Termination of Initialized Rational Linear Programs

B. Tech. Project Stage II Report

Submitted in partial fulfillment of the requirements
for the degree of

Bachelor of Technology

by

Rohit Singh
Roll No: 07005034

under the guidance of

Prof. Supratik Chakraborty

Department of Computer Science and Engineering
Indian Institute of Technology, Bombay
Mumbai

Contents

Abstract

Tiwari showed in 2004 that the problem of determining if a linear loop program with real-valued variables terminates over all inputs is decidable. Braverman showed in 2006 that the problem remains decidable even when all variables are restricted to take integer values. We consider the problem of determining if a linear loop program over rationals terminates when started with a given initialization vector. Our contributions can be summarized as follows.

1. We show that an order-reduction technique can be formulated to simplify the problem, and ensure that all eigenvalues (including the dominant one) of the reduced linear transformation have non-zero contributions to the loop condition. A corollary of this order-reduction is the equivalence of our problem and that of deciding positivity of linear homogenous recurrences. We show that an adaptation of the technique used in [9] to decide termination of linear loops with polynomial condition on all inputs can be used to decide a subclass of our order reduced problem.

2. We present a characterization of the above subclass for which our technique is complete. We describe a hard instance of the problem outside this subclass with the smallest reduced order (four). Deciding termination in this case corresponds to the as-yet open problem of deciding the positivity of a linear homogenous recurrence of order four.

1 Introduction

We consider the problem of determining if a linear loop program over rationals terminates when started with a given initialization vector. The general structure of the program being the following (Program `P0`):

$$\texttt{P0:} \quad \boldsymbol{x} = \boldsymbol{b};\ \texttt{while}\ (B\boldsymbol{x} > \boldsymbol{e})\ \boldsymbol{x} = A\boldsymbol{x} + \boldsymbol{d}$$

where A and B are $n \times n$ and $m \times n$ rational matrices respectively, $\boldsymbol{e}$ is a m-dimensional and, $\boldsymbol{b}$ and $\boldsymbol{d}$ are n-dimensional column vectors with rational entries. We will also call this problem single input initialized linear loop termination problem.

Tiwari ([1]) and Braverman ([5]) considered the termination problem for linear loops under all inputs when the variables are restricted to be reals and integers respectively. This was motivated from the applicability of such problems in analysis of safety critical systems. Their methods would reject a program even if it does not terminate on a single input. To evaluate the programs with a better precision, it is important to characterize the points on which it will terminate. In this regard, decidability of termination on a particular input will enable us to characterize some finite safety sets of points on which a particular program of the form `P0` will certainly terminate. Their work has been recently extended to include polynomial loop condition in [9] and multiple choices of linear transformations based on linear conditionals in [11]. Both the extensions are incomplete and require some special structure on the input program to ensure decidability.

The single input initialized termination problem looks similar to the *Orbit problem* ([2]) where one needs to decide equality of a particular vector $\boldsymbol{y}$ with any of the future values of the variable $\boldsymbol{x}$ in the program (Orbit of the vector $\boldsymbol{b}$ with respect to the matrix A). In our termination problem we want to find if at some iteration value of $\boldsymbol{x}$ belongs to a convex class ($B\boldsymbol{x} < 0$) or not. Some insights from the *Orbit problem* and its extension, the *ABC problem* ([3]) have been used to develop our solution to this problem. Nevertheless, the problems are quite significantly different.

We describe an order reduction technique and give the reduction of the single input initialized termination problem to deciding positivity of linear recurrences. Positivity for second and third order homogenous recurrences have recently been shown decidable in 2006([8]) and 2009([7]) respectively. Our method is complete for deciding termination for all third order linear recurrences and also for fourth order linear recurrences except a class of programs which can be characterized by a necessary structure for the characteristic polynomial of the reduced matrix A.

