(t), g_1(t), g_2(t)$ s.t. $f_2(t)$ and $f_1'(t)$ share same real zeros, $g_2(t)$ and $g_1'(t)$ share same real zeros, and $f_1(t)$ and $f_2(t)$ have no common real zeros;

(2) an open interval (a, b) ;

(3) $\mathcal{S}_1, \mathcal{S}_2$, two sets of closed intervals contained in (a, b) , s.t. $f_1(t)$ has no real zeros in $\cup \mathcal{S}_1$, $f_2(t)$ has no real zeros in $\cup \mathcal{S}_2$, $\cup \mathcal{S}_1 \cap \cup \mathcal{S}_2 = \emptyset$;

(4) \mathcal{L} , a real root isolation of $g_2(t)$ on $(a, b) \setminus \cup(\mathcal{S}_1 \cup \mathcal{S}_2)$.

Output: (1) \mathcal{S}'_1 and \mathcal{S}'_2 with the same properties as \mathcal{S}_1 and \mathcal{S}_2 , respectively;

(2) \mathcal{L}_2 , a real root isolation of $g_1(t)$ on $(a, b) \setminus \cup(\mathcal{S}'_1 \cup \mathcal{S}'_2)$.

- 1 $\mathcal{S}'_1 \leftarrow \mathcal{S}_1, \mathcal{S}'_2 \leftarrow \mathcal{S}_2$;
- 2 **for** (l, u) in \mathcal{L} **do**
- 3 **while** $0 \in g_1([l, u])$ **do**
- 4 **if** $0 \notin f_1([l, u])$ **then**
- 5 $\lfloor \mathcal{S}'_1 \leftarrow \mathcal{S}'_1 \cup \{(l, u)\}$; **break**;
- 6 **if** $0 \notin f_2([l, u])$ and $f_1(l)f_1(u) \neq 0$ **then**
- 7 $\lfloor \mathcal{S}'_2 \leftarrow \mathcal{S}'_2 \cup \{(l, u)\}$; **break**;
- 8 **if** $g_2(l)g_2(\frac{l+u}{2}) < 0$ **then**
- 9 $\lfloor u \leftarrow \frac{l+u}{2}$;
- 10 **else if** $g_2(\frac{l+u}{2}) = 0$ **then**
- 11 $\lfloor l \leftarrow \frac{3l+u}{4}; u \leftarrow \frac{l+3u}{4}$;
- 12 **else**
- 13 $\lfloor l \leftarrow \frac{l+u}{2}$;
- 14 $\mathcal{L}_1 \leftarrow \mathcal{L}; \mathcal{L}_2 \leftarrow \emptyset; \mathcal{L}_3 \leftarrow \{(a_1, b_1), \dots, (a_m, b_m)\}$;
/* where $a_1, b_1, \dots, a_m, b_m$ are the endpoints of the intervals in \mathcal{S}_1 and \mathcal{S}_2 s.t. $a \leq a_1 < b_1 < \dots < a_m < b_m \leq b$, $(a_i, b_i) \subseteq (a, b) \setminus \cup(\mathcal{S}_1 \cup \mathcal{S}_2)$ for $i = 1, \dots, m$, and $\cup_{i=1}^m (a_i, b_i) = (a, b) \setminus \cup(\mathcal{S}_1 \cup \mathcal{S}_2)$. */
- 15 **for** (c, d) in \mathcal{L}_3 **do**
- 16 $\mathcal{L}_1(c, d) \leftarrow \{I \mid I \in \mathcal{L}_1 \text{ and } I \subset (c, d)\}$;
- 17 Obtain a real root isolation $\mathcal{L}_{(c,d)}$ for $g_1(t)$ on (c, d) from $\mathcal{L}_1(c, d)$ by Theorem 7;
- 18 $\mathcal{L}_2 \leftarrow \mathcal{L}_2 \cup \mathcal{L}_{(c,d)}$;
- 19 **return** $\mathcal{S}'_1, \mathcal{S}'_2, \mathcal{L}_2$;

whose square free part is denoted by

$$\hat{f}(t, y_1, \dots, y_n) = f_1(t, y_1, \dots, y_n) \cdots f_s(t, y_1, \dots, y_n).$$

This yields a PEF $\hat{f}(t, e^{a_1 t}, \dots, e^{a_n t})$, denoted as the square free part of $f(t, e^{a_1 t}, \dots, e^{a_n t})$.

The following corollaries can be derived based on Schanuel's conjecture.

Corollary 3: Let a_1, \dots, a_n be algebraic numbers that are linearly independent over \mathbb{Q} . The transcendence degree of the field extension $\mathbb{Q}(t, e^{a_1 t}, \dots, e^{a_n t})$ is at least n , if $t \neq 0$.

Proof: Since a_1, \dots, a_n are linearly independent over \mathbb{Q} and $t \neq 0$, $a_1 t, \dots, a_n t$ are linearly independent over \mathbb{Q} . By Schanuel's conjecture, the transcendence degree of the field extension

$$\mathbb{Q}(a_1 t, \dots, a_n t, e^{a_1 t}, \dots, e^{a_n t})$$

is at least n . Besides, a_1, \dots, a_n are algebraic numbers, thus $\mathbb{Q}(t) = \mathbb{Q}(a_1 t, \dots, a_n t)$, i.e., $\mathbb{Q}(a_1 t, \dots, a_n t, e^{a_1 t}, \dots, e^{a_n t}) = \mathbb{Q}(t, e^{a_1 t}, \dots, e^{a_n t})$. Therefore, the transcendence degree of the field extension $\mathbb{Q}(t, e^{a_1 t}, \dots, e^{a_n t})$ is at least n . ■

Corollary 4: Let $f(t, e^{a_1 t}, \dots, e^{a_n t})$ be a PEF w.r.t. t , and thus a polynomial w.r.t. $t, e^{a_1 t}, \dots, e^{a_n t}$, where a_1, \dots, a_n are linearly independent. Suppose $f(t, y_1, \dots, y_n)$ is square free, then $f(t, e^{a_1 t}, \dots, e^{a_n t})$ has no multiple real root except 0.

Proof: Since $f(t, y_1, \dots, y_n)$ is square free, we may write

$$f(t, y_1, \dots, y_n) = f_1(t, y_1, \dots, y_n) \cdots f_m(t, y_1, \dots, y_n)$$

where for any $1 \leq i, j \leq m$, $i \neq j$, $f_i(t, y_1, \dots, y_n)$ is irreducible and $f_i(t, y_1, \dots, y_n)$ and $f_j(t, y_1, \dots, y_n)$ are coprime.

