Journal of Symbolic Computation 45 (2010) 1234–1249

Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

Termination of linear programs with nonlinear constraints[☆]

Bican Xia[a], Zhihai Zhang[a,b,1]

[a] LMAM & School of Mathematical Sciences, Peking University, Beijing 100871, China

[b] Department of Computer Science, University of New Mexico, Albuquerque, USA

ARTICLE INFO

Article history:
Received 25 March 2010
Accepted 11 April 2010
Available online 22 June 2010

Keywords:
Termination
Quantifier elimination
Semi-algebraic system
Rationally independent group
Cyclotomic polynomial

ABSTRACT

Tiwari (2004) proved that the termination problem of a class of linear programs (loops with linear loop conditions and updates) over the reals is decidable through Jordan forms and eigenvector computation. Braverman (2006) proved that it is also decidable over the integers. Following their work, we consider the termination problems of three more general classes of programs which are loops with linear updates and three kinds of polynomial loop conditions, i.e., strict constraints, non-strict constraints and both strict and non-strict constraints, respectively. First, we prove that the termination problems of such loops over the integers are all undecidable. Then, for each class we provide an algorithm to decide the termination of such programs over the reals. The algorithms are complete for those programs satisfying a property, *Non-Zero Minimum*.

1. Introduction

Termination analysis is an important aspect of program verification. Guaranteed termination of program loops is necessary for many applications, especially those for which unexpected behavior can be catastrophic. For a generic loop

while (*conditions*) {*updates*},

it is well known that the termination problem is undecidable in general, even for a simple class of polynomial programs (Bradley et al., 2005). Blondel et al. (2001) proved that, even when all the

[☆] This work is supported in part by NSFC-90718041, NKBRPC-2005CB321902 and China Scholarship Council in China.

E-mail addresses: xbc@math.pku.edu.cn (B. Xia), infzzh@gmail.com, infzzh@math.pku.edu.cn (Z. Zhang).

[1] Tel.: +86 10 62767219; fax: +86 10 62751801.

0747-7171/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2010.06.006

conditions and updates are given as piecewise linear functions, the termination of the loop remains undecidable.

Tiwari (2004) proved that termination of the following program is decidable over $\mathbb{R}$ (the real numbers)

$$LP_0: \quad \textbf{while} \quad (BX > b) \quad \{X := AX + C\},$$

where $X = [x_1 \dots x_N]^{\mathrm{T}}$ is the vector of state variables of the program, A and B are respectively $N \times N$ and $M \times N$ rational matrices, b and C are rational vectors, $BX > b$ represents a conjunction of linear inequalities over the state variables X and $X := AX + C$ represents a (deterministic) simultaneous update of all variables. His method is based on Jordan forms and eigenvector computation. However, Xia et al. provided a symbolic method to determine the termination of LP_0 in Xia et al. (2009). Braverman (2006) proved that the termination of LP_0 is decidable over $\mathbb{Z}$ (the integers).

In this paper, we consider the termination problem of the following loop:

$$\widetilde{LP}_1: \quad \textbf{while} \quad (P(X) > b) \quad \{X := AX + C\},$$

where $P(X) = [P_1(X)\ P_2(X) \dots P_M(X)]^{\mathrm{T}} > b$ are polynomial constraints, each $P_i(X)$ $(1 \le i \le M)$ is a polynomial in $\mathbb{Q}[X]$ and A is an $N \times N$ matrix over $\mathbb{Q}$ (the rational numbers). That is to say, we replace the linear constraints in the loop condition of LP_0 with polynomial constraints and keep linear updates unchanged. If $b = \mathbf{0}$ and $C = \mathbf{0}$, $\widetilde{LP}_1$ becomes

$$LP_1: \quad \textbf{while} \quad (P(X) > 0) \quad \{X := AX\}.$$

The termination of $\widetilde{LP}_1$ can be reduced to the termination of some LP_1 by replacing X with $(X^T, 1)^T$ and A with A' where

$$A' = \begin{pmatrix} A & C \\ 0 & 1 \end{pmatrix}.$$

Without loss of generality, we will consider the termination problems of LP_1 and the following two more classes of programs

$$LQ_1: \quad \textbf{while} \quad (P(X) \ge 0) \quad \{X := AX\}$$
$$LR_1: \quad \textbf{while} \quad (P(X) > 0 \wedge R(X) \ge 0) \quad \{X := AX\},$$

where X, A and P are the same as in LP_1 and $R(X)$ is a set of polynomials in $\mathbb{Q}[X]$. Throughout this paper, we mainly discuss the termination of LP_1.

There are some well known techniques for deciding termination of some special kinds of programs. Ranking functions are most often used for this purpose. A ranking function for a loop maps the values of the loop variables to a well-founded domain; further, the values of the map decrease on each iteration. A linear ranking function is a ranking function that is a linear combination of the loop variables and constants. Recently, the synthesis of ranking functions draws increasing attention, and some heuristics concerning how to automatically generate linear ranking functions for linear programs have been proposed, for example, in Colon and Sipma (2001), Dams et al. (2000) and Podelski and Rybalchenko (2004). Podelski and Rybalchenko (2004) provided an efficient and complete synthesis method based on linear programming to construct linear ranking functions. Chen et al. (2007) proposed a method to generate nonlinear ranking functions based on semi-algebraic system solving. However, the existence of ranking function is only a sufficient condition on the termination of a program. There are programs, which terminate, but do not have ranking functions. Another popular technique, presented in Lee et al. (2001), is size-change principle, which is based on parameter size changes and well-founded data. The well-founded data can ensure that there are no infinitely descents, which guarantees termination of programs.

To solve the termination problem of LP_1, we do not use the technique of ranking functions, size-change principle or Jordan forms. Our method is similar to that of Tiwari in some sense, but use different techniques. Our main contributions in this paper are as follows. First, we prove that the termination problems of LP_1, LQ_1 and LR_1 over $\mathbb{Z}$ are undecidable. Furthermore, if the entries of A in LP_1, LQ_1 and LR_1 are confined to integers, the termination problems of the resulted LP_1, LQ_1 and

LR_1 over $\mathbb{Z}$ are still undecidable. Second, we provide an algorithm to decide the termination of LP_1 satisfying an additional property over $\mathbb{R}$. Then, we extend this algorithm to determine the termination of LQ_1 and LR_1 over $\mathbb{R}$. Finally, we conjecture that the termination problems of LP_1, LQ_1 and LR_1 over $\mathbb{R}$ are undecidable in general.

The rest of the paper is organized as follows. Section 2 proves the undecidability of LP_1, LQ_1 and LR_1 over $\mathbb{Z}$. Section 3 presents our main algorithm and the proof for its correctness is given in Section 4. The main algorithm is extended to determine the termination of LQ_1 and LR_1 over $\mathbb{R}$ in Section 5. The details of some proofs and algorithms are presented in Section 6. We conclude the paper in Section 7.

2. Undecidability of LP_1 over $\mathbb{Z}$

Definition 1. A loop with N variables is called *terminating* over a ring R if for any input $X \in R^N$, it terminates; otherwise it is called *nonterminating*.

The undecidability of LP_1 over $\mathbb{Z}$ is obtained by reduction of Hilbert's 10^{th} problem. Consider the following loop:

$$LP_2: \quad \textbf{while} \quad (x_N - f(x_1, \ldots, x_{N-1})^2 > 0) \quad \{X := AX\}$$

where $X = [x_1 \ldots x_N]^{\mathrm{T}}$, $A = \mathrm{diag}(1, \ldots, 1, 1/2)$ is a diagonal matrix and $f(x_1, \ldots, x_{N-1})$ is a polynomial with integer coefficients.

Lemma 2. *For any input $(x_1, \ldots, x_N) \in \mathbb{Z}^N$ LP_2 terminates if and only if $f(x_1, \ldots, x_{N-1})$ does not have integer roots.*

Proof. ($\Rightarrow$) If f has an integer root, say $(y_1, \ldots, y_{N-1})$, obviously LP_2 does not terminate with the input $Y = (y_1, \ldots, y_{N-1}, 1)$.

($\Leftarrow$) If $f(x_1, \ldots, x_{N-1})$ has no integer roots, for any given $X \in \mathbb{Z}^N$, $-f(x_1, \ldots, x_{N-1})^2$ is a fixed negative number. Because $(x_1, \ldots, x_{N-1})$ will never be changed and $(1/2)^n \to 0$ as $n \to +\infty$, the loop will terminates after sufficiently large n iterations. □

Theorem 3. *Termination of LP_1 over $\mathbb{Z}$ is undecidable.*

Proof. Because the existence of an integer root of an arbitrary Diophantine equation is undecidable, the termination of LP_1 over $\mathbb{Z}$ is undecidable according to Lemma 2. □

Let us denote by LQ_2 the loop obtained by substituting "$\geq$" for "$>$" in LP_2. From the proof of Lemma 2, it is easy to see that Lemma 2 still holds for LQ_2. Then we get the following theorem.