Reduction to the homogenous problem over integers. We will reduce the termination of program `P0` to a homogenous problem over integers which we shall consider subsequently. Similar to the reduction in [1], we can formulate a homogenous program `P1` with a new scalar variable z which terminates iff `P0` terminates.

$$\texttt{P1:} \quad \boldsymbol{x} = \boldsymbol{b}; z = 1;\ \texttt{while}\ (B\boldsymbol{x} - \boldsymbol{e}z > 0)\ \{\boldsymbol{x} = A\boldsymbol{x} + \boldsymbol{d}z;\ z = z\}$$

Hence, we need to consider only homogenous linear programs as given by the structure `P2`.

$$\texttt{P2:} \quad \boldsymbol{x} = \boldsymbol{b};\ \texttt{while}\ (B\boldsymbol{x} > \boldsymbol{0})\ \boldsymbol{x} = A\boldsymbol{x}$$

Also, the loop termination condition $B\boldsymbol{x} > \boldsymbol{0}$ can be broken as a conjunction of inequalities of the form $\boldsymbol{c}^T\boldsymbol{x}$ where $\boldsymbol{c}^T$'s are the row vectors of the matrix B. We need to consider the individual problems for each row $\boldsymbol{c}^T$ of the form P3 since all these problems will be non-terminating iff P2 is non-terminating.

$$\texttt{P3:} \quad \boldsymbol{x} = \boldsymbol{b};\ \texttt{while}\ (\boldsymbol{c}^T\boldsymbol{x} > 0)\ \boldsymbol{x} = A\boldsymbol{x}$$

We can restate the problem as checking the validity of the following formula:

$$\exists\ k, k \in \mathbb{N} \cup \{0\}\ \wedge\ \boldsymbol{c}^T A^k \boldsymbol{b} \leq 0$$

If $l > 0$ is the LCM of all denominators of rational entries in $\boldsymbol{b}$, A and $\boldsymbol{c}$, then its easy to see that $\boldsymbol{c}^T A^k \boldsymbol{b} \leq 0$ iff $(l\boldsymbol{c})^T(lA)^k(l\boldsymbol{b}) \leq 0$, where $l\boldsymbol{b}$, lA and $l\boldsymbol{c}$ have integer entries. Hence, we need to consider programs of the form P3 with $\boldsymbol{b}$, A and $\boldsymbol{c}$ having integer entries for deciding termination for a general program of the form P0. Also, Note that we can restate problem P3 over integers as the following program:

$$\texttt{P3:} \quad \boldsymbol{x} = \boldsymbol{b};\ \texttt{while}\ (\boldsymbol{c}^T\boldsymbol{x} \geq 1)\ \boldsymbol{x} = A\boldsymbol{x}$$

Using transformation similar to program P1 we can restructure the program as follows:

$$\texttt{P4:} \quad \boldsymbol{x} = \boldsymbol{b}; z = 1;\ \texttt{while}\ (\boldsymbol{c}^T\boldsymbol{x} - z \geq 0)\ \boldsymbol{x} = A\boldsymbol{x}; z = z;$$

which allows us to consider only the programs of form

$$\texttt{P5:} \quad \boldsymbol{x} = \boldsymbol{b};\ \texttt{while}\ (\boldsymbol{c}^T\boldsymbol{x} \geq 0)\ \boldsymbol{x} = A\boldsymbol{x}$$

with $\boldsymbol{b}, \boldsymbol{c}$ and A having integer entries. The corresponding formula to be checked for satisfiability being $\exists\ k, k \in \mathbb{N} \cup \{0\}\ \wedge\ \boldsymbol{c}^T A^k \boldsymbol{b} < 0$

2 Order reduction of the problem

We present an order reduction method which can be used to ease the algebraic computation by reducing the problem to an instance with a special structure and only necessary eigenvalues. Some potential benefits and their applications are summarized below:

- Order reduction ensures that every eigenvalue has a non-zero contribution in the order reduced problem (base problem)
- Every eigenvalue has a unique Jordan block in the JNF decomposition. Hence, the largest modulus eigenvalue of the base problem matrix is also the dominant eigenvalue in the loop condition.
- The minimal polynomial of the base problem matrix is the same as its characteristic polynomial and the matrix is also invertible.
- Starting from a problem with a large order, if the reduced problem has order less than or equal to 3 or when there is exactly one (real) largest modulus eigenvalue for the base problem matrix, we can ensure that we can decide termination easily by looking at only the coefficient of the dominant eigenvalue in the loop condition.

In the following two cases, we observe that order reduction helps us bypass the computation intensive step of computing the Jordan Normal Form and the infimum of the leading coefficient. Computing the infimum involves polynomials with arbitrarily large degrees as the multiples of the angles from the rationally independent set of irrational angles can be arbitrarily large.