We first prove, by contradiction, that $f_i(t, e^{a_1 t}, \dots, e^{a_n t})$ and $f_j(t, e^{a_1 t}, \dots, e^{a_n t})$ have no nonzero common real root. Suppose $t_0 \neq 0$ is a common real root of $f_i(t, e^{a_1 t}, \dots, e^{a_n t})$ and $f_j(t, e^{a_1 t}, \dots, e^{a_n t})$. By Corollary 3, we have that the transcendence degree of $\mathbb{Q}(t_0, e^{a_1 t_0}, \dots, e^{a_n t_0})$ is at least n . Then, there must exist n elements in $\{t_0, e^{a_1 t_0}, \dots, e^{a_n t_0}\}$ that are algebraically independent. Without loss of generality, let $\{t_0, e^{a_1 t_0}, \dots, e^{a_{n-1} t_0}\}$ be the n elements that are algebraically independent. Besides, let $g(t, y_1, \dots, y_{n-1})$ be the resultant of $f_i(t, y_1, \dots, y_n)$ and $f_j(t, y_1, \dots, y_n)$ w.r.t. y_n , then $(t_0, e^{a_1 t_0}, \dots, e^{a_{n-1} t_0})$ is a real root of $g(t, y_1, \dots, y_{n-1})$. Further since $f_i(t, y_1, \dots, y_n)$ and $f_j(t, y_1, \dots, y_n)$ are coprime, $g(t, y_1, \dots, y_{n-1})$ is nontrivial polynomial, indicating that $(t_0, e^{a_1 t_0}, \dots, e^{a_{n-1} t_0})$ is a real root of some nontrivial polynomial. This contradicts that $\{t_0, e^{a_1 t_0}, \dots, e^{a_{n-1} t_0}\}$ are algebraically independent. Consequently, $f_i(t, e^{a_1 t}, \dots, e^{a_n t})$ and $f_j(t, e^{a_1 t}, \dots, e^{a_n t})$ have no nonzero common real root.

Next, we prove that $f_i(t, e^{a_1 t}, \dots, e^{a_n t})$ has no multiple real root. Suppose

$$f_i(t, e^{a_1 t}, \dots, e^{a_n t}) = h_0(t) + \sum_{j=1}^s h_j(t)(e^{a_1 t})^{b_{j1}} \cdots (e^{a_n t})^{b_{jn}}$$

where $h_0(t), \dots, h_n(t)$ are nontrivial polynomials, $b_{jk} \in \mathbb{N}$, $1 \leq j \leq s$, and $1 \leq k \leq n$. Then, we have

$$f'_i(t, e^{a_1 t}, \dots, e^{a_n t}) = h'_0(t) + \sum_{j=1}^s (h'_j(t) + (a_1 b_{j1} + \cdots + a_n b_{jn}) h_j(t)) (e^{a_1 t})^{b_{j1}} \cdots (e^{a_n t})^{b_{jn}}.$$

Moreover

$$f_i(t, y_1, \dots, y_n) = h_0(t) + \sum_{j=1}^s h_j(t) y_1^{b_{j1}} \cdots y_n^{b_{jn}}$$

$$f'_i(t, e^{a_1 t}, \dots, e^{a_n t}) = h'_0(t) + \sum_{j=1}^s (h'_j(t) + (a_1 b_{j1} + \cdots + a_n b_{jn}) h_j(t)) y_1^{b_{j1}} \cdots y_n^{b_{jn}}.$$

Consider the degree and $h_0(t)$ to be nontrivial, it is evident to see that $f_i(t, y_1, \dots, y_n) \nmid f'_i(t, y_1, \dots, y_n)$. Then, $f_i(t, y_1, \dots, y_n)$ and $f'_i(t, y_1, \dots, y_n)$ are coprime, since $f_i(t, y_1, \dots, y_n)$ is irreducible. For the same reason as above, $f_i(t, e^{a_1 t}, \dots, e^{a_n t})$ and $f'_i(t, e^{a_1 t}, \dots, e^{a_n t})$ have no common real root. Therefore, $f_i(t, e^{a_1 t}, \dots, e^{a_n t})$ has no multiple real root. ■

4) Complexity analysis of PEFIsolation: Here, we give a rough complexity analysis of PEFIsolation. Suppose $f(t) = f_0(t) + f_1(t)e^{\nu_1 t} + \cdots + f_s(t)e^{\nu_s t}$, $L(f)$ and $U(f)$ are, respectively, a lower bound and an upper bound on real roots of $f(t)$, $\deg(f) = (d_0, d_1, \dots, d_s)$. PEFIsolation computes all real roots for a PEF chain $f(t) = 0$, $f'(t) = 0$, $f''(t) = 0, \dots$, totally, $d_0 + \cdots + d_{s-1} + s + 1$ such

PEFs at most, with the corresponding degree. The last element in the chain is a polynomial with degree d_s , so it has at most d_s real roots. Clearly, for each function in the chain, the number of intervals in its real root isolation is at most $d_0 + d_1 + \cdots + d_s + s + 1$. In addition, suppose the lower bound on the distances between real roots of S_i and those of S_{i+1} is δ , then the while loop (line 3–13) in Algorithm IV-D2 always terminates after the length of an interval is less than δ . Since the length of every interval is less than or equal to $U(f) - L(f)$, the while loop must terminate in $\log_2 \frac{U(f) - L(f)}{\delta}$ steps. In a summary, the complexity of PEFIsolation is about $\mathcal{O}((\sum_{i=0}^s d_i + s + 1)^2 \log_2 \frac{U(f) - L(f)}{\delta})$.

V. PURELY IMAGINARY EIGENVALUES

In this section, we give a decision procedure for the purely imaginary case described in Section II-C.

A. Solution Form

Theorem 10: Given an SS as (4) as described above, for any initial point $\mathbf{x} \in \mathbb{R}^n$, the solution $\Phi(\mathbf{x}, t)$ is of the following form

$$(\Phi(\mathbf{x}, t))_i = \sum_{k=1}^{K_i} z_{ik}^c(\mathbf{x}) \cos(\gamma_{ik} t) + z_{ik}^s(\mathbf{x}) \sin(\gamma_{ik} t) \quad (20)$$

for $i = 1, \dots, n$, where $z_{ik}^c(\mathbf{x}), z_{ik}^s(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$ and $\gamma_{ik} \in \mathbb{R}$.

Proof: Similar to Theorem 5.

Example 3: Let

$$\begin{bmatrix} \dot{\xi}_1 \\ \dot{\xi}_2 \\ \dot{\xi}_3 \\ \dot{\xi}_4 \end{bmatrix} = \begin{bmatrix} -\xi_2 \\ \xi_1 \\ 2\xi_3 + 2\xi_4 - \xi_1^2 \\ -3\xi_3 - 2\xi_4 + \xi_1 \xi_2 \end{bmatrix} \quad (21)$$

an initial state $\mathbf{x} = (x_1, x_2, x_3, x_4) \in \mathbb{R}^4$, then, the solution is

$$\xi_1(t, \mathbf{x}) = x_1 \cos(t) - x_2 \sin(t)$$

$$\xi_2(t, \mathbf{x}) = x_1 \sin(t) + x_2 \cos(t)$$

$$\xi_3(t, \mathbf{x}) = \frac{\sqrt{2}}{2}(x_1^2 + 2x_1x_2 - 2x_2^2 + 2c + 2d) \sin(\sqrt{2}t)$$

$$+ (2x_1x_2 + x_2^2 + c) \cos(\sqrt{2}t)$$

$$+ \frac{1}{2}(x_1^2 - 4x_1x_2 - x_2^2) \cos(2t)$$

$$- (x_1^2 + x_1x_2 - x_2^2) \sin(2t) - \frac{x_1^2 + x_2^2}{2}$$

$$\xi_4(t, \mathbf{x}) = \frac{1}{2}(x_1^2 - 2x_1x_2 - 4x_2^2 + 2x_4) \cos(\sqrt{2}t)$$

$$- \frac{\sqrt{2}}{2}(x_1^2 + 4x_1x_2 - x_2^2 + 3x_3 + 2x_4) \sin(\sqrt{2}t)$$

$$+ \frac{1}{4}(-5x_1^2 + 5x_2^2 + 4x_1x_2) \cos(2t)$$

$$- \frac{1}{2}(x_1^2 - x_2^2 + 5x_1x_2) \sin(2t) + \frac{3}{4}(x_1^2 + x_2^2)$$

which is a TMF vector.