Theorem 4. *Termination of LQ_1 over $\mathbb{Z}$ is undecidable.*

In order to obtain the undecidability of LR_1 over $\mathbb{Z}$, let us consider the following loop.

$$LR_2: \quad \textbf{while} \quad (x_{N+1} - f(x_1, \ldots, x_{N-1})^2 > 0 \wedge x_N \geq 0) \quad \{X := AX\}$$

where f is the same as in LP_2 and $A = \mathrm{diag}(1, \ldots, 1, 1/2)$ is an $(N+1) \times (N+1)$ diagonal matrix. According to the proof of Lemma 2, it still holds for LR_2. Hence, we obtain the following theorem.

Theorem 5. *Termination of LR_1 over $\mathbb{Z}$ is undecidable.*

In LP_2, LQ_2 and LR_2, one of the entries of A is a rational number. A natural question is whether the termination problems of LP_1, LQ_1 and LR_1 over $\mathbb{Z}$ are still undecidable if all the entries of A are confined to integers. Let us consider the following program.

$$LP_3: \quad \textbf{while} \quad (x_N - x_{N+1}^2 f(x_1, \ldots, x_{N-1})^2 > 0 \wedge x_{N+1}^2 - 1 > 0) \quad \{X := AX\}$$

where $X = [x_1 \ldots x_{N+1}]^{\mathrm{T}}$, $A = \mathrm{diag}(1, \ldots, 1, 2)$ is a diagonal matrix and $f(x_1, \ldots, x_{N-1})$ is a polynomial with integer coefficients.

Lemma 6. *For any input $X \in \mathbb{Z}^{N+1}$ LP_3 terminates if and only if $f(x_1, \ldots, x_{N-1})$ does not have integer roots.*

Proof ($\Rightarrow$). If f has an integer root, say $(y_1, \dots, y_{N-1})$, obviously LP_3 does not terminate with the input $Y = (y_1, \dots, y_{N-1}, 1, 2)$.

($\Leftarrow$) If $f(x_1, \dots, x_{N-1})$ has no integer roots, for any given $X \in \mathbb{Z}^{N+1}$ satisfying the loop constraint of LP_3, $-x_{N+1}^2 f(x_1, \dots, x_{N-1})^2$ will go to the negative infinity as LP_3 is executed. However, the assignment in LP_3 does not change the value of x_N. Finally, $x_N - x_{N+1}^2 f(x_1, \dots, x_{N+1})^2$ will become negative. Hence, the loop will terminate after sufficiently large n iterations. □

Thus, we obtain the following theorem.

Theorem 7. *If all the entries of A in LP_1 are confined to integers, termination of LP_1 over $\mathbb{Z}$ is still undecidable.*

Similarly, we can get the following theorem.

Theorem 8. *If all the entries of A in LQ_1 (LR_1) are confined to integers, termination of LQ_1 (LR_1) over $\mathbb{Z}$ is still undecidable.*

3. Algorithm for termination of LP_1 over $\mathbb{R}$

To decide whether LP_1 is terminating, it is equivalent to check whether there exists X such that $P(A^n X) > 0$ holds for all $n \geq 0$. That means we should check the sign of each $P_i(A^n X)$ for all $i = 1, \dots, N$ and for all $n \geq 0$. To this end, we first compute $A^n X$, the value of state variables X after n iterations, and obtain a unified formula expressing each entry of $A^n X$. Then we express the value of $P_i(A^n X)$ using the formula. Finally, we may try to determine whether $P_i(A^n X) > 0$ as $n \to +\infty$ by guessing its dominant term and deciding the sign of this term. That is the main idea of our algorithm which will be described formally in Section 3.4.

3.1. Formulae expressing each entry of $A^n X$

Intuitively, by considering the Jordan form of A over $\mathbb{C}$, each entry of $A^n X$ can be expressed in $x_1, \dots, x_N$, n and the complex eigenvalues ξ_i's of A. The following proposition gives an exact description of each entry of $A^n X$ and its proof is presented in Section 6.

Proposition 9. *Suppose A is a $d \times d$ square matrix with its entries in $\mathbb{Q}$ and the characteristic polynomial of A is $D(x) = x^d + \alpha_1 x^{d-1} + \cdots + \alpha_{d-u} x^u$, where $\alpha_{d-u} \neq 0$ and $u \geq 0$. Define $F(X, n) = A^{n+u} X$ and let $F_j(X, n)$ be the jth component of $F(X, n)$. Then for each j, $F_j(X, n)$ can be expressed as*

$$F_j(X, n) = \sum_{i=1}^{k} f_{ji}(X, n) \xi_i^n, \tag{1}$$

where ξ_i's are all the distinct non-zero complex eigenvalues of A and $f_{ji}(X, n)$ is a polynomial in n of degree less than the multiplicity of ξ_i.

Remark 10. According to Proposition 9, we may compute the unified formulae for $A^{n+u} X$ in the form of Eq. (1) as follows. First, compute all the complex eigenvalues of A and their multiplicities. Second, suppose each $F_j(X, n)$ of $F(X, n)$ is in the form of Eq. (1) where the coefficients of f_{ji} are to be computed. Third, compute $F(X, 1), \dots, F(X, d)$, and obtain a set of linear equations by comparing the coefficients of the result $F_j(X, i)$ ($1 \leq i \leq d$) to those of Eq. (1). Finally, by solving those linear equations, we can obtain $F_j(X, n)$ and $F(X, n)$.

Example 11. For clarity, let us consider a simple loop:

$$\textbf{while} \quad (x_1^2 + x_1 x_2 > 0) \quad \{X := AX\},$$

where

$$A = \begin{bmatrix} 1 & -\frac{2}{5} \\ 2 & \frac{1}{5} \end{bmatrix}.$$

We shall show how to compute the unified formula for each entry of A^nX by Proposition 9. The characteristic polynomial of A is

$$D(\lambda) = \lambda^2 - \frac{6}{5}\lambda + 1.$$

The eigenvalues of A are

$$\xi_1 = \frac{3+4\mathbf{i}}{5}, \qquad \xi_2 = \frac{3-4\mathbf{i}}{5}.$$

Set $F(X,n) = A^nX = \begin{bmatrix} F_1(X,n) & F_2(X,n) \end{bmatrix}^T$. Because the multiplicities of ξ_1 and ξ_2 are all 1, by Proposition 9 we get

$$F_1(X,n) = (a_{11}x_1 + a_{12}x_2)\xi_1^n + (b_{11}x_1 + b_{12}x_2)\xi_2^n,$$
$$F_2(X,n) = (a_{21}x_1 + a_{22}x_2)\xi_1^n + (b_{21}x_1 + b_{22}x_2)\xi_2^n.$$

Let $F(X,1)$ and $F(X,2)$ be equal to AX and A^2X, respectively, and by solving some linear equations (see Remark 10) we obtain

$$F_1(X,n) = \left(\frac{2-\mathbf{i}}{4}x_1 + \frac{\mathbf{i}}{4}x_2\right)\xi_1^n + \left(\frac{2+\mathbf{i}}{4}x_1 - \frac{\mathbf{i}}{4}x_2\right)\xi_2^n,$$
$$F_2(X,n) = \left(\frac{-5\mathbf{i}}{4}x_1 + \frac{2+\mathbf{i}}{4}x_2\right)\xi_1^n + \left(\frac{5\mathbf{i}}{4}x_1 + \frac{2-\mathbf{i}}{4}x_2\right)\xi_2^n.$$

3.2. *Formulae expressing each resulted $P_j(X)$ after n iterations*

If we substitute the unified formulae of $A^{n+u}X$ for X in $P(X)$ and denote the resulted $P_j(X)$ $(1 \le j \le M)$ by $P_j(X,n)$, then $P_j(X,n)$ can be written as

$$P_j(X,n) = p_{j0}(X,n) + p_{j1}(X,n)\eta_1^n + \cdots + p_{jm}(X,n)\eta_m^n, \tag{2}$$

where η_k $(1 \le k \le m)$ is the product of some ξ_j's.

To determine whether LP_1 terminates, we have to determine whether there exists X such that for each j, $P_j(X,n) > 0$ holds for all n. To this end, it is sufficient to know whether there exists X such that all the dominant terms (*leading terms*, to be defined later) of the $P_j(X,n)$'s are positive as $n \to +\infty$. In the following, we shall give a more detailed description of $P_j(X,n)$ so that we can obtain the expression of its leading term.