Input: $(n, \boldsymbol{b}, \boldsymbol{c}, A)$
  reduce$(n, \boldsymbol{b}, \boldsymbol{c}, A)$ //one reduce called by default
  done $\leftarrow$ **false**
  while !*done* **do**
    $p \leftarrow$ min-poly$(A,\boldsymbol{b})$ //minimal polynomial of matrix A w.r.t $\boldsymbol{b}$
    $q \leftarrow$ min-poly$(A^T,\boldsymbol{c})$ //minimal polynomial of matrix A^T w.r.t $\boldsymbol{c}$
    if $deg(p) < n$ **then**
      reduce$(n, \boldsymbol{b}, \boldsymbol{c}, A)$
    else if $deg(q) < n$ **then**
      reduce$(n, \boldsymbol{c}, \boldsymbol{b}, A^T)$
    else if $p(0) = 0$ **then**
      reduce$(n, A\boldsymbol{b}, \boldsymbol{c}, A)$ //degree of p can be reduced by an iteration shift
    else if $q(0) = 0$ **then**
      reduce$(n, A^T\boldsymbol{c}, \boldsymbol{b}, A^T)$ //degree of q can be reduced by an iteration shift
    else
      done $\leftarrow$ **true**
    end if
  end while
Output: $(n, \boldsymbol{b}, \boldsymbol{c}, A)$

Figure 1: *Order Reduction*

- We can apply an interesting result due to Braverman (Lemma 4 in [5] which we will subsequently call Braverman's theorem for ease of notation) to decide termination in the case when there is no real largest modulus eigenvalue of the base problem.
- Also, if all terms of the base problem matrix turn out to be non-negative, then the program will terminate iff it terminates for the first n steps where n is the order of the base problem.

We denote the decision problem for termination of the program `P3` by $\pi(n, \boldsymbol{b}, \boldsymbol{c}, A)$ where n is a natural number, $\boldsymbol{b}$ and $\boldsymbol{c}$ are n-dimensional integer (column) vectors, and A is an $n \times n$ integer matrix. Before proceeding further, we recall some results from basic linear algebra which can be found in [12].

Lemma 2.1. *For any matrix $A \in \mathbb{Z}^{n\times n}$ and n-dimensional vector $\boldsymbol{b} \in \mathbb{Z}^n$:*

- *The minimal polynomial of vector $\boldsymbol{b}$ with respect to matrix A is defined as the monic polynomial $p_{\boldsymbol{b},A}(x)$ which satisfies $p_{\boldsymbol{b},A}(A).b = \mathbf{0}$ and has the least possible degree. The minimal polynomial $m_A(x)$ of the matrix A is defined the monic polynomial which satisfies $m_A(A) = 0$ and has the least possible degree.*
- *$p_{\boldsymbol{b},A} | m_A | c_A$ where $|$ denotes polynomial divisibility relation and c_A is the characteristic polynomial of A.*
- *$m_A = c_A$ iff every eigenvalue has a unique Jordan block in Jordan Normal Form(JNF) decomposition of matrix A with size equal to its algebraic multiplicity as a root of the polynomial $c_A(t) = det(tI - A)$.*

Although we are working in a full-fledged n-dimensional vector space, all the vectors that we are going to consider are constrained in a possibly smaller vector space comprising of linearly independent vectors $\{\boldsymbol{b}, A\boldsymbol{b}, A^2\boldsymbol{b}, ..., A^{m-1}\boldsymbol{b}\}$ where m is the degree of minimal polynomial of the vector $\boldsymbol{b}$ with respect to the matrix A. We can change our basis to these vectors thereby reducing the order(n) of the problem. A similar approach with the vector $\boldsymbol{c}$ can be used to further reduce the order of the problem, if possible.

Theorem 2.2. *Given a problem instance $\pi(n, \boldsymbol{b}, \boldsymbol{c}, A)$ and the minimal polynomial of $\boldsymbol{b}$ w.r.t A $p_{\boldsymbol{b},A}(x) = x^m - \sum_{i=0}^{m-1} \alpha_i x^i$, if $m = deg(p_{\boldsymbol{b},A}) \leq n$ then $\pi(n, \boldsymbol{b}, \boldsymbol{c}, A)$ is non-terminating iff it doesn't terminate for first m steps and another problem $\pi(m, \boldsymbol{b}', \boldsymbol{c}', A')$ is also non-terminating, where $\boldsymbol{b}'$ and $\boldsymbol{c}'$ are m-dimensional integer vectors, and A' is an $m \times m$ integer matrix given by:*

$$\boldsymbol{b}' = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} \quad \boldsymbol{c}' = \begin{pmatrix} \boldsymbol{c}^T A^{m-1}\boldsymbol{b} \\ \boldsymbol{c}^T A^{m-2}\boldsymbol{b} \\ \vdots \\ \boldsymbol{c}^T A\boldsymbol{b} \\ \boldsymbol{c}^T\boldsymbol{b} \end{pmatrix} \quad A' = \begin{pmatrix} \alpha_{m-1} & 1 & 0 & \cdots & 0 & 0 \\ \alpha_{m-2} & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1 & 0 & 0 & \cdots & 0 & 1 \\ \alpha_0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