As X and Y are two open semialgebraic sets, there exist some polynomial $p_1(\mathbf{x}), \dots, p_J(\mathbf{x})$ such that

$$\begin{aligned} X &= \{\mathbf{x} \in \mathbb{R}^n \mid p_1(\mathbf{x}) > 0, \dots, p_{J_1}(\mathbf{x}) > 0\} \\ Y &= \{\mathbf{x} \in \mathbb{R}^n \mid p_{J_1+1}(\mathbf{x}) > 0, \dots, p_J(\mathbf{x}) > 0\}. \end{aligned}$$

Thus, the problem (13) can be further reduced to

$$\mathcal{F}(X, Y) = \exists \mathbf{x} \exists \mathbf{y} \exists t : \Omega \quad (22)$$

where

$$\Omega = p_1(\mathbf{x}) > 0, \dots, p_{J_1}(\mathbf{x}) \wedge p_{J_1+1}(\mathbf{y}) > 0, \dots, p_J(\mathbf{y}) > 0$$

$$\wedge t \geq 0 \wedge \bigwedge_{i=1}^n y_i = \sum_{k=1}^{K_i} z_{ik}^c(\mathbf{x}) \cos(\gamma_{ik}t) + z_{ik}^s(\mathbf{x}) \sin(\gamma_{ik}t). \quad (23)$$

B. Reduction to Decision Problem of Tarski's Algebra

In this part, we show the problem (22) can be reduced to the decision problem of Tarski's algebra [39]. There have been many tools available for the decision procedure, e.g., [6], [11], [13], [19], [22], [29], [36], all of which are based on CAD [10].

From now on, we will focus on how to reduce (23) to Tarski's algebra equivalently.

For (23), let $\Gamma = \{\gamma_{ik} \mid 1 \leq k \leq K_i, 1 \leq i \leq n\}$, i.e., the set of all reals appearing in some trigonometric expression in (23), 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.

In addition, 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 $1 \leq k \leq K_i, 1 \leq i \leq n$, that is

$$\cos(\gamma_{ik}t) = f_{ik}^c(\sin(\delta_1 t), \cos(\delta_1 t), \dots, \sin(\delta_N t), \cos(\delta_N t)) \quad (24)$$

$$\sin(\gamma_{ik}t) = f_{ik}^s(\sin(\delta_1 t), \cos(\delta_1 t), \dots, \sin(\delta_N t), \cos(\delta_N t)) \quad (25)$$

where f_{ik}^c, f_{ik}^s are polynomials in their arguments. Denote the following formula by Ξ , i.e.

$$\begin{aligned} \Xi &\triangleq \mathbf{x} \in X \wedge \mathbf{y} \in Y \wedge \bigwedge_{j=1}^N u_j^2 + v_j^2 = 1 \wedge \\ &\bigwedge_{i=1}^n y_i = \sum_{k=1}^{K_i} \left(z_{ik}^c(\mathbf{x}) f_{ik}^c(u_1, v_1, \dots, u_N, v_N) \right. \\ &\quad \left. + z_{ik}^s(\mathbf{x}) f_{ik}^s(u_1, v_1, \dots, u_N, v_N) \right). \end{aligned}$$

Theorem 11: Suppose X, Y both are open semialgebraic sets, Γ is defined as above, which is a set of real numbers, Δ is an integer-basis of Γ , f_{ik}^c and f_{ik}^s are defined as (24), (25), and Ω and Ξ are two formulas defined as above, then

$$\exists \mathbf{x} \exists \mathbf{y} \exists t : \Omega \Leftrightarrow \exists \mathbf{x} \exists \mathbf{y} \exists_{j=1}^N u_j \exists_{j=1}^N v_j : \Xi. \quad (26)$$

Proof: It is obviously that

$$\exists \mathbf{x} \exists \mathbf{y} \exists t : \Omega \Rightarrow \exists \mathbf{x} \exists \mathbf{y} \exists_{j=1}^N u_j \exists_{j=1}^N v_j : \Xi \quad (27)$$

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

$$\exists \mathbf{x} \exists \mathbf{y} \exists_{j=1}^N u_j \exists_{j=1}^N v_j : \Xi \Rightarrow \exists \mathbf{x} \exists \mathbf{y} \exists t : \Omega. \quad (28)$$

Let

$$\begin{aligned} S &= \{(\sin(\delta_1 t), \cos(\delta_1 t), \dots, \sin(\delta_N t), \cos(\delta_N t)) \mid t \geq 0\} \\ \bar{S} &= \left\{ (u_1, v_1, \dots, u_N, v_N) \in \mathbb{R}^{2N} \mid \bigwedge_{i=1}^N u_i^2 + v_i^2 = 1 \right\}. \end{aligned}$$

From Theorem 2, it follows that S is dense in \bar{S} . Denote $\mathbf{w} = (u_1, v_1, \dots, u_N, v_N)$. Let $\mathbf{x}', \mathbf{y}', u'_1, \dots, u'_N, v'_1, \dots, v'_N$ satisfy Ξ , i.e.

$$\mathbf{x}' \in X \wedge \mathbf{y}' \in Y \wedge \mathbf{w}' \in \bar{S} \wedge$$

$$\bigwedge_{i=1}^n y'_i = \sum_{k=1}^{K_i} z_{ik}^c(\mathbf{x}') f_{ik}^c(\mathbf{w}') + z_{ik}^s(\mathbf{x}') f_{ik}^s(\mathbf{w}')$$

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

$$y_i = \sum_{k=1}^{K_i} z_{ik}^c(\mathbf{x}') f_{ik}^c(\mathbf{w}') + z_{ik}^s(\mathbf{x}') f_{ik}^s(\mathbf{w}')$$

is a continuous function on \mathbf{w} (denote by $\mathbf{y} = \mathbf{y}(\mathbf{w})$). Thus, there must exist an open ball $B_\sigma(\mathbf{w}')$ such that $\mathbf{y}(B_\sigma(\mathbf{w}')) \subset B_\varepsilon(\mathbf{y}') \subset Y$, where $\sigma > 0$. Besides, as $\mathbf{w}' \in \bar{S}$ and S is dense in \bar{S} , there must exist $\mathbf{w}_0 \in B_\sigma(\mathbf{w}')$, i.e., there exists $t_0 > 0$ with $(a_1 t_0, \dots, a_N t_0) \in B_\sigma(\mathbf{w}')$ and $\mathbf{y}_0 = \mathbf{y}(\mathbf{w}_0) \in B_\varepsilon(\mathbf{y}') \subset Y$. Hence, $\mathbf{x}', \mathbf{y}_0, t_0$ satisfy Ω . ■

From the decidability of Tarski's algebra [39], an immediate result of Theorem 11 is

Theorem 12: The problem described in (22) is decidable.