Let $\eta_k = r_k e^{\alpha_k 2\pi \mathbf{i}}$, where $\mathbf{i} = \sqrt{-1}$ and r_k is the modulus of η_k. Without loss of generality, we assume $r_1 < r_2 < \cdots < r_m$. Set $\eta_0 = r_0 = 1$ and rewrite $P_j(X,n)$ as

$$P_j(X,n) = p_{j0}(X,n)r_0^n + \cdots + p_{jm}(X,n)e^{n\alpha_m 2\pi\mathbf{i}}r_m^n. \tag{3}$$

Suppose T is the common period[2] of all $e^{\alpha_q 2\pi \mathbf{i}}$'s contained in $P_j(X,n)$ $(1 \le j \le M)$ where α_q is rational. Obviously $e^{(Tn+t)\alpha_q 2\pi\mathbf{i}} = e^{t\alpha_q 2\pi\mathbf{i}}$ for all rational α_q and $0 \le t \le T-1$. Hence

$$\exists X \forall n \wedge_{j=1}^{M} P_j(X,n) > 0 \Leftrightarrow \exists X \bigwedge_{t=0}^{T-1} (\forall n \wedge_{j=1}^{M} P_j(X, Tn+t) > 0).$$

Thus, in what follows, we shall focus on checking whether there exists X such that

$$\bigwedge_{t=0}^{T-1} (\forall n \wedge_{j=1}^{M} P_j(X, Tn+t) > 0).$$

[2] An algorithm, `ComputingCommonPeriod`, for computing T is presented in Section 6.

Definition 12. For each j $(1 \le j \le MT)$, if $j = (s-1)T + t$ $(1 \le t \le T)$, then define

$$G_j(X, n) \triangleq P_s(X, Tn + t - 1).$$

Notation 1. For each j $(1 \le j \le MT)$, expand $G_j(X, n)$, collect the result with respect to (w.r.t.) $n^l r_k^n$, and let $C_{jkl}(X, n)$ denote the coefficient of the term $n^l r_k^n$.

Then $G_j(X, n)$ can be written as

$$\begin{aligned} &C_{j00}(X, n)r_0^n + C_{j01}(X, n)nr_0^n + \cdots + C_{j0d_0}(X, n)n^{d_0}r_0^n + \cdots \\ &\quad + C_{jm0}(X, n)r_m^n + C_{jm1}(X, n)nr_m^n + \cdots + C_{jmd_m}(X, n)n^{d_m}r_m^n, \end{aligned}$$

where d_l $(0 \le l \le m)$ is the greatest degree of n in $G_j(X, n)$ w.r.t. r_l.

It can be deduced that if $r_i < r_j$, $n^{l_1}r_i^n/n^{l_2}r_j^n$ tends to zero for any l_1 and l_2 as n goes to infinity. Similarly, if $l_1 < l_2$, $n^{l_1}r_i^n/n^{l_2}r_i^n$ tends to zero too as n goes to infinity. So, it is natural to define an ordering over the terms $n^l r_j^n$ as follows.

Definition 13. We define $n^{l_1}r_i^n \lessdot n^{l_2}r_j^n$ if $r_i < r_j$ or $r_i = r_j$ and $l_1 < l_2$. A term $C_{jkl}n^l r_k^n$ in $G_j(X, n)$ is said to be the *leading term* and C_{jkl} the *leading coefficient* if $n^l r_k^n$ occurring in $G_j(X, n)$ is the largest one under that ordering $\lessdot$.

Suppose $G_j(X, n) = P_s(X, Tn + t)$ for some s and t. If α_q is a rational number

$$\mathrm{e}^{(Tn+t)\alpha_q 2\pi \mathbf{i}} = \mathrm{e}^{t\alpha_q 2\pi \mathbf{i}},$$

and n is eliminated from the above expression. However, since there may be some $\mathrm{e}^{(Tn+t)\alpha_q 2\pi \mathbf{i}}$'s with irrational α_q's, each $C_{jkl}(X, n)$ can be divided into two parts,

$$C_{jkl}(X, n) = C_{jkl1}(X) + C_{jkl2}(X, n),$$

where $C_{jkl1}(X)$ does not depend on n and $C_{jkl2}(X, n)$ contains those $\mathrm{e}^{(T_s n+t)\alpha_q 2\pi \mathbf{i}}$ with irrational α_q,[3] where n cannot be eliminated. Further, $C_{jkl2}(X, n)$ can be written as

$$\begin{aligned} &C'_{jkl2}(X, \sin((nT + t)\alpha_{k1}2\pi), \cos((nT + t)\alpha_{k1}2\pi), \ldots, \sin((nT + t)\alpha_{ks_k}2\pi), \\ &\quad \cos((nT + t)\alpha_{ks_k}2\pi)), \end{aligned}$$

where $\{\alpha_{k1}, \ldots, \alpha_{ks_k}\}$ is a maximum *rationally independent* group.[4] For the sake of clarity, these two notations will be used interchangeably in what follows.

Example 14. We continue to use the loop in Example 11 to illustrate the above concepts and notations.

Because $|\xi_1| = |\xi_2| = 1$, let $\xi_1 = \mathrm{e}^{\alpha_1 2\pi \mathbf{i}}$ and $\xi_2 = \mathrm{e}^{-\alpha_1 2\pi \mathbf{i}}$, where $\alpha_1 2\pi$ is the argument of ξ_1. With an algorithm in Section 6 it can be checked that α_1 is an irrational number,[5] and there is no eigenvalue of A whose argument is a rational multiple of π. Hence T is 1. For clarity, in the following we firstly reduce the expressions of $F_1(X, n)$ and $F_2(X, n)$, and then substitute them in the loop guard. After careful computation, it is obtained that

$$F_1(X, n) = x_1 \cos(n\alpha_1 2\pi) + \frac{x_1 - x_2}{2}\sin(n\alpha_1 2\pi),$$

$$F_2(X, n) = x_2 \cos(n\alpha_1 2\pi) + \frac{5x_1 - x_2}{2}\sin(n\alpha_1 2\pi).$$

[3] In fact $C_{jkl1}(X)$ and $C_{jkl2}(X, n)$ are real for any n.

[4] An algorithm, `MaximumRationallyIndependentGroup`, described in Section 6 aims at computing a maximum rationally independent group, and the related further explanations will be made.

[5] It is solved by an algorithm, `FindingPeriod`, presented in Section 6, which checks whether the argument of an algebraic number is a rational multiple of π.

Substituting $F_1(X,n)$ and $F_2(X,n)$ for x_1 and x_2 respectively in the loop guard, we get that the resulted loop guard is

$$G_1(X,n) = C_{100}(X,n)1^n = C_{1001}(X) + C_{1002}(X,n),$$

where

$$C_{1001}(X) = \frac{5x_1^2 + x_2^2 - 2x_1x_2}{4}, \qquad C_{1002}(X,n) = D_1\cos(n2\alpha_1 2\pi) + D_2\sin(n2\alpha_1 2\pi),$$
$$D_1 = \frac{-x_1^2 - x_2^2 + 6x_1x_2}{4}, \qquad D_2 = \frac{7x_1^2 - x_2^2 - 2x_1x_2}{4}.$$

3.3. The Non-Zero Minimum (NZM) property

Let $\mathbb{T} = \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 = 1\}$. Denote by

$$Y = (y_{11}, y_{12}, \ldots, y_{D1}, y_{D2}) \in \mathbb{T}^D$$

if $(y_{i1}, y_{i2}) \in \mathbb{T}$ for $1 \le i \le D$. In the following we shall write $Y \in \mathbb{T}^D$ for short.

Notation 2. Denote by $C_{jkl}(X,n) \succ 0$ (and call $C_{jkl}(X,n)$ “positive") if

$$\min\{C_{jkl1}(X) + C'_{jkl2}(X,Y)\} > 0 \quad \text{subject to } Y \in \mathbb{T}^{s_k},$$

where y_{i1} and y_{i2} correspond to $\sin(n\alpha_{ki}2\pi)$ and $\cos(n\alpha_{ki}2\pi)$ respectively for $1 \le i \le s_k$ in $C_{jkl2}(X,n)$. If $\succ$ and $>$ are replaced with $\succeq$ and $\ge$ respectively in the above, we get the notation of $C_{jkl}(X,n) \succeq 0$ (“nonnegative").

Remark 15. According to the definition of Notation 2, $C_{jkl}(X,n) \succ 0$ iff

$$\forall Y\ (Y \in \mathbb{T}^{s_k} \Rightarrow C_{jkl1}(X) + C'_{jkl2}(X,Y) > 0).$$

Since $\mathbb{T}^{s_k}$ is a bounded closed set, there exists some $c > 0$ such that

$$\forall Y\ (Y \in \mathbb{T}^{s_k} \Rightarrow C_{jkl1}(X) + C'_{jkl2}(X,Y) > c),$$

and then $\forall n \ge 0$, $C_{jkl}(X,n) > c$. Similarly, $C_{jkl}(X,n) \succeq 0$ iff

$$\forall Y\ (Y \in \mathbb{T}^{s_k} \Rightarrow C_{jkl1}(X) + C'_{jkl2}(X,Y) \ge 0).$$

Roughly speaking, for any $G_j(X,n)$, if its leading coefficient $C_{jkl}(X,n) \succ 0$ (“positive"), there exists an integer N_1 such that for all $n > N_1$, $G_j(X,n) > 0$. If the leading coefficients of all the $G_j(X,n)$'s are “positive", there exists N' such that for all $n > N'$, all the $G_j(X,n)$'s are positive. Therefore, LP_1 is nonterminating with input $X' := A^{N'}X$. On the other hand, if LP_1 is nonterminating, does there exist an input X such that the leading coefficients of all the $G_j(X,n)$'s are “positive"? We do not know the answer yet. However, if LP_1 satisfies the property below, the answer is yes.