Proof. We reduce the problem $\pi(n, \boldsymbol{b}, \boldsymbol{c}, A)$ to $\pi(m, \boldsymbol{b}', \boldsymbol{c}', A')$ as follows:

If any component of the vector $\boldsymbol{c}'$ is negative or zero then the loop must terminate in atmost m steps. In case $\boldsymbol{c}' > 0$, we define an $n \times m$ matrix $B_k := \left[A^k\boldsymbol{b}; A^{k-1}\boldsymbol{b}; ...; A^{k-m+1}\boldsymbol{b}\right]$.

$p_{\boldsymbol{b},A}(A)\boldsymbol{b} = 0 \implies A^m\boldsymbol{b} = \sum_{i=0}^{m-1} \alpha_i A^i\boldsymbol{b} \implies A^k\boldsymbol{b} = \sum_{i=0}^{m-1} \alpha_i A^{k-m+i}\boldsymbol{b} \implies B_k = B_{k-1}A'$ for all $k \geq m \implies B_k = B_{m-1}(A')^{k-m+1}$ for all $k \geq m$.

Also, $\boldsymbol{c}^T A^k\boldsymbol{b} = c^T(B_k(1, 0, ..., 0)^T) = \boldsymbol{c}^T B_{m-1}(A')^{k-m+1}\boldsymbol{b}' = (\boldsymbol{c}')^T(A')^{k-m+1}\boldsymbol{b}'$ for all $k \geq m$. Hence, $\exists\ k \in \mathbb{N} \cup \{0\} \wedge \boldsymbol{c}^T A^k\boldsymbol{b} \leq 0$

$\iff (\exists\ k \in \{0, 1, ..., m-1\} \wedge \boldsymbol{c}^T A^k\boldsymbol{b} \leq 0) \vee (\exists\ k \in \mathbb{N} \cup \{0\} \wedge (\boldsymbol{c}')^T(A')^k\boldsymbol{b}' \leq 0)$

The first expression can be evaluated by checking the values of $\boldsymbol{c}^T x$ in first m iterations. The second expression matches exactly with the decision problem $\pi(m, \boldsymbol{b}', \boldsymbol{c}', A')$. □

Theorem 2.2 provides a one step reduction procedure for decision problem $\pi(n, \boldsymbol{b}, \boldsymbol{c}, A)$: reduce($n, \boldsymbol{b}, \boldsymbol{c}, A$) which performs the assignment $(n, \boldsymbol{b}, \boldsymbol{c}, A) \leftarrow (m, \boldsymbol{b}', \boldsymbol{c}', A')$ in terms of the notation used in Theorem 2.2. Note that for $m = n$ the procedure just tranforms the matrix into its rational normal form. Since, $\boldsymbol{c}^T A^k\boldsymbol{b} = (\boldsymbol{c}^T A^k\boldsymbol{b})^T = \boldsymbol{b}^T(A^T)^k\boldsymbol{c}$, we observe that $\pi(n, \boldsymbol{b}, \boldsymbol{c}, A)$ is equivalent to $\pi(n, \boldsymbol{c}, \boldsymbol{b}, A^T)$. Hence, we can again apply the reduction mentioned in Theorem 2.2 to the equivalent transpose problem by considering the minimal polynomial of $\boldsymbol{c}$ with respect to A^T. We can also consider the first iteration separately followed by the problem $\pi(n, A\boldsymbol{b}, \boldsymbol{c}, A)$. In the case when constant term of polynomial $p_{\boldsymbol{b},A}$ is zero, this reduction to $\pi(n, A\boldsymbol{b}, \boldsymbol{c}, A)$ will ensure that degree of $p_{A\boldsymbol{b},A}$ is less than n and we can apply the previously mentioned reductions. The complete order reduction method is shown in Figure 1. In the final reduced problem $\pi(n, \boldsymbol{b}, \boldsymbol{c}, A)$ both minimal polynomials $p_{\boldsymbol{b},A}$ and $p_{\boldsymbol{c},A^T}$ have degree n and non-zero constant terms.