Example 4: Continue to consider Example 3. Let the initial set X and unsafe set Y defined as following:

$$\begin{aligned} X &= \{(x_1, x_2, x_3, x_4) \mid -1 < x_1 < 1 \wedge x_2 = 0 \wedge x_3^2 + x_4^2 < 1\} \\ Y &= \{(y_1, y_2, y_3, y_4) \mid y_3 + y_4 > 4\} \end{aligned}$$

we want to check whether this system is safe or not. In order to use Theorem 11, we first introduce some new variables as

$$\alpha_1 = \sin(t), \beta_1 = \cos(t), \alpha_2 = \sin(\sqrt{2}t), q = \cos(\sqrt{2}t).$$

Then, the solution of (21) is

$$\xi_1(t, \mathbf{x}) = x_1 \beta_1 - x_2 \alpha_1$$

$$\xi_2(t, \mathbf{x}) = x_1 \alpha_1 + x_2 \beta_1$$

$$\begin{aligned} \xi_3(t, \mathbf{x}) &= \frac{\sqrt{2}}{2} (x_1^2 + 2x_1 x_2 - 2x_2^2 + 2c + 2d) \alpha_2 \\ &\quad + (2x_1 x_2 + x_2^2 + c) \beta_2 \end{aligned}$$

$$\begin{aligned}
& + \frac{1}{2}(x_1^2 - 4x_1x_2 - x_2^2)(\beta_1^2 - \alpha_1^2) \\
& - 2(x_1^2 + x_1x_2 - x_2^2)\alpha_1\beta_1 - \frac{x_1^2 + x_2^2}{2} \\
\xi_4(t, \mathbf{x}) = & \frac{1}{2}(x_1^2 - 2x_1x_2 - 4x_2^2 + 2x_4)\beta_2 \\
& - \frac{\sqrt{2}}{2}(x_1^2 + 4x_1x_2 - x_2^2 + 3x_3 + 2x_4)\alpha_2 \\
& + \frac{1}{4}(-5x_1^2 + 5x_2^2 + 4x_1x_2)(\beta_1^2 - \alpha_1^2) \\
& - (x_1^2 - x_2^2 + 5x_1x_2)\alpha_1\beta_1 + \frac{3}{4}(x_1^2 + x_2^2).
\end{aligned}$$

By Theorem 11, we just need to check whether

$$\begin{aligned}
\mathcal{F} := & -1 < x_1 < 1 \wedge x_3^2 + x_4^2 < 1 \wedge \alpha_1^2 + \beta_1^2 = 1 \wedge \\
& \alpha_2^2 + \beta_2^2 = 1 \wedge \left(\frac{1}{4}(3\alpha_1^2 - 3\beta_1^2 - 4\alpha_1\beta_1 + 1)x_1^2 \right. \\
& \left. + \frac{1}{2}(x_1^2 + 2x_3 + 2x_4)\beta_2 - \frac{\sqrt{2}}{2}x_3\alpha_2 \right) > 4
\end{aligned}$$

is satisfiable or not. It is easy to prove that there does not exist any $x_1, x_2, x_3, x_4, \alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{R}$ such that the above formula holds. Thus, the system is safe.

Remark 2: Note that the openness of the initial set X and the unsafe set Y plays a very important role in our approach. Otherwise, there may be some point on the boundary of X or Y , which cannot be contained by any ball contained correspondingly in X or Y . But in case either of them is not open, we can resort to the below approach to approximate the reachable set.

VI. ABSTRACTION OF SOLVABLE DYNAMICAL SYSTEMS

In this section, we present an approach to approximate the reachable sets of the general solvable dynamical systems SS (4) by abstracting to the case only with real eigenvalues as discussed in Section IV.

A. Solution Form of the General Case

Given an SS of (4), we will show that its solution is a PETF vector. Namely,

Theorem 13: Given an SS as (4) and an initial point $\mathbf{x} \in \mathbb{R}^n$, then its solution $\Phi(\mathbf{x}, t)$ can be represented by the following form

$$(\Phi(\mathbf{x}, t))_i = \sum_{k=1}^{K_i} e^{\alpha_{ik}t} (z_{ik}^c(\mathbf{x}) \cos(\gamma_{ik}t) + z_{ik}^s(\mathbf{x}) \sin(\gamma_{ik}t)) \quad (29)$$

for $i = 1, \dots, n$, where $z_{ik}^c(\mathbf{x}), z_{ik}^s(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$ and $\alpha_{ik}, \gamma_{ik} \in \mathbb{R}$.

Proof: Similar to Theorem 5. \blacksquare

B. Approximation of Reachable Sets by Abstraction

Using the solution form above, the reachability of Y from X , i.e., the safety problem, can be formally described as

$\exists \mathbf{x} \exists \mathbf{y} \exists t : \Omega$, where the quantifier free part Ω is defined by

$$\Omega \doteq \mathbf{x} \in X \wedge \mathbf{y} \in Y \wedge t \geq 0 \wedge$$

$$\bigwedge_{i=1}^n y_i = \sum_{k=1}^{K_i} e^{\alpha_{ik}t} (z_{ik}^c(\mathbf{x}) \cos(\gamma_{ik}t) + z_{ik}^s(\mathbf{x}) \sin(\gamma_{ik}t)).$$

The reachability problem of this form is generally undecidable due to the TMFs in the formula. However, if there are no such functions it becomes decidable, and a decision procedure has been proposed in [16]. This fact hints us to eliminate the TMFs by overapproximation of the reachable set, which is analogous to the technique used in Section V. Let

$$\Xi \doteq \mathbf{x} \in X \wedge \mathbf{y} \in Y \wedge t \geq 0 \wedge \bigwedge_{j=1}^N u_j^2 + v_j^2 = 1 \wedge$$

$$\bigwedge_{i=1}^n y_i = \sum_{k=1}^{K_i} e^{\alpha_{ik}t} \left(z_{ik}^c(\mathbf{x}) f_{ik}^c(u_1, v_1, \dots, u_N, v_N) + z_{ik}^s(\mathbf{x}) f_{ik}^s(u_1, v_1, \dots, u_N, v_N) \right).$$

Then, it follows immediately that

$$\text{Theorem 14: } \exists \mathbf{x} \exists \mathbf{y} \exists t : \Omega \Rightarrow \exists \mathbf{x} \exists \mathbf{y} \exists t \exists_{j=1}^N u_j \exists_{j=1}^N v_j : \Xi.$$

Hence, we can conclude, by Theorem 14, the system to be verified is safe, i.e., Y is not reachable from X , as long as we can prove $\exists \mathbf{x} \exists \mathbf{y} \exists t \exists_{j=1}^N u_j \exists_{j=1}^N v_j : \Xi$ does not hold.