Property Non-Zero Minimum (NZM): We say that LP_1 satisfies NZM if for any $X \in \mathbb{R}^N$ and any $C_{jkl}(X,n)$, $C_{jkl2}(X,n)$ being not identically zero implies

$$\min(C_{jkl1}(X) + C'_{jkl2}(X,Y)) \ne 0 \quad \text{subject to } Y \in \mathbb{T}^{s_k}. \tag{4}$$

According to the definition, NZM is equivalent to the following formula:

$$\begin{aligned}&[\forall X \forall Y\ (C_{jkl2}(X,n) \equiv 0 \vee (Y \in \mathbb{T}^{s_k} \Rightarrow C_{jkl1}(X) + C'_{jkl2}(X,Y) > 0))] \bigvee \\ &[\forall X \exists Y\ (C_{jkl2}(X,n) \equiv 0 \vee (Y \in \mathbb{T}^{s_k} \wedge C_{jkl1}(X) + C'_{jkl2}(X,Y) < 0))],\end{aligned}$$

where for a real value X, $C_{jkl2}(X,n) \equiv 0$ means that $C_{jkl2}(X,n) = 0$ for any $n \ge 0$. Because $C_{jkl2}(X,n)$ can be written as

$$\sum_{i \in I} f_{i1}(X)\sin(n\alpha_{ki}2\pi) + f_{i2}(X)\cos(n\alpha_{ki}2\pi),$$

where I is an index set, $C_{jkl2}(X, n) \equiv 0$ is equivalent to

$$\bigwedge_{i \in I} (f_{i1}(X) = f_{i2}(X) = 0).$$

Thus, NZM can be checked with real quantifier elimination techniques.

A large number of programs satisfy the property NZM, which include, for example, the following classes of programs where

1. all the eigenvalues of A are real numbers, for example when A is symmetric; or
2. the argument of each imaginary eigenvalue of A is a rational multiple of π; or
3. after substituting $A^{n+u}X$ for X in $P(X)$, the resulted $P(X)$ does not contain those $\mathrm{e}^{n\alpha_q 2\pi \mathbf{i}}$'s with irrational α_q's.

Since all the above cases can make $C_{jkl2}(X, n) \equiv 0$, the NZM is satisfied.

Example 16. For those C_{jkl}'s in Example 14, let us check whether they satisfy NZM. This example is so simple that we can check it by hand without real quantifier elimination techniques. From Example 14

$$\forall X, \quad D = \inf_{Y \in \mathbb{T}} C'_{1002}(X, Y) = \inf_{Y \in \mathbb{T}} D_1 y_2 + D_2 y_1 = -\sqrt{(D_1)^2 + (D_2)^2}.$$

Thus, $D = -\sqrt{\left(\frac{-x_1^2 - x_2^2 + 6x_1x_2}{4}\right)^2 + \left(\frac{7x_1^2 - x_2^2 - 2x_1x_2}{4}\right)^2}$.

Since $(C_{1001}(X))^2 - D^2 = \frac{-1}{16}(5x_1^2 + x_2^2 - 2x_1x_2)^2 \le 0$,

$$\forall X, \min_{Y \in \mathbb{T}} C_{100}(X, Y) = C_{1001}(X) + D \le 0. \tag{5}$$

If $C_{1001}(X) + D = 0$, $(C_{1001}(X))^2 - D^2 = \frac{-1}{16}(5x_1^2 + x_2^2 - 2x_1x_2)^2 = 0$. Then we obtain that $x_1 = x_2 = 0$ and $C_{1002}(X, n) \equiv 0$. Thus, NZM is satisfied.

Remark 17. There are, indeed, programs which do not satisfy NZM. The following example is one

$$\textbf{while} \quad (x_1x_2 + 5 > 0) \quad \left\{ X := \begin{bmatrix} \frac{3}{5} & -\frac{4}{5} \\ \frac{4}{5} & \frac{3}{5} \end{bmatrix} X \right\}.$$

However, this program is nonterminating by letting $x_1 = x_2 = 0$.

3.4. Main algorithm

Now, we are ready to describe our main algorithm. For brevity, the algorithm is described as a nondeterministic algorithm. The basic idea is to guess a leading term for each $G_j(X, n)$ first. Then, setting its coefficient to be “positive" and the coefficients of the terms with higher ordering to be “nonnegative", we get a semi-algebraic system (SAS). If one of our guesses is satisfiable, *i.e.*, one of the SASs has solutions, LP_1 is nonterminating. Otherwise, check whether NZM is satisfied. If so, return “terminating"; otherwise return “uncertain".

Main Algorithm 1 `Termination`$(A, P(X))$

```
Step 0 Compute the general expression of $A^{n+u}X$.
Step 1 Substitute $A^{n+u}X$ for $X$ in $P(X)$, and compute all $G_j(X, n)$ (finitely many, say, $j = 1, \dots, L$).
Step 2 Guess a leading term for each $G_j(X, n)$, say $C_{jk_jl_j} n^{l_j} r_{k_j}^n$.
Step 3 Construct a semi-algebraic system $S$ as follows.
           $S_j = C_{jk_jl_j} \succ 0 \wedge \bigwedge_{n^{l_j} r_{k_j}^n \lessdot n^l r_k^n} C_{jkl}(X, n) \succeq 0,$
           $S = \bigwedge_{j=1}^{L} S_j.$
Step 4 If one of these systems is satisfiable, return “nonterminating". Otherwise, if NZM is satisfied
       return “terminating"; otherwise return “uncertain".
```

Remark 18. It is well known that real quantifier elimination is decidable since Tarski's work (Tarski, 1951). Therefore, the semi-algebraic systems in Step 3 can be solved. For practical tools for solving semi-algebraic systems, please refer to Collins (1975), Collins and Hong (1991), Dolzman and Sturm (1997) and Xia (2007).

Example 19. For the loop in Example 11, we have computed $G_1(X, n)$ in Example 14 and verified that it satisfies NZM in Example 16. We shall finish the termination decision for this example, following the steps in `Termination`.

By Steps 2 and 3 of `Termination`, we should guess leading terms and construct SASs accordingly. Since there is only one $C_{100}(X, n)$, there is only one guess, $C_{100}(X, n) \succ 0$. In Example 16, we have shown that $\forall X, \min_{Y \in \mathbb{T}} C_{100}(X, Y) = C_{1001}(X) + D \leq 0$. Thus, the above predicate formula does not hold. Thus, the loop in Example 11 is terminating.

Remark 20. It may be interesting to point out that there are no continuous real-valued ranking functions for the program in Example 11.

Assume that there is a continuous real-valued ranking function, $\mathrm{Ran}(x_1, x_2)$, for the program in Example 11. According to the *ranking condition* of the ranking function, there exists $\epsilon > 0$ such that

$$\forall x_1, x_2, x_1^2 + x_1x_2 > 0 \Rightarrow \mathrm{Ran}(x_1, x_2) - \mathrm{Ran}\left(x_1 - \frac{2x_2}{5}, 2x_1 + \frac{x_2}{5}\right) > \epsilon.$$

Let $x_1 = x_2 = \frac{1}{n}$, which satisfy $x_1^2 + x_1x_2 > 0$ for any n. Hence,

$$\mathrm{Ran}\left(\frac{1}{n}, \frac{1}{n}\right) - \mathrm{Ran}\left(\frac{3}{5n}, \frac{11}{5n}\right) > \epsilon \quad \text{for any } n.$$

As n goes to infinity, the distance between $(\frac{1}{n}, \frac{1}{n})$ and $(\frac{3}{5n}, \frac{11}{5n})$ goes to zero, which means that the distance between $\mathrm{Ran}(\frac{1}{n}, \frac{1}{n})$ and $\mathrm{Ran}(\frac{3}{5n}, \frac{11}{5n})$ goes to zero since $\mathrm{Ran}(x_1, x_2)$ is continuous. But according to the ranking condition, the distance is always greater than ϵ. That is a contradiction. Thus, there are no continuous ranking functions for that program.

4. Correctness

To prove the correctness of `Termination`, we need some further results. For readers interested in *ergodic theory*, please refer to Mane (1987).