Example. Consider the problem $\pi(n, \boldsymbol{b}, \boldsymbol{c}, A)$ with $n = 5$

$$\boldsymbol{b} = \begin{pmatrix} -8 \\ 3 \\ 1 \\ -8 \\ -11 \end{pmatrix} \quad \boldsymbol{c} = \begin{pmatrix} 3 \\ 8 \\ 1 \\ -3 \\ 2 \end{pmatrix} \quad A = \begin{pmatrix} -14 & -40 & -8 & 0 & 0 \\ 6 & 17 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ -15 & -40 & 0 & -40 & 30 \\ -21 & -56 & 0 & -56 & 42 \end{pmatrix}$$

Here, A is singular and $\boldsymbol{c}^T\boldsymbol{b} > 0$. Hence, we reduce the problem to $\pi\left(5, \boldsymbol{b}_1, \boldsymbol{c}, A\right)$ where $\boldsymbol{b}_1 = A\boldsymbol{b} = (-16, 6, 1, -10, -14)^T$ and observe that $A^3\boldsymbol{b}_1 = 4A^2\boldsymbol{b}_1 - 5A\boldsymbol{b}_1 + 2\boldsymbol{b}_1$ (corresponding to the minimal polynomial of $\boldsymbol{b}$ with respect to matrix A). Using Theorem 2.2, we reduce the problem to $\pi\left(3, \boldsymbol{b}_2, \boldsymbol{c}_2, A_2\right)$ where $\boldsymbol{b}_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ $\boldsymbol{c}_2 = \begin{pmatrix} 17 \\ 9 \\ 5 \end{pmatrix}$ $A_2 = \begin{pmatrix} 4 & 1 & 0 \\ -5 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}$. This problem is equivalent to its transpose problem $\pi\left(3, \boldsymbol{c}_2, \boldsymbol{b}_2, A_2^T\right)$. We observe that $(A_2^T)^2\boldsymbol{c}_2 = A_2^T\boldsymbol{c}_2 - 2\boldsymbol{c}_2$ which reduces the problem to $\pi\left(2, \boldsymbol{b}_3, \boldsymbol{c}_3, A_3\right)$ where $\boldsymbol{b}_3 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $\boldsymbol{c}_3 = \begin{pmatrix} 33 \\ 17 \end{pmatrix}$ $A_3 = \begin{pmatrix} 3 & 1 \\ -2 & 0 \end{pmatrix}$. Now, this base problem of order 2 can be solved by observing that the matrix A_3 has two eigenvalues 2 and 1 and hence can be diagonalized to $diag(2, 1)$, leading to equivalence of this problem (as explained in the next subsection) to checking if $16 \times 2^k + 1 \leq 0$ for some integer $k \geq 0$ or not, which cannot be the case since all coefficients on the LHS are positive.

2.1 Using the Jordan Normal Form

Similar to the techniques used in [1], we will use the Jordan Normal Form of the matrix A to find an expression for the loop inequality. For an invertible matrix P the termination of $\mathcal{P}0$ is equivalent to:

$$\exists\ k, k \in \mathbb{N} \cup \{0\}\ \wedge\ (\boldsymbol{c}^T P^{-1})(PAP^{-1})^k(P\boldsymbol{b}) \leq 0$$

We choose P to be a matrix over $\mathbb{C}$ such that PAP^{-1} is in Jordan Normal Form.

$$PAP^{-1} = \begin{pmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \cdots & 0 \\ & & \cdots & \\ 0 & 0 & \cdots & J_l \end{pmatrix} \qquad J_i = \begin{pmatrix} \lambda_i & 1 & 0 & \cdots & 0 \\ 0 & \lambda_i & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_i \end{pmatrix}$$

Now, the termination of `P3` is equivalent to:

$$\exists\ k, k \in \mathbb{N} \cup \{0\} \wedge \sum_{i=1}^{l} \boldsymbol{f}_i J_i^k \boldsymbol{e}_i \leq 0 \tag{1}$$

where $\boldsymbol{f}_i, \boldsymbol{e}_i$ are row and cloumn vectors from $\boldsymbol{c}^T P^{-1}$ and $P\boldsymbol{b}$ respectively, corresponding to i^{th} block i.e. $P\boldsymbol{b} = (e_{11}, ..., e_{1m_1}, e_{21}, ..., e_{2m_2}, ..., e_{l1}, ..., e_{lm_l})^T$ and $\boldsymbol{c}^T P^{-1} = (f_{1m_1}, ..., f_{11}, f_{2m_2}, ..., f_{21}, ..., f_{lm_l}, \cdots$