VII. IMPLEMENTATION AND EXPERIMENTAL RESULTS

We have discussed the reachability problem for four cases: nilpotent, real, purely imaginary, and general case. For the nilpotent and purely imaginary case, the reachability problem can be reduced to a quantifier elimination problem in Tarski's algebra by introducing some new variables. Therefore, it is easy to obtain the decidability since the quantifier elimination of Tarski's algebra is decidable. We implement a tool to decide the reachability problem for the real case. And then using such tool to obtain an incomplete method for the general case.

A. Part 1: Only With Real Eigenvalues

We have implemented the proposed approach for the case only with real eigenvalues described in Section IV in *Mathematica* as a prototype, called *LinR*,² which takes an SS reachability problem as input, and gives either *False* if the problem is not satisfiable, or *True* otherwise associated with some valid sample points. In the following, we report some experimental results with *LinR*.

Example 6: Adopted from Example 3 in [16].

Example 7 (Adapted from [1]): Consider a vessel of water containing a radioactive isotope, to be used as a tracer for the food chain, which consists of aquatic plankton varieties phytoplankton A and zooplankton B . Let $\xi_1(t)$ be the isotope concentration in the water, $\xi_2(t)$ the isotope concentration in A and $\xi_3(t)$ the isotope concentration in B . The dynamics of the vessel is modeled as $\dot{\xi} = A\xi$, where

$$A = \begin{bmatrix} -3 & 6 & 5 \\ 2 & -12 & 0 \\ 1 & 6 & -5 \end{bmatrix}.$$

²Both the tool and the case studies in this section can be found at <http://lcs.ios.ac.cn/~chenms/tools/LinR.tar.bz2>.

The initial radioactive isotope concentrations $\xi_1(0) = x_1 > 0$, $\xi_2(0) = 0$, $\xi_3(0) = 0$.

The safety property of our concern is whether $\forall t > 0 \xi_1(t) \geq \xi_2(t) + \xi_3(t)$. To this end, we consider a more general problem: For which $n_1, n_2 \in \mathbb{N}$ s.t. $\mathcal{F}(n_1, n_2) = \exists x_1 > 0 \exists t > 0 \xi_1(t) < n_1 \xi_2(t) + n_2 \xi_3(t)$ holds.

It is easy to see that the matrix A is diagonalizable with eigenvalues $0, -10 + \sqrt{6}, -10 - \sqrt{6}$. When $(n_1, n_2) = (1, 1)$, using the method in Section IV-C, we obtain two sample points for (x_1, t) , i.e., $(-0.1, 1), (0.1, 1)$. But none of them satisfies $\mathcal{F}(1, 1)$, which simply implies the safety property holds. When $(n_1, n_2) = (2, 2)$, similarly, we obtain four sample points for (x_1, t) , i.e., $(-0.1, 0), (0.1, 0), (-0.1, 1), (0.1, 1)$, in which $(0.1, 1)$ satisfies $\mathcal{F}(2, 2)$. It can be proved that $\xi_i(t) \geq 0$ for any $t > 0$ and $i = 1, 2, 3$. So, it is clear that, if $\mathcal{F}(n_1, n_2)$ holds, $\mathcal{F}(m_1, m_2)$ holds for $m_1 \geq n_1$ and $m_2 \geq n_2$. Then, by checking some pairs of $(n_1, n_2) \in \mathbb{N} \times \mathbb{N}$ in a similar way as above, we conclude that all pairs $(n_1, n_2) \in \mathbb{N} \times \mathbb{N}$ satisfy $\mathcal{F}(n_1, n_2)$, except for the pairs $\{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2), (2, 0), (2, 1), (3, 0), (3, 1), (4, 0), (5, 0)\}$.

Example 8 (Adapted from [1]): Consider a typical home with attic, basement, and insulated main floor. Let $x_3(t), x_2(t), x_1(t)$ be the temperature in the attic, main living area, and basement, respectively, and t is the time in hours. Assume it is winter time, the outside temperature is nearly $35^\circ F$, and the basement earth temperature is nearly $45^\circ F$. Suppose a small electric heater is turned on, and it provides $20^\circ F$ rise per hour. We want to verify that the temperature in main living area will never reach too high (maybe $70^\circ F$). Analyze the changing temperatures in the three levels using Newton's cooling law and given the value of the cooling constants, we obtain the model as follows:

$$\begin{aligned}\dot{x}_1 &= \frac{1}{2}(45 - x_1) + \frac{1}{2}(x_2 - x_1) \\ \dot{x}_2 &= \frac{1}{2}(x_1 - x_2) + \frac{1}{4}(35 - x_2) + \frac{1}{4}(x_3 - x_2) + 20 \\ \dot{x}_3 &= \frac{1}{4}(x_2 - x_3) + \frac{3}{4}(35 - x_3)\end{aligned}$$

with the initial set $X = \{(x_1, x_2, x_3)^T \mid 1 - (x_1 - 45)^2 - (x_2 - 35)^2 - (x_3 - 35)^2 > 0\}$ and the unsafe set $Y = \{(y_1, y_2, y_3)^T \mid y_2 - 70 > 0\}$. The safety property we are concerning is to check if some state in Y is reachable from X , which holds by using *LinR*.

Example 9: Consider a nonlinear SS as follows

$$\begin{aligned}\dot{\xi}_1 &= -\xi_1 + 2\xi_2 \\ \dot{\xi}_2 &= \xi_1 - \xi_2 \\ \dot{\xi}_3 &= -\xi_3 + \xi_1 \xi_2\end{aligned}$$

with the initial set $X = \{(x_1, x_2, x_3)^T \mid -x_1 + x_2 - x_3 + 2 < 0\}$ and the unsafe set $Y = \{(y_1, y_2, y_3)^T \mid -y_1 + y_2 - y_3 - 2 > 0\}$. For an initial point $x = (x_1, x_2, x_3)$, the solution is

$$\begin{aligned}\xi_1(t, x) &= \left(\frac{1}{2}a + \frac{\sqrt{2}}{2}b\right) e^{(\sqrt{2}-1)t} - \left(-\frac{1}{2}a + \frac{\sqrt{2}}{2}b\right) e^{-(\sqrt{2}+1)t} \\ \xi_2(t, x) &= \left(\frac{\sqrt{2}}{4}a + \frac{1}{2}b\right) e^{(\sqrt{2}-1)t} + \left(-\frac{\sqrt{2}}{4}a + \frac{1}{2}b\right) e^{-(\sqrt{2}+1)t}\end{aligned}$$

$$\begin{aligned}\xi_3(t, x) &= e^{-t} \left(\frac{e^{(2\sqrt{2}-1)t}}{2\sqrt{2}-1} \left(\frac{\sqrt{2}}{8}x_1^2 + \frac{\sqrt{2}}{4}x_2^2 + \frac{1}{2}x_1x_2 \right) \right. \\ &\quad \left. + \frac{e^{-(2\sqrt{2}+1)t}}{2\sqrt{2}+1} \left(\frac{\sqrt{2}}{8}x_1^2 + \frac{\sqrt{2}}{4}x_2^2 - \frac{1}{2}x_1x_2 \right) \right) \\ &\quad + c - \frac{1}{8} \frac{\sqrt{2}x_1^2}{2\sqrt{2}-1} - \frac{1}{4} \frac{\sqrt{2}x_2^2}{2\sqrt{2}-1} - \frac{1}{2} \frac{x_1x_2}{2\sqrt{2}-1} \\ &\quad \left. + \frac{1}{8} \frac{\sqrt{2}x_1^2}{-2\sqrt{2}-1} + \frac{1}{4} \frac{\sqrt{2}x_2^2}{-2\sqrt{2}-1} - \frac{1}{2} \frac{x_1x_2}{-2\sqrt{2}-1} \right).\end{aligned}$$