Usually, (a, b) $(\in \mathbb{T})$ can be denoted as $a + b\mathbf{i} = \mathrm{e}^{x\mathbf{i}}$. Thus, $\mathbb{T}^{m'}$ can be rewritten as $\mathbb{T}^{m'} = \{(\mathrm{e}^{x_1 2\pi \mathbf{i}}, \ldots, \mathrm{e}^{x_{m'} 2\pi \mathbf{i}}) | \, x_j \in \mathbb{R}\}$ and define $L_{\pi(\alpha)} : \mathbb{T}^{m'} \to \mathbb{T}^{m'}$ as

$$(\mathrm{e}^{y_1 2\pi \mathbf{i}}, \ldots, \mathrm{e}^{y_{m'} 2\pi \mathbf{i}}) \to (\mathrm{e}^{(y_1+\alpha_1)2\pi \mathbf{i}}, \ldots, \mathrm{e}^{(y_{m'}+\alpha_{m'})2\pi \mathbf{i}}),$$

where $\alpha = (\alpha_1, \ldots, \alpha_{m'}) \in \mathbb{R}^{m'}$.

Lemma 21 (Mane, 1987)**.** *If $\alpha \in \mathbb{R}^{m'}$, the translation $L_{\pi(\alpha)}(X)$ is ergodic if and only if for all $K \in \mathbb{Z}^{m'}$, $(K, \alpha) \notin \mathbb{Z}$, where (K, α) stands for the inner product of K and α.*

Definition 22. Irrational numbers $\alpha_1, \ldots, \alpha_{m'}$ are *rationally independent* if there do not exist rational numbers $\beta_1, \ldots, \beta_{m'}$ such that $\sum_{j=1}^{m'} a_j\beta_j \in \mathbb{Q}$.

Remark 23. It can be deduced that $\{\alpha_1, \ldots, \alpha_{m'}\}$ are rationally independent if and only if $\forall(b_1, \ldots, b_{m'}) \in \mathbb{Z}^{m'}, \sum_{j=1}^{m'} b_j\alpha_j \notin \mathbb{Z}$. According to Lemma 21, if $\{\alpha_1, \ldots, \alpha_{m'}\}$ are rationally independent, $L_{\pi(\alpha)}(X)$ is ergodic, and then the closure of $\{L^n_{\pi(\alpha)}(0)\}_{n\geq 1}$ is $\mathbb{T}^{m'}$, where $L^n_{\pi(\alpha)}$ is the composition of $L_{\pi(\alpha)}$ by n times and

$$\{L^n_{\pi(\alpha)}(0)\}_{n\geq 1} = \{(\mathrm{e}^{n\alpha_1 2\pi \mathbf{i}}, \ldots, \mathrm{e}^{n\alpha_{m'} 2\pi \mathbf{i}}) | n \geq 1\}.$$

Thus, if $\{\alpha_{k1}, \ldots, \alpha_{ks_k}\}$ are rationally independent, then for a fixed X

$$\inf_{n\geq 1} C'_{jkl2}(X, \sin(n\overline{\alpha_{k1}}), \cos(n\overline{\alpha_{k1}}), \ldots, \sin(n\overline{\alpha_{ks_k}}), \cos(n\overline{\alpha_{ks_k}})) = \min_{Y \in \mathbb{T}^{s_k}} C'_{jkl2}(X, Y),$$

where $\overline{\alpha_{ki}} = \alpha_{ki}2\pi$ for $i = 1, \ldots, s_k$.

Proposition 24. *Let* $\gamma_i = (Tn + t)\alpha_{ki}2\pi$ $(1 \le i \le s_k)$, *where* $\{\alpha_{k1}, \ldots, \alpha_{ks_k}\}$ *are rationally independent. Then*

$$\inf_{n\ge 1}\{C'_{jkl2}(X, \sin(\gamma_1), \cos(\gamma_1), \ldots, \sin(\gamma_{s_k}), \cos(\gamma_{s_k}))\} = \min\{C'_{jkl2}(X, Y)\}$$

subject to $Y \in \mathbb{T}^{s_k}$.

Proof. It is sufficient to prove that $\mathbb{T}^{s_k}$ is the closure of $\{(\mathrm{e}^{\gamma_1\mathbf{i}}, \ldots, \mathrm{e}^{\gamma_{s_k}\mathbf{i}})\}_{n\ge 1}$. Because $\{\alpha_{k1}, \ldots, \alpha_{ks_k}\}$ are rationally independent, $\{T\alpha_{k1}, \ldots, T\alpha_{ks_k}\}$ are rationally independent, too. According to Remark 23, $\mathbb{T}^{s_k}$ is the closure of $\{(\mathrm{e}^{nT\alpha_{k1}2\pi\mathbf{i}}, \ldots, \mathrm{e}^{nT\alpha_{ks_k}2\pi\mathbf{i}})\}_{n\ge 1}$. The result of rotating $(\mathrm{e}^{nT\alpha_{k1}2\pi\mathbf{i}}, \ldots, \mathrm{e}^{nT\alpha_{ks_k}2\pi\mathbf{i}})$ by $(t\alpha_{k1}2\pi, \ldots, t\alpha_{ks_k}2\pi)$ is $(\mathrm{e}^{\gamma_1\mathbf{i}}, \ldots, \mathrm{e}^{\gamma_{s_k}\mathbf{i}})$. Consequently, $\mathbb{T}^{s_k}$ is the closure of $\{(\mathrm{e}^{\gamma_1\mathbf{i}}, \ldots, \mathrm{e}^{\gamma_{s_k}\mathbf{i}})\}_{n\ge 1}$. That completes the proof. □

Remark 25. Since $\mathbb{T}^{s_k}$ is a bounded closed set, according to Proposition 24,

$$I = \inf_{n\ge 1}\{C_{jkl}(X, n)\} = \min_{Y\in\mathbb{T}^{s_k}}\{C_{jkl1}(X) + C'_{jkl2}(X, Y)\},$$

and if $I < 0$, there exists some $c < 0$ such that $C_{jkl}(X, n) < c$ for infinitely many n's.

If `Termination` finds one solution X_0, the leading coefficient of $G_j(X_0)$ $(j = 1, \ldots, L)$, say $C_{jkl}(X_0, n)$, satisfies $C_{jkl}(X_0, n) \succ 0$. According to Remark 15 there exist $c_j > 0$ such that $C_{jkl}(X_0, n) > c_j$ for all n. Thus LP_1 is nonterminating. This means that if the algorithm outputs “nonterminating", then LP_1 is nonterminating indeed.

On the other hand, if `Termination` outputs “terminating", then NZM must be satisfied. For any $\{C_{jk_jl_j}(X, n) | 1 \le j \le L\}$ there is a subset $V \subseteq \{1, \ldots, L\}$ such that $\forall j \in V$

$$C_{jk_jl_j}(X, n) \succ 0 \wedge \bigwedge_{n^{l_j} r^n_{k_j} < n^l r^n_k} C_{jkl}(X, n) \succeq 0$$

is not satisfiable subject to

$$\bigwedge_{j\notin V}\left(C_{jk_jl_j} \succ 0 \wedge \bigwedge_{n^{l_j} r^n_{k_j} < n^l r^n_k} C_{jkl}(X, n) \succeq 0\right). \tag{6}$$

If there is some j such that $\bigwedge_{n^{l_j} r^n_{k_j} < n^l r^n_k} C_{jkl}(X, n) \succeq 0$ does not hold, then there is some $C_{jkl}(X, n)$ such that $I = \inf_{n\ge 1} C_{jkl}(X, n) < 0$. Thus, according to Remark 25, there is some $c < 0$ such that $C_{jkl}(X, n) < c$ for infinitely many n's. Then $C_{jk_jl_j}(X, n)n^{l_j}r^n_{k_j}$ cannot be the dominant term, and our guess does not hold. Otherwise $C_{jk_jl_j}(X, n) \succ 0$ does not hold for any $j \in V$, and we get that for those X satisfying Eq. (6),

$$\forall j \in V, \quad I_j = \min_{Y\in\mathbb{T}^{s_{k_j}}} C_{jk_jl_j1}(X) + C'_{jk_jl_j2}(X, Y) \le 0.$$

According to NZM, $\forall j \in V$, $C_{jk_jl_j2}(X, n)$ is identically zero or $I_j < 0$. If the former holds, $C_{jk_jl_j}(X, n) \le 0$ for any n. If the latter holds, by Remark 25 there are infinitely many n's and some $c_j < 0$ such that $C_{jk_jl_j}(X, n) < c_j$ for $\forall j \in V$. Neither can make all the dominant terms identically positive. That means LP_1 is terminating. Therefore, we get the following theorem.

Theorem 26. *For those programs satisfying NZM,* `Termination` *returns “terminating" if and only if* LP_1 *is terminating. For those not,* LP_1 *is nonterminating if* `Termination` *return “nonterminating".*

5. Algorithm for termination of LQ_1 and LR_1 over $\mathbb{R}$

Let us first consider termination of LQ_1. The difference between LP_1 and LQ_1 is that the loop condition of LQ_1 is $P(X) \geq 0$ instead of $P(X) > 0$. It means that $G_j(X, n)$ need not have a positive leading term, and if so, all $C_{jkl}(X, n)$ in $G_j(X, n)$ should be “nonnegative". Hence, we need to add this into the algorithm `Termination`. Here is the modified algorithm for the termination of LQ_1 over $\mathbb{R}$.