For a Jordan block J of size $m \times m$ (corresponding to eigenvalue λ) and $k > m$, we have:

$$J^k = \begin{pmatrix} \binom{k}{0}\lambda^k & \binom{k}{1}\lambda^{k-1} & \binom{k}{2}\lambda^{k-2} & \cdots & \binom{k}{m-1}\lambda^{k-m+1} \\ 0 & \binom{k}{0}\lambda^k & \binom{k}{1}\lambda^{k-1} & \cdots & \binom{k}{m-2}\lambda^{k-m+2} \\ 0 & 0 & \binom{k}{0}\lambda^k & \cdots & \binom{k}{m-3}\lambda^{k-m+3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & \binom{k}{1}\lambda^{k-1} \\ 0 & 0 & 0 & \cdots & \binom{k}{0}\lambda^k \end{pmatrix}$$

Therefore,

$$\boldsymbol{f}_j J_j^k \boldsymbol{e}_j = \lambda_j^k R_j(k) = \lambda_j^k (P_j(k) + iQ_j(k)) \tag{2}$$

where $R_j(k)$ is a polynomial in k over $\mathbb{C}$ and, $P_j(k)$ and $Q_j(k)$ are polynomials in k over $\mathbb{R}$. Note that degree of all these polynomials is bounded by m_j (size of the j^{th} Jordan block). We

denote the argument of λ_j by θ_j i.e. $\lambda_j = |\lambda_j| e^{i\theta_j}$.
Now, $\mathrm{Re}(\boldsymbol{f}_j J_j^k \boldsymbol{e}_j) = |\lambda_j|^k (P_j(k)\cos k\theta_j - Q_j(k)\sin k\theta_j)$
$\implies \mathcal{LHS}$ of (1) $= \sum_{j=1}^{l} |\lambda_j|^k (P_j(k)\cos k\theta_j - Q_j(k)\sin k\theta_j)$
Define $I_\lambda = \{j : |\lambda_j| = \lambda\}$, $m_\lambda = \max_{j\in I_\lambda} \deg(R_j(k))$ and $L = \{\lambda : I_\lambda \neq \phi\}$.
$\implies \mathcal{LHS}$ of (1) $= \sum_{\lambda\in L}\sum_{r=1}^{m_\lambda}\sum_{j\in I_\lambda} \lambda^k k^r (a_{j,r}\cos k\theta_j + b_{j,r}\sin k\theta_j)$
$= \sum_{\lambda\in L}\sum_{r=1}^{m_\lambda} \lambda^k k^r E_{\lambda,r}(k)$ where $E_{\lambda,r}(k) = \sum_{j\in I_\lambda}(a_{j,r}\cos k\theta_j + b_{j,r}\sin k\theta_j)$

Example. Consider the following instance of the Order-reduced problem with

$$b = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad c = \begin{pmatrix} 2654 \\ 9674 \\ 1966 \\ 134 \end{pmatrix} \quad A = \begin{pmatrix} 14 & 1 & 0 & 0 \\ -121 & 0 & 1 & 0 \\ 776 & 0 & 0 & 1 \\ -1536 & 0 & 0 & 0 \end{pmatrix}$$

To write the loop inequality we use the JNF of the matrix A. Note that, $c_A(x) = (x^2 - 3x + 64)(x-8)(x-3)$. Hence, JNF of A is a diagonal matrix with eigenvalues $8, 8\alpha, 8\bar{\alpha}$ and 3 where $\alpha,\ \bar{\alpha}$ are roots of $\alpha^2 = \frac{3}{8}\alpha + 1$ with $Im(\alpha) > 0$ i.e. $\alpha = e^{i\theta}$ for some $\theta \in (0, \frac{\pi}{2})$ satisfying $\cos\theta = \frac{3}{16}$. We compute the eigenvectors symbolically in the algebraic extension $\mathbb{Q}[\alpha]$ and form the matrix P^{-1} with these vectors as its columns. Also, we just need the first column of the matrix P which we solve symbolically in $\mathbb{Q}[\alpha]$ using the linear equations corresponding to the first column of P obtained from $P^{-1}P = I$. (Note that $8\bar{\alpha} = 3 - 8\alpha$ also belongs to $\mathbb{Q}[\alpha]$)