The safety property we are concerning is to check if some state in Y is reachable from X , i.e., check whether the following formula is true of not:

$$\begin{aligned}\exists x_1 \exists x_2 \exists x_3 \exists t : & -x_1 + x_2 - x_3 + 2 < 0 \wedge t \geq 0 \\ & \wedge -\xi_1 + \xi_2 - \xi_3 - 2 > 0.\end{aligned}$$

Using our tool, a point $(x_1, x_2, x_3, t) = (-36.1203, 20.7631, 59.1, 1)$ can be found that satisfy the above formula, which means that the system will reach Y from the initial point $(-36.1203, 20.7631, 59.1) \in X$ at time $t = 1$. Thus, it is unsafe.

The above four examples are verified by *LinR*. Both the time and memory costs on a 64-bit Linux computer with a 2.93GHz Intel Core-i7 processor and 4GB of RAM are shown in Table I. Besides, we have also compared on the same platform with the performance of Strzeboński's approach (i.e., CT1D) [38], as well as verification tools dReach [25], HSolver [33], and Flow* [7] on these examples. Note that both dReach and Flow* cannot handle unbounded model checking, and even for BMC, they are less efficient than our tool in many cases (see Examples 6, 7, and 9).³ In particular, Flow* accepts only rectangular initial set, i.e., each variable needs to be specified within a closed interval and polynomial constraints are not allowed, and thus we tried different cube to approximate the spherical initial set in Example 6, while none of them can derive a desired result (unsafe). As for HSolver, due to the rejection of "sqrt," we simplify the original model by replacing all the irrational numbers with their approximate decimals, however, 2 of the 3 examples still cannot be answered by HSolver in reasonable time and memory.

Remark 4: In the above examples, all constraints are open sets. Actually, more general initial and unsafe sets, i.e., when either $Pre(X)$ or $Post(X)$ is not *open semialgebraic*, can be coped with in our approach also, as we have implemented CAD in the algorithms. For the [27, Example 3.4], where A is diagonalizable with rational eigenvalues and $Pre(X)$ and $Post(X)$ are both closed sets, it takes 57 ms using Lafferriere *et al.*'s approach based on quantifier elimination by QEPCAD [11]. In contrast, *LinR* takes 39 ms, and CT1D takes 33 ms. In brief, our approach shares nearly same complexity as Strzeboński's in general case, but is still better than other approaches, see Table II (QEPCAD stands for Lafferriere *et al.*'s approach).

Remark 5: It is worth clarifying the aim of the comparison done in this section, though we recognize that the comparisons

³Here, we set the time bounds 2s, 2s, 5s, and 2s resp. for Examples 6, 7, 8, and 9 when using dReach and Flow*.

TABLE I
EVALUATION RESULTS OF DIFFERENT METHODS

LDS	Time (s)					Memory (kb)				
	LinR	CT1D	dReach	HSolver	Flow*	LinR	CT1D	dReach	HSolver	Flow*
Example 6	1.35	×	37.36	–	–	112	×	3812	–	–
Example 7	0.03	0.20	0.71	–	–	131	2018	3816	–	–
Example 8	1.68	×	0.05	0.72	16.50	166	×	3812	1 076 932	113 492
Example 9	17.56	×	22.48	–	–	580	×	3820	–	–

× : The verification fails by nontermination within reasonable amount of time (10 hours).
 – : The verification fails because of giving an answer as “safety unknown.”

TABLE II
TIME CONSUMPTION (IN MILLISECONDS) ON EXAMPLE 3.4 FROM [27]

LinR	CT1D	QEPCAD	dReach	HSolver	Flow*
39	33	57	110	–	–

with dReach, Flow*, and HSolver are not essentially fair in general, due to distinction of their scopes. A more reasonable way of doing the comparison might be with several state-of-the-art tools for quantifier elimination, e.g., REDLOG [14], QEPCAD, and SyNRAC [24]. However, these implementations are not capable of dealing with the examples listed in Table I, as we are considering more general classes of systems featuring decidability results. For instance, SyNRAC performs quantifier elimination only over polynomial formulas, yet not available for constraints involving transcendental functions. While, CT1D, a generalized CAD implementation of Mathematica’s Reduce command, is theoretically competent in solving those examples, and thus is listed as one of the candidates in Table I.

Aiming at an extensive evaluation of our algorithms, especially for the efficiency, we resort to the verification community by performing comparisons with tools therein for reachability computation. Whereas unfortunately, neither dReach, Flow*, HSolver, nor SpaceEx [15] is fully compatible with our examples, and therefore, some simplifications or approximations over the examples are conducted before triggering those tools. For instance, we feed dReach and Flow* with a time bound, respectively, for each example, as they cannot handle unbounded verification; we replace the unbounded initial set with a small compact one in Examples 7 and 9 when evaluating HSolver, dReach, and Flow*, due to their intractability of unbounded initial set; while a rectangular approximation of the initial set is always needed for Flow* if the variables are not originally specified within closed intervals.

Particularly, for systems considered in this paper, if no simplification or approximation techniques are involved, one could get an immediate overview of the advantages of our approach through Table III.

B. Part 2: Abstraction of Solvable Dynamical Systems

To demonstrate the effectiveness of our technique that uses abstraction for general solvable dynamical systems with complex eigenvalues, we have extended our tool called *LinR* [16] in Mathematica, which has been demonstrated more efficient

TABLE III
FEATURES SUPPORTED BY DIFFERENT TOOLS

Features	LinR	HSolver	dReach	Flow*	SpaceEx
Unbounded time verification	✓	✓	–	–	✓ [#]
Unbounded initial set	✓	–	–	–	–
Nonlinear semialgebraic initial set	✓	✓	✓	–	–
Nonlinear SSS	✓	✓	✓	✓	–

✓[#] : Based on existence of fixed-points of the reachable states.

than existing approaches based on approximation and numeric computation in general, e.g., HSolver, dReach, FLOW*, 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 a practical proportional-integral-derivative (PID) controller.

Consider a PID controller (taken from [31]), which is used to control a simple mass, spring, and damper problem. The modeling equation of the mass, spring, and damper system (plant) is

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

where $M = 1$ kg, $b = 10$ N·s/m, $k = 20$ N/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

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

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:

$$\mathbf{G}(t > 0.5 \Rightarrow x \geq 0.9 \wedge x \leq 1.1). \quad (30)$$

Note that this case has been studied in [31] but unfortunately it cannot be proved by the method proposed there.