Extended Algorithm 1 `TerminationM`$(A, P(X))$

```
Step 0 Compute the general expression of $A^{n+u}X$.
Step 1 Substitute $A^{n+u}X$ for $X$ in $P(X)$, and compute all $G_j(X, n)$ (finitely many, say, $j = 1, \ldots, L$).
Step 2 Guess no leading term or a leading term, say $C_{jk_jl_j} n^{l_j} r_{k_j}^n$, for each $G_j(X, n)$.
Step 3 If $G_j(X, n)$ is guessed to have a leading term,
           $S_j = C_{jk_jl_j} \succ 0 \wedge \bigwedge_{n^{l_j} r_{k_j}^n < n^l r_k^n} C_{jkl}(X, n) \succeq 0;$   otherwise $S_j = \bigwedge_{k,l} C_{jkl}(X, n) \succeq 0.$
       Construct a semi-algebraic system $S = \bigwedge_{j=1}^{L} S_j$.
Step 4 If one of these systems is satisfiable, return “nonterminating". Otherwise, if NZM is satisfied
       return “terminating"; otherwise return “uncertain".
```

With similar idea `Termination` can be extended to determine the termination of LR_1 over $\mathbb{R}$.

Extended Algorithm 2 `TerminationR`$(A, P(X), R(X))$

```
Step 0 Compute the general expression of $A^{n+u}X$.
Step 1 Substitute $A^{n+u}X$ for $X$ in $P(X)$, and compute all $G_j(X, n)$ (finitely many, say, $j = 1, \ldots, L$).
Step 2 Guess a leading term, say $C_{jk_jl_j} n^{l_j} r_{k_j}^n$, for each $G_j(X, n)$ from some $P_i(X) \in P(X)$; guess no leading
       term or a leading term, say $C_{jk_jl_j} n^{l_j} r_{k_j}^n$ too, for each $G_j(X, n)$ from some $R_i(X) \in R(X)$.
Step 3 If $G_j(X, n)$ is guessed to have a leading term,
           $S_j = C_{jk_jl_j} \succ 0 \wedge \bigwedge_{n^{l_j} r_{k_j}^n < n^l r_k^n} C_{jkl}(X, n) \succeq 0;$   otherwise $S_j = \bigwedge_{k,l} C_{jkl}(X, n) \succeq 0.$
       Construct a semi-algebraic system $S = \bigwedge_{j=1}^{L} S_j$.
Step 4 If one of these systems is satisfiable, return “nonterminating". Otherwise, if NZM is satisfied
       return “terminating"; otherwise return “uncertain".
```

Remark 27. The proofs of correctness of `TerminationM` and `TerminationR` are similar to the proof in Section 4. However, let us give a more intuitive one here.

If one of the systems is satisfiable, it means that for each $G_j(X, n)$ from some strict loop condition there is a positive leading term and for each $G_j(X, n)$ from some non-strict loop condition there is a positive leading term or all the terms are nonnegative. Hence, the loop must be “nonterminating".

Otherwise, if NZM is satisfied, our algorithm will output “terminating". Suppose there is indeed some X_0 such that the loop is nonterminating. Hence, $G_j(X_0, n)$ is greater than zero for each $n(\geq 0)$ if it comes from some strict loop condition; otherwise $G_j(X_0, n)$ is greater than or equal to zero for each $n(\geq 0)$. Now let us check the coefficient, say $C_{jk_jl_j}$, of its leading term for each non-zero $G_j(X_0, n)$. Since its minimum is non-zero according to the NZM, it must be greater than or less than zero. Since X_0 makes the loop nonterminating, the minimum of $C_{jk_jl_j}$ w.r.t Y (see Eq. (4)) must be positive. Now, let us construct a semi-algebraic system. If $G_j(X_0, n)$ is non-zero,

$$S_j = C_{jk_jl_j} \succ 0 \wedge \bigwedge_{n^{l_j} r_{k_j}^n < n^l r_k^n} C_{jkl}(X, n) \succeq 0,$$

where $C_{jk_jl_j}$ is the coefficient of its leading term. Otherwise,

$$S_j = \bigwedge_{k,l} C_{jkl}(X, n) \succeq 0.$$

Let $S = \bigwedge_{j=1}^{L} S_j$, and S must be satisfiable since X_0 is such a solution. However, according to our algorithm none of the possible semi-algebraic systems is satisfiable. This is a contradiction. Hence, there is no such X_0.

6. Proofs and algorithms

For the sake of self-containedness, this section presents the details of the proofs and the algorithms mentioned in the above sections.

6.1. *Proof of Proposition 9*

Before proving Proposition 9, let us introduce a useful lemma.

Lemma 28 (Stanley, 1997)**.** *Let $\alpha_1, \dots, \alpha_d$ be a sequence of complex numbers, $d \ge 1$ and $\alpha_d \ne 0$. The following conditions on a function $f : \mathbb{N} \to \mathbb{C}$ are equivalent to each other:*

i. *$\sum_{n\ge0} f(n)x^n = \frac{P(x)}{Q(x)}$, where $Q(x) = 1 + \alpha_1 x + \cdots + \alpha_d x^d$ and $P(x)$ is a polynomial in x of degree less than d.*
ii. *For all $n \ge 0$, $f(n+d) + \alpha_1 f(n+d-1) + \alpha_2 f(n+d-2) + \cdots + \alpha_d f(n) = 0$.*
iii *For all $n \ge 0$, $f(n) = \sum_{i=1}^{k} P_i(n)\gamma_i^n$, and $Q(x) = 1 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_d x^d = \prod_{i=1}^{k}(1-\gamma_i x)^{d_i}$, where the γ_i's are distinct, and $P_i(n)$ is a polynomial in n of degree less than d_i.*

Proof of Proposition 9. In what follows, the X in $F(X, n)$ will be regarded as constants. First,

$$A^d + \alpha_1 A^{d-1} + \cdots + \alpha_{d-u}A^u = 0,$$

because $D(x)$ is the characteristic polynomial of A. So, for any $n \ge 0$,

$$\begin{aligned} &F(X, n+d-u) + \alpha_1 F(X, n+d-(u+1)) + \cdots + \alpha_{d-u}F(X, n) \\ &\quad = A^{n+d}X + \alpha_1 A^{n+d-1}X + \cdots + \alpha_{d-u}A^{n+u}X \\ &\quad = (A^d + \alpha_1 A^{d-1} + \cdots + \alpha_{d-u}A^u)A^n X = 0. \end{aligned}$$

Thus, for each j,

$$F_j(X, n+d-u) + \alpha_1 F_j(X, n+d-(u+1)) + \cdots + \alpha_{d-u}F_j(X, n) = 0.$$

By Lemma 28, $F_j(X, n) = \sum_{i=1}^{k} f_{ji}(X, n)\xi_i^n$ and

$$Q(x) = 1 + \alpha_1 x + \cdots + \alpha_{d-u}x^{d-u} = \prod_{i=1}^{k}(1-\xi_i x)^{d_i},$$

where $f_{ji}(X, n)$ is a polynomial in n of degree less than d_i. It is obvious that $x = 0$ is not a solution of $Q(x)$ and $\sum_{i=1}^{k} d_i = d - u$. Because

$$\begin{aligned} D(x) = x^d Q\left(\frac{1}{x}\right) &= x^d + \alpha_1 x^{d-1} + \cdots + \alpha_{d-u}x^u \\ &= x^d \prod_{i=1}^{k}\left(1 - \frac{\xi_i}{x}\right)^{d_i} = x^u \prod_{i=1}^{k}(x-\xi_i)^{d_i}. \end{aligned}$$

The ξ_i's are all the distinct non-zero complex eigenvalues of A and d_i is the multiplicity of ξ_i. That completes the proof. □

6.2. Algorithm `ComputingCommonPeriod`

T is necessary for defining $G_j(X, n)$, where T is the common period of all the $e^{\alpha_q 2\pi \mathbf{i}}$'s with rational α_q that are contained in $P_s(X, n)$ $(1 \le s \le M)$. However, in order to compute T we need to solve the following problems:

1. Compute the minimal polynomial of η_k $(1 \le k \le m)$ over $\mathbb{Q}$ in Eq. (2) that is the product of some ξ_j's.
2. Given $\eta_q = r_q e^{\alpha_q 2\pi \mathbf{i}}$ and its minimal polynomial over $\mathbb{Q}$, check whether α_q is a rational number.
3. If α_q in the above is a rational number, compute the period of $e^{\alpha_q 2\pi \mathbf{i}}$ that is the minimal $t_q \in \mathbb{Z}_{>0}$ s.t. $e^{t_q \alpha_q 2\pi \mathbf{i}} = 1$.