$$P^{-1} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -6 & -14+8\alpha & -14+8\bar{\alpha} & -11 \\ 73 & 57-88\alpha & 57-88\bar{\alpha} & 88 \\ -192 & -72+192\alpha & -72+192\bar{\alpha} & -512 \end{pmatrix} \quad PAP^{-1} = J = \begin{pmatrix} 8 & 0 & 0 & 0 \\ 0 & 8\alpha & 0 & 0 \\ 0 & 0 & 8\bar{\alpha} & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

$$c^T P^{-1} = \begin{pmatrix} 62400 \\ -416(73+168\alpha) \\ -416(73+168\bar{\alpha}) \\ 640 \end{pmatrix} \quad Pb = \begin{pmatrix} 64/65 \\ (632+88\alpha)/(104(-3+16\alpha)) \\ (632+88\bar{\alpha})/(104(-3+16\bar{\alpha})) \\ -27/320 \end{pmatrix}$$

There are only two moduli of the eigenvalues ($L = \{3, 8\}$). For this instance, $\mathcal{LHS}$ of (1) $= c^T P^{-1} J^k P b = 15(8^{k+4}) + (-32000 + 14048\alpha)(8\alpha)^k + (-32000 + 14048\bar{\alpha})(8\bar{\alpha})^k - 54(3^k) = 15(8^{k+4}) + (8-64\alpha)(8\alpha)^{k+3} + (8-64\bar{\alpha})(8\bar{\alpha})^{k+3} - 2(3^{k+3}) = 8^{k+4}\left(15 + 2\cos{(k+3)\theta} + \sqrt{247}\sin{(k+3)\theta}\right) - 2(3^{k+3})$. Clearly, the infimum of the dominant coefficient $E_{8,0} = 15 + 2\cos{(k+3)\theta} + \sqrt{247}\sin{(k+3)\theta}$ is $15 - \sqrt{2^2 + 247} < 0$ (here $k' = k+3$ is the index corresponding to the original loop iteration). Hence, the loop will definitely terminate. On running the program, we observed that it terminates in the 8^{th} iteration.

2.2 Properties of the Order reduction

We consider some properties of the final order-reduced problem $\pi(n, b, c, A)$, which are of important consequences towards finding a solution to the decision problem. The nature of reduction process enforces $b = e_1 = (1, 0, ..., 0)^T$ and $c > 0$. Since the minimal polynomial of b and c with respect to A have degree n, hence, we must have, $p_{b,A} \equiv p_{c,A} \equiv m_A$ (minimal polynomial of A) $\equiv c_A$ (characteristic polynomial of A). In other words, the sets $\{A^i b\}_{0\le i\le n-1}$ and $\{(A^T)^i c\}_{0\le i\le n-1}$ are linearly independent and form a basis for $\mathbb{C}^n$. Moreover, since the characteristic polynomial of A has non-zero constant term, A must be an invertible matrix and has all non-zero eigenvalues.

Since the minimal polynomial can be characterized using the JNF decomposition, there must be a unique Jordan block corresponding to each eigenvalue of the matrix A because otherwise the power of $(x-\lambda)$ in the minimal polynomial will be lesser than that in the characteristic polynomial (Lemma 2.1). We have reduced the problem to its essence, thereby, ensuring that we have contribution from only those eigenvalues which are really necessary for evaluating the while loop condition.

Lemma 2.3. *In the final order-reduced problem, every eigenvalue of the matrix A has a non-zero contribution to the while loop condition. Also, the coefficient of the largest power of k multiplied with λ_j^k is non-zero. In other words, using symbols from equation (2), $deg(R_j(k)) = m_j$ for all j.*