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

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

and $\mathbf{u} = [0, 0, 350, 1]^T$. 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 \mathbf{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

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

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 $\lambda_{1,2} = \alpha \pm \beta i$, then the solution can be rewritten as

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

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

$$\begin{aligned} \exists u \exists v \exists t : u^2 + v^2 = 1 \wedge t > 0.5 \wedge \\ (\phi(u, v, t) < -0.1 \vee \phi(u, v, t) > 0.1) \end{aligned} \quad (31)$$

where $\phi(u, v, t) = c_0\lambda_0 e^{\lambda_0 t} + 2(\text{Re}(c_1\lambda_1)u - \text{Im}(c_1\lambda_1)v)e^{\alpha t}$. Then, using the method proposed in [16], we prove that 1) $\phi(u, v, t) > 0.1$ is invalid, and thus $x \leq 1.1$ in (30) is verified; and 2) the interval $(0.5, T]$ covers all t that make $\phi(u, v, t) < -0.1$ satisfiable in (31). Here, T is the unique root of $|c_0\lambda_0|e^{\lambda_0 t} + 2|c_1\lambda_1|e^{\alpha t} - 0.1$, which can be approximated by real root isolation with arbitrary precision. We adopt 0.6 as an overapproximation of T here (see Fig. 1).

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 [18], [23] that even for $t \in (0.5, 0.6]$ Y cannot be reached. Therefore, we have proved the property (30) for the given system.

VIII. CONCLUSION

In this paper, we extended our previous approaches on reachability analysis for linear vector fields given in [16] and [17] to solvable nonlinear vector fields. To this end, we first identified

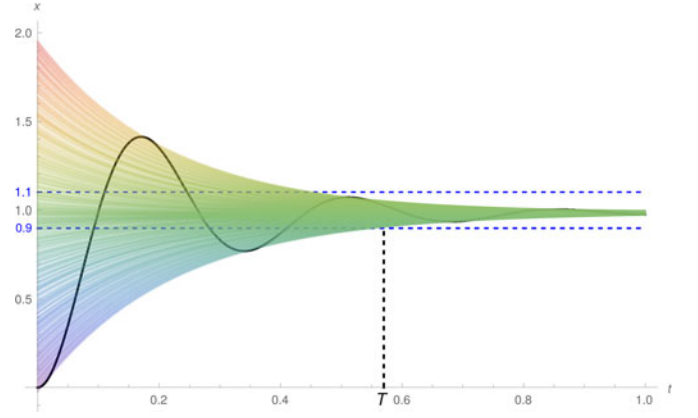


Fig. 1. Overapproximation (the “broom”) of the trajectory of x (the curve) starting from 0. Here, the two horizontal dashed lines specify the boundaries of the safe set, while T indicates a point in time, after which the behavior of the overapproximated system stays within the safe region.

three families of solvable nonlinear vector fields, i.e., the cases when the matrices in (4) are, respectively, *nilpotent*, *only with real eigenvalues* and *only with pure imaginary eigenvalues*, and proved their reachability problems are decidable. In addition, we presented an approach on how to abstract the reachability problem of general solvable dynamical systems (4) to the decision problem of \mathcal{T}_e . A prototypical tool has been implemented, and experimental results indicate our approach is efficient.

As a future work, it could be interesting to investigate whether the reachable set computation of general nonlinear vector fields, even nonpolynomial vector fields can be abstracted to that of solvable ones, further to that of linear ones, by exploiting our previous work in [28].

ACKNOWLEDGMENT

The authors would like to thank Dr. M. Xu for insightful discussions on the density results in number theory. They are also indebted to the anonymous referees for their constructive comments, which improve the presentation of this paper so much.

REFERENCES

- [1] [Online]. Available: <http://www.math.utah.edu/~gustafso/s2013/2250/systemsExamplesTheory2008.pdf>
- [2] M. Achatz, S. McCallum, and V. Weispfenning, “Deciding polynomial-exponential problems,” in *Proc. Int. Symp. Symbolic Algebr. Comput.*, 2008, pp. 215–222.
- [3] R. Alur *et al.*, “The algorithmic analysis of hybrid systems,” *Theor. Comput. Sci.*, vol. 138, no. 1, pp. 3–34, 1995.
- [4] R. Alur and D. L. Dill, “A theory of timed automata,” *Theor. Comput. Sci.*, vol. 126, no. 2, pp. 183–235, 1994.
- [5] H. Anai and V. Weispfenning, “Reach set computations using real quantifier elimination,” in *Proc. Hybrid Syst., Comput. Control*, vol. 2034, 2001, pp. 63–76.
- [6] C. W. Brown, “Improved projection for cylindrical algebraic decomposition,” *J. Symbolic Comput.*, vol. 32, no. 5, pp. 447–465, 2001.
- [7] X. Chen, E. Ábrahám, and S. Sankaranarayanan, “Flow*: An analyzer for non-linear hybrid systems,” in *Proc. Comput. Aided Verification*, vol. 8044, 2013, pp. 258–263.
- [8] V. Chonev, J. Ouaknine, and J. Worrell, “On recurrent reachability for continuous linear dynamical systems,” in *Proc. 31st Annu. ACM/IEEE Symp. Logic Comput. Sci.*, 2016, pp. 515–524.
- [9] V. Chonev, J. Ouaknine, and J. Worrell, “On the Skolem problem for continuous linear dynamical systems,” in *Proc. 43rd Int. Colloq. Automata, Lang., Program.*, 2016, pp. 100:1–100:13.