Then, T is the least common multiple of the above t_q's. In fact, the first problem is solved by Strzebonski (1997), and in the following we shall solve the next two problems.

The minimal polynomial of an algebraic number α over $\mathbb{Q}$ is a monic polynomial, $M(x) \in \mathbb{Q}[x]$ with the least degree that satisfies $M(\alpha) = 0$, and the degree of $M(x)$ is defined as the degree of α. The jth cyclotomic polynomial over $\mathbb{Q}$ is the monic polynomial

$$CP_j(x) = \prod_{j=1}^{r} (x - \xi_j),$$

where $\xi_1, \dots, \xi_r$ are all the distinct primitive jth roots of unity in $\mathbb{Q}$. In fact for each j, $CP_j(x)$ can be computed in advance.

Suppose the minimal polynomial of α is $M(x)$ whose degree is d. Without loss of generality suppose $\alpha = re^{\beta 2\pi \mathbf{i}}$. Since the degree of α is d, the degree of $\overline{\alpha}$ must be d. Then the degree of $\alpha \cdot \overline{\alpha} = r^2$ is at most d^2. Thus the degree of r is at most $2d^2$. The degree of r^{-1} is at most $2d^2$ because the degree of r^{-1} is equal to the degree of r. Since the degree of α is d, the degree of $\alpha \cdot r^{-1} = e^{i\beta 2\pi}$ is at most $2d^3$.

If β is a rational number, $\alpha \cdot r^{-1}$ must be a root of unity and its minimal polynomial must be a cyclotomic polynomial. As a result, if β is a rational number, the minimal polynomial of $\alpha \cdot r^{-1}$ must be a cyclotomic polynomial whose degree is less than or equal to $2d^3$. Since the degree of the jth cyclotomic polynomial is $\phi(j)$, the Euler function, and $\phi(n) \ge \sqrt{n}$ for all n except $n = 2$ and 6, $j \le \max\{4d^6, 6\}$. We can bound α in a rectangle, W, by isolating all the complex roots of $M(x)$. Then, β is a rational number if and only if there is some $j(1 \le j \le \max\{4d^6, 6\})$ s.t.

$$\exists r \left((r \ne 0) \bigwedge (CP_j(x/r) = 0) \bigwedge (M(x) = 0) \bigwedge (x \in W) \right) \tag{7}$$

is satisfiable. Assume the minimal j that satisfies Eq. (7) is j', then the period of $e^{\beta 2\pi \mathbf{i}}$ is j'.

The formal description of the above idea is presented as follows.

Algorithm `FindingPeriod(W,`$M(x)$`)`
Input: W is a rectangle and contains only one complex root, say η, of $M(x)$, where $M(x)$ is a polynomial with rational coefficients.
Output: If the argument of η is a rational multiple of π, return the period of $\frac{\eta}{|\eta|}$; otherwise, return 0.

```
Step 1. $d \leftarrow degree(M(x))$;
Step 2. Compute $CP_j(x)$, $1 \le j \le \max\{4d^6, 6\}$, $l \leftarrow 1$;
Step 3. While($l \le \max\{4d^6, 6\}$) do
          If
              $\exists r \left( (r \ne 0) \bigwedge (CP_l(x/r) = 0) \bigwedge (M(x) = 0) \bigwedge (x \in W) \right)$     (8)
          is TRUE, return l;
          else $l \leftarrow l + 1$;
        End do
        Return 0;
End
```

The formal description of ComputingCommonPeriod is given as follows.

Algorithm ComputingCommonPeriod($W[H]$,$f_1(x), \ldots, f_H(x)$)
Input: $W[\,]$ is an array of rectangles, and $W[j]$ contains only one complex root, say η_j, of $f_j(x)(1 \le j \le H)$, where $f_j(x)$ is a polynomial with rational coefficients.
Output: If there exist some η_j's whose arguments are rational multiples of π, return their common period; otherwise return 0.

```
    for ($j$ from 1 to $H$) do
        $IP_j \leftarrow$ FindingPeriod($W[j], f_j(x)$);
    end do
    Return the least common multiple of $\{IP_1, \ldots, IP_H\}$.
End
```

6.3. *Algorithm* MaximumRationallyIndependentGroup

We are given a set of algebraic numbers, $\alpha_1 = \mathrm{e}^{\beta_1 2\pi\mathbf{i}}, \ldots, \alpha_d = \mathrm{e}^{\beta_d 2\pi\mathbf{i}}$, where all β_i are irrational numbers. In this subsection we present a method to compute a maximum rationally independent group of $\beta_1, \ldots, \beta_d$. In fact it is sufficient to devise an algorithm to check whether a given group of irrational numbers are rationally independent. That is because if they are rationally dependent, we can delete one at a time from $\{\beta_1, \ldots, \beta_d\}$ until the remaining ones are rationally independent, and the resulted group is a maximum rationally independent group. In the following, we shall present a method to check whether $\{\beta_1, \ldots, \beta_d\}$ are rationally independent. First, let us introduce a useful lemma which ensures correctness of our method.

Lemma 29 (*Baker, 1966*). *Let $\lambda_1, \ldots, \lambda_m$ with $m \ge 2$ be linearly dependent logarithms of algebraic numbers. Define $\alpha'_j = \mathrm{e}^{\lambda_j}$ $(1 \le j \le m)$. For $1 \le j \le m$, let $\log A_j \ge 1$ be an upper bound for $\max\{h(\alpha'_j), \frac{|\lambda_j|}{D}\}$ where D is the degree of the number field $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ over $\mathbb{Q}$ and $h(\alpha)$ denotes the absolute logarithmic height of α. Then there exist rational integers $n_1, \ldots, n_m$, not all of which are zero, such that $n_1\lambda_1 + \ldots + n_m\lambda_m = 0$ and $|n_k| < (11(m-1)D^3)^{m-1}\frac{(\log A_1)\ldots(\log A_m)}{\log A_k}$, $1 \le k \le m$.*

Remark 30. Baker is the first one to use transcendence arguments to establish such an estimate. However, the description here follows Lemma 7.19 in Waldschmidt (2000).

According to Definition 22, $\{\beta_1, \ldots, \beta_d\}$ are rationally dependent iff $\{\beta_1, \ldots, \beta_d, 1\}$ are linearly dependent in $\mathbb{Q}$. If $\{\beta_1, \ldots, \beta_d, 1\}$ are linearly dependent in $\mathbb{Q}$, according to Lemma 29 there exist integers $n_1, \ldots, n_{d+1}$, not all of which are zero, such that $n_1\beta_1 + \cdots + n_d\beta_d + n_{d+1} = 0$ and $|n_k| < (11dD^3)^d \frac{(\log A_1)\ldots(\log A_{d+1})}{\log A_k} (1 \le k \le d+1)$, where $D, A_1, \ldots, A_{d+1}$ are defined as in Lemma 29. Then $n_1\beta_1 2\pi\mathbf{i} + \cdots + n_{d+1}2\pi\mathbf{i} = 0$ and $\mathrm{e}^{n_1\beta_1 2\pi\mathbf{i}} \cdots \mathrm{e}^{n_d\beta_d 2\pi\mathbf{i}} = 1$. That is, $\alpha_1^{n_1} \cdots \alpha_d^{n_d} = 1$.

Thus, according to Lemma 29 we can decide whether $\{\beta_1, \ldots, \beta_d\}$ are rationally independent by enumerating n_k from

$$\left\lfloor -(11dD^3)^d \frac{(\log A_1)\cdots(\log A_{d+1})}{\log A_k} \right\rfloor$$

to

$$\left\lceil (11dD^3)^d \frac{(\log A_1)\cdots(\log A_{d+1})}{\log A_k} \right\rceil,$$

for $k = 1, \ldots, d$ and checking whether $\alpha_1^{n_1} \cdots \alpha_d^{n_d} = 1$. If there exists $\{n_1, \ldots, n_d\}$ such that $\alpha_1^{n_1} \cdots \alpha_d^{n_d} = 1$, then $\{\beta_1, \ldots, \beta_d\}$ are rationally dependent; otherwise they are rationally independent. For any given $(n_1, \ldots, n_d)$, whether $\alpha_1^{n_1} \cdots \alpha_d^{n_d} = 1$ can be determined by checking whether the following SAS has solutions.

$$\{x_1^{n_1} \cdots x_d^{n_d} = 1, q_j(x_j) = 0, x_j \in W_j, j = 1, \ldots, d\},$$

where q_j is the minimal polynomial of α_j and W_j contains only one complex root, α_j, of q_j for $j = 1, \ldots, d$.

The formal description of the above idea is presented as follows.

Algorithm `CheckingRationalInpendence`$(W[d], q_1(x_1), \ldots, q_d(x_d))$
Input: $W[\,]$ is an array of rectangles, and $W[j]$ contains only one complex root, say α_j, of $q_j(x_j)$, $1 \le j \le d$. $q_j(x_j)$ is a polynomial with rational coefficients.
Output: If $\{\beta_1, \ldots, \beta_d\}$ are rationally independent, return 1, where $\beta_j 2\pi$ is the argument of α_j, $1 \le j \le d$; otherwise return 0.

```
Step 1. $MB_1 \leftarrow \lfloor -(11dD^3)^d \frac{(\log A_1)\cdots(\log A_{d+1})}{\log A_k} \rfloor$;
        $MB_2 \leftarrow \lceil (11dD^3)^d \frac{(\log A_1)\cdots(\log A_{d+1})}{\log A_k} \rceil$;
Step 2. for ($i_1$ from $MB_1$ to $MB_2$) do
                    $\cdots$
            for ($i_d$ from $MB_1$ to $MB_2$) do
              If
                 $\{x_1^{n_1} \cdots x_d^{n_d} = 1,\ q_j(x_j) = 0,\ x_j \in W_j, j = 1, \ldots, d\}$
                 is satisfiable, return 0.
            end do
          $\cdots$
        end do
      Return 1.
End
```

The formal description of `MaximumRationallyIndependentGroup` is presented as follows.

Algorithm `MaximumRationallyIndependentGroup`$(W[d], q_1(x_1), \ldots, q_d(x_d))$
Input: The same as that of `CheckingRationalInpendence`.
Output: A maximum rationally independent group of $\{\beta_1, \ldots, \beta_d\}$, where β_j $(1 \le j \le d)$ is the same as in `CheckingRationalInpendence`.

```
Step 1. $ST \leftarrow W[d]$, $PT \leftarrow \{q_1(x_1), \ldots, q_d(x_d)\}$;
Step 2. while (CheckingRationalInpendence($ST$, $PT$) $= 0$[6]) do
            delete one element, say $W[j]$, from $ST$, and delete $q_j(x_j)$ from $PT$;
        end do
    Return those $\beta_j$'s contained in each $W[j] \in ST$.
End
```

Remark 31. Suppose that $G = \{\gamma_1, \ldots, \gamma_l\}$ is a maximum rationally independent group of $\{\beta_1, \ldots, \beta_d\}$. In the above method each β_i $(1 \le i \le d)$ not in G, can be represented by a linear function of G with rational coefficients. However, we hope that each β_i not in G, could be represented by a linear function of G with integer coefficients. In fact this can be easily done. In what follows, our main idea is illustrated with an example.

If β_1 and β_2 not in G, can be represented as follows

$$\beta_1 = \frac{\gamma_1}{2} + \frac{3\gamma_2}{8}, \qquad \beta_2 = \frac{2\gamma_1}{3} + \frac{3\gamma_2}{4},$$

then let $\gamma_1' = \frac{\gamma_1}{6}$, $\gamma_2' = \frac{\gamma_2}{8}$ and substitute γ_1' and γ_2' for γ_1 and γ_2 respectively in G. Thus,

$$\beta_1 = 3\gamma_1' + 3\gamma_2', \qquad \beta_2 = 4\gamma_1' + 6\gamma_2', \qquad \gamma_1 = 6\gamma_1', \qquad \gamma_2 = 8\gamma_2'$$

and all the elements in the resulted G are still rationally independent.

[6] This is a shorthand for invocation for `CheckingRationalInpendence`.

7. Conclusion and future works

In this paper we have proved that termination problems of LP_1, LQ_1 and LR_1 over $\mathbb{Z}$ are undecidable. Furthermore, if the entries of A in LP_1, LQ_1 and LR_1 are confined to integers, the termination problems of the resulted LP_1, LQ_1 and LR_1 over $\mathbb{Z}$ are still undecidable. Then we have given a relatively complete algorithm to determine whether LP_1 is terminating over $\mathbb{R}$. If LP_1 satisfies NZM, it is terminating if and only if our algorithm outputs "terminating". If not, it is nonterminating if our algorithm outputs "nonterminating". We have demonstrated the main steps of our algorithm by an example. Finally, we extend this algorithm to determine the termination of LQ_1 and LR_1 over $\mathbb{R}$. It is obvious that the complexity of our main algorithms is very high because we have used many quantifier eliminations (at most $2(MT)^N$ quantifier eliminations, where M is the number of loop conditions, T is the common period and N is the number of variables). Hence, our future work will focus on how to reduce the complexity of our algorithms.

However, it is not easy to deal with the case that NZM is not satisfied. Here we make the following conjecture.

Conjecture. *The termination problems of LP_1, LQ_1 and LR_1 over $\mathbb{R}$ are undecidable in general.*

Acknowledgements

The authors would like to thank Prof. Lu Yang for proposing the problem to us and encouraging us to work on it. We thank Prof. Michel Waldschmidt for his introduction to Baker's work. We are also grateful to Prof. Bob Caviness, Prof. Hoon Hong and Prof. Daniel Richardson for their insightful suggestions. Finally, we would like to thank Prof. Chaochen Zhou, Prof. Naijun Zhan and all the other members in our group for the discussion at our weekly seminar. Furthermore, we would like to thank the reviewers for their valuable comments and suggestions.

References

Baker, A., 1966. Linear forms in the logarithms of algebraic numbers I, II, III, IV. Mathematika 13, 204–216;
Baker, A., 1967. Linear forms in the logarithms of algebraic numbers I, II, III, IV. Mathematika 14, 102–107. 220–228;
Baker, A., 1968. Linear forms in the logarithms of algebraic numbers I, II, III, IV. Mathematika 15, 204–216.

Blondel, V.D., Bournez, O., Koiran, P., Papadimitriou, C.H., Tsitsiklis, J.N., 2001. Deciding stability and mortality of piecewise affine dynamical systems. Theoretical Computer Science 255 (1–2), 687–696.

Bradley, A.R., Manna, Z., Sipma, H.B., 2005. Termination of polynomial programs. In: Proc. Verification, Model-Checking, and Abstract-Interpretation (VMCAI), January 2005. In: LNCS, vol. 3385. pp. 113–129.

Braverman, M., 2006. Termination of integer linear programs. In: CAV, 2006. In: LNCS, vol. 4114. pp. 372–385.

Chen, Y., Xia, B., Yang, L., Zhan, N., Zhou, C., 2007. Discovering Non-linear ranking functions by Solving Semi-algebraic Systems. In: LNCS, vol. 4711. pp. 34–49.

Collins, G.E., 1975. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In: Brakhage, H. (Ed.), Automata Theory and Formal Languages. In: LNCS, vol. 33. Springer, Berlin, Heidelberg, pp. 134–165.

Collins, G.E., Hong, H., 1991. Partial cylindrical algebraic decomposition for quantifier elimination. Journal of Symbolic Computation 12 (3), 299–328.

Colon, M., Sipma, H.B., 2001. Synthesis of linear ranking functions. In: TACAS01. In: LNCS, vol. 2031. pp. 67–81.

Dams, D., Gerth, R., Grumberg, O., 2000. A heuristic for the automatic generation of ranking functions. In: Workshop on Advances in Verification, WAVe00, pp. 1–8.

Dolzman, A., Sturm, T., 1997. REDLOG: Computer algebra meets computer logic. ACM SIGSAM Bulletin 31 (2), 2–9.

Lee, C.S., Jones, N.D., Ben-Amram, A.M., 2001. The size-change principle for program termination. In: POPL2001: Principles of Programming Languages, ACM SIGPLAN Notices, 36(3). ACM Press, pp. 81–92.

Mane, R., 1987. Ergodic Theory and Differentiable Dynamics. Springer-Verlag, New York.

Podelski, A., Rybalchenko, A., 2004. A complete method for the synthesis of linear ranking functions. In: VMCAI. In: LNCS, vol. 2937. pp. 465–486.

Stanley, R., 1997. Enumerative Combinatorics, vol. 1. Cambridge University Press.

Strzebonski, A.W., 1997. Computing in the field of complex algebraic numbers. J. Symbolic Computation 24 (6), 647–656.

Tarski, A., 1951. A Decision Method for Elementary Algebra and Geometry, 2nd edn.. University of California Press, Berkeley.

Tiwari, A., 2004. Termination of Linear Programs. In: Alur, R., Peled, D.A. (Eds.), CAV. In: LNCS, vol. 3114. pp. 70–82.

Waldschimidt, M., 2000. Diophantine Approximation on Linear Algebraic Groups. Springer-Verlag, Berlin.

Xia, B., 2007. DISCOVERER: A tool for solving semi-algebraic systems. In: Software Demo at ISSAC 2007, Waterloo, July 30, 2007. ACM SIGSAM Bulletin 41 (3), 102–103.

Xia, B., Yang, L., Zhan, N., Zhang, Z., 2009. Symbolic decision procedure for termination of linear programs. Formal Aspects of Computing (doi:10.1007/s00165-009-0144-5), available online since December 17, 2009.