- [10] G. E. Collins, "Quantifier elimination for real closed fields by cylindrical algebraic decomposition," in *Proc. 2nd GI Conf. Automata Theory Formal Lang.*, 1975, pp. 134–183.
- [11] G. E. Collins and H. Hong, "Partial cylindrical algebraic decomposition for quantifier elimination," *J. Symbolic Comput.*, vol. 12, no. 3, pp. 299–328, 1991.
- [12] G. E. Collins and R. Loos, "Real zeros of polynomials," in *Comput. Algebra—Symbolic Algebr. Comput.* Berlin, Germany: Springer-Verlag, 1982, pp. 83–94.
- [13] J. H. Davenport and J. Heintz, "Real quantifier elimination is doubly exponential," *J. Symbolic Comput.*, vol. 5, no. 1, pp. 29–35, 1988.
- [14] A. Dolzmann and T. Sturm, "Redlog: Computer algebra meets computer logic," *ACM SIGSAM Bull.*, vol. 31, no. 2, pp. 2–9, 1997.
- [15] G. Frehse *et al.*, "SpaceEx: scalable verification of hybrid systems," in *Proc. Comput. Aided Verification*, 2011, pp. 379–395.
- [16] T. Gan, M. Chen, L. Dai, B. Xia, and N. Zhan, "Decidability of the reachability for a family of linear vector fields," in *Proc. Automated Technol. Verification Anal.*, vol. 9364, 2015, pp. 482–499.
- [17] T. Gan, M. Chen, Y. Li, B. Xia, and N. Zhan, "Computing reachable sets of linear vector fields revisited," in *Proc. Eur. Control Conf.*, 2016, pp. 419–426.
- [18] A. Girard and G. Pappas, "Verification using simulation," in *Proc. Hybrid Syst., Comput. Control*, vol. 3927, 2006, pp. 272–286.
- [19] J. Han, L. Dai, and B. Xia, "Constructing fewer open cells by GCD computation in CAD projection," in *Proc. Int. Symp. Symbolic Algebr. Comput.*, 2014, pp. 240–247.
- [20] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* 5th ed. Oxford, U.K.: Oxford Univ. Press, 1979.
- [21] T. A. Henzinger, P. W. Kopke, A. Puri, and P. Varaiya, "What's decidable about hybrid automata?" *J. Comput. Syst. Sci.*, vol. 57, no. 1, pp. 94–124, 1998.
- [22] H. Hong, "An improvement of the projection operator in cylindrical algebraic decomposition," in *Proc. Int. Symp. Symbolic Algebr. Comput. ACM*, 1990, pp. 261–264.
- [23] Z. Huang and S. Mitra, "Computing bounded reach sets from sampled simulation traces," in *Proc. Hybrid Syst., Comput. Control*, 2012, pp. 291–294.
- [24] H. Iwane, H. Yanami, and H. Anai, "SyNRAC: A toolbox for solving real algebraic constraints," in *Proc. Int. Congr. Math. Softw.* Berlin, Germany: Springer, 2014, pp. 518–522.
- [25] S. Kong, S. Gao, W. Chen, and E. Clarke, "dReach: Delta-reachability analysis for hybrid systems," in *Proc. Int. Conf. Tools Algorithms Construction Anal. Syst.*, vol. 9035, 2015, pp. 200–205.
- [26] G. Lafferriere, G. J. Pappas, and S. Sastry, "O-minimal hybrid systems," *Math. Control, Signals Syst.*, vol. 13, no. 1, pp. 1–21, 2000.
- [27] G. Lafferriere, G. J. Pappas, and S. Yovine, "Symbolic reachability computation for families of linear vector fields," *J. Symbolic Comput.*, vol. 32, pp. 231–253, 2001.
- [28] J. Liu, N. Zhan, H. Zhao, and L. Zou, "Abstraction of elementary hybrid systems by variable transformation," in *Proc. Format Methods*, vol. 9109, 2015, pp. 360–377.
- [29] S. McCallum, "An improved projection operation for cylindrical algebraic decomposition of three-dimensional space," *J. Symbolic Comput.*, vol. 5, no. 1, pp. 141–161, 1988.
- [30] S. McCallum and V. Weispfenning, "Deciding polynomial-transcendental problems," *J. Symbolic Comput.*, vol. 47, no. 1, pp. 16–31, 2012.
- [31] S. Mover, A. Cimatti, A. Tiwari, and S. Tonetta, "Time-aware relational abstractions for hybrid systems," in *Proc. Int. Conf. Embedded Softw.*, 2013, pp. 14:1–14:10.
- [32] J. Ouaknine, J. Sousa-Pinto, and J. Worrell, "On the polytope escape problem for continuous linear dynamical systems," in *Proc. Int. Conf. Hybrid Syst., Comput. Control*, 2017, pp. 11–17.
- [33] S. Ratschan and Z. She, "Safety verification of hybrid systems by constraint propagation based abstraction refinement," in *Proc. Hybrid Syst., Comput. Control*, vol. 3414, 2005, pp. 573–589.
- [34] D. Richardson, "How to recognize zero," *J. Symbolic Comput.*, vol. 24, pp. 627–645, 1997.
- [35] E. Rodríguez-Carbonell and D. Kapur, "Generating all polynomial invariants in simple loops," *J. Symbolic Comput.*, vol. 42, no. 4, pp. 443–476, 2007.
- [36] A. Strzeboński, "Solving systems of strict polynomial inequalities," *J. Symbolic Comput.*, vol. 29, no. 3, pp. 471–480, 2000.
- [37] A. Strzeboński, "Real root isolation for exp-log functions," in *Proc. Int. Symp. Symbolic Algebr. Comput.*, 2008, pp. 303–314.
- [38] A. Strzeboński, "Cylindrical decomposition for systems transcendental in the first variable," *J. Symbolic Comput.*, vol. 46, pp. 1284–1290, 2011.
- [39] A. Tarski, *A Decision Method for Elementary Algebra and Geometry*. Berkeley, CA, USA: Univ. of California Press, 1951.
- [40] J. Wing, "How can we provide people with cyber-physical systems they can bet their lives on?" *Comput. Res. News*, vol. 20, no. 1, 2008.
- [41] M. Xu, Z. Li, and L. Yang, "Quantifier elimination for a class of exponential polynomial formulas," *J. Symbolic Comput.*, vol. 68, no. Part 1, pp. 146–168, 2015.
- [42] M. Xu, J. Zhu, and Z. Li, "Some decidable results on reachability of solvable systems," *Int. J. Gen. Syst.*, vol. 42, no. 4, pp. 405–425, 2013.
- [43] H. Yazarel and G. J. Pappas, "Geometric programming relaxations for linear system reachability," in *Proc. 2004 Amer. Control Conf.*, vol. 1, 2004, pp. 553–559.

Ting Gan received the B.Sc. degree in mathematics from the Department of Mathematics, Beihang University, Beijing, China, in 2011, and the Ph.D. degree in mathematics from Peking University, Beijing, China, in 2017.

He currently holds a Postdoc position at the Computer School of Wuhan University, Wuhan, China. His research interests include program verification and formal design of hybrid systems.

Mingshuai Chen received the B.Sc. degree in computer science from the School of Computer Science and Technology, Jilin University, Changchun, China, in 2013, and is currently working toward the Ph.D. degree at the Institute of Software, Chinese Academy of Sciences, Beijing, China.

His research interests include program verification and formal design of hybrid systems.

Yangjia Li received the B.Sc. and Ph.D. degrees in computer science from the Department of Computer Science and Technology, Tsinghua University, Beijing, China, in 2008 and 2014.

He currently holds a Postdoc position at the Institute of Software, Chinese Academy of Sciences, Beijing, China. His research interests include quantum computation and hybrid systems.

Bican Xia received the Ph.D. degree in mathematics from the Department of Mathematics, Sichuan University, Chengdu, China, in 1998.

He is currently a Professor at Peking University, Beijing, China. His research interests include semialgebraic system solving, automated reasoning, and hybrid system verification.

Naijun Zhan received the B.Sc. degree in mathematics and the M.Sc. degree in computer science both from Nanjing University, Nanjing, China, in 1993 and in 1996, respectively, and the Ph.D. degree in computer science from the Institute of Software, Chinese Academy of Sciences, Beijing, China.

He was with the Faculty of Mathematics and Information, University of Mannheim, Mannheim, Germany, as a Research Fellow, from 2001 to 2004. Since then, he joined the Institute of Software, Chinese Academy of Sciences, as an Associate Research Professor, and was promoted to be a Full Research Professor in 2008. His research interests include real-time, embedded, and hybrid systems, program verification, concurrent computation models, and modal and temporal logics.