Proof. $\{A^i b\}_{0\leq i\leq n-1}$ is a basis for $\mathbb{C}^n \implies \{P^{-1}J^iPb\}_{0\leq i\leq n-1}$ is a basis for $\mathbb{C}^n \implies \{J^iPb\}_{0\leq i\leq n-1}$ is a basis for $\mathbb{C}^n$. Using the notation of subsection 2.1, $Pb = (e_{11}, ..., e_{1m_1}, e_{21}, ..., e_{2m_2}, ..., e_{l1}, ..., e_{lm_l})^T$ and $c^TP^{-1} = (f_{1m_1}, ..., f_{11}, f_{2m_2}, ..., f_{21}, ..., f_{lm_l}, ..., f_{l1})$. Coefficient of the largest power of k multiplied by λ_j^k in the while loop condition = the coefficient of $(m_j, m_j)^{th}$ element of the matrix J_j^k in the expression $f_j^T J_j^k e_j$ (since there is exactly one Jordan block for each eigenvalue) $= e_{jm_j} f_{jm_j}$. We need to show that $e_{jm_j} f_{jm_j} \neq 0$ for all $j = 1, 2, ..., l$.

Suppose that $e_{jm_j} = 0$ for some $1 \leq j \leq m_j$. Now, the m_j^{th} element of $J_j^i e_j$ for $0 \leq i \leq n-1$ is always zero since J_j^i is upper triangular and its last row has only one non-zero element which multiplies with $e_{jm_j} = 0$. This is not possible because the vector $v = (0, ...0, 1, 0, ..., 0)^T$ with an entry 1 at $(m_1 + ... + m_j)^{th}$ position cannot be represented as a linear combination of vectors from $\{J^iPb\}_{0\leq i\leq n-1}$ as their $(m_1 + ... + m_j)^{th}$ element is same as m_j^{th} element of $J_j^i e_j$ which is always zero. Therefore, $e_{jm_j} \neq 0$ for all $1 \leq j \leq l$.

A similar proof by considering $\{(J^T)^i(P^{-1})^Tc\}_{0\leq i\leq n-1}$ as the basis yields $f_{jm_j} \neq 0$ for all $1 \leq j \leq l$. □

Order reduction also establishes an equivalence between deciding termination of the single-input linear program `P3` and deciding positivity of integer linear homogenous recurrences. The value for loop conditional in k^{th} iteration can be seen as the k^{th} term of a linear recurrence.

Corollary 2.4. *The final order-reduced problem $\pi(n, \boldsymbol{b}, \boldsymbol{c}, A)$ can be seen as deciding positivity (whether $c_n > 0$ for all $n \geq 0$ or not) of the linear recurrence $c_{n+m} = \sum_{i=0}^{m-1} \alpha_i c_{n+i}$ with initial conditions $c_i = \boldsymbol{c}^T A^i \boldsymbol{b}$ for all $i = 0, 1, ..., m-1$.*

3 Deciding the Base Problem

For deciding termination of the all inputs problem there seems to be two separate proof approaches: one on the lines of Tiwari and Braverman's work([1] and [5]), and the other as presented in [9]. The second approach extends the termination paradigm to incorporate polynomial loop conditions, but leaves the problem with inputs ranging over reals unsolved for a class of problems. The first approach cannot be easily extended to be used for the single input case, whereas the other proof approach symbolically maintains the input and hence is promising to aid in the single input case. We try to adapt the second approach to solve the base problem. Our adaptation however uses a polynomial optimization technique as opposed to using a semi-algebraic solver as used in [9].

Following the approach in [9], we first prove that the set $\{E_{\lambda,r}(k)|\ k \in \mathbb{N}\}$ (Notation from subsection 2.1) is a dense subset of $\mathbb{R}$ and then present a procedure to find infimum of the expression $E_{\lambda,r}(k)$ ($k \in \mathbb{N} \cup \{0\}$).Let λ^* be the largest modulus of the eigenvalues and $r^* = m_{\lambda^*}$ be the largest degree of the polynomials corresponding to the eigenvalues with modulus λ^*. We define $\nu(\lambda, r) := \inf_{k\in\mathbb{N}} E_{\lambda,r}(k)$.

Note that even when we constrain the input to integers and loop condition to a linear inequality the undecidability proof for deciding termination over integers in [9] doesn't go through. Also their ability to use a semi-algebraic system solver relies on the fact that the symbolic inputs can range over the whole set of reals. As we will see later we can continue to use decision procedures for real arithmetic in our adaptation of their method, despite the fact that we use a rational (not arbitrary real) initialization vector. Specifically, instead of checking satisfiability of a semi-algebraic system we just need to solve a polynomial optimization problem over reals to find the infimum $\nu(\lambda^*, r^*)$. This can be done using techniques based on Grobner Bases ([13]) or Tarski's quantifier elimination ([14]). We take cases based on the sign of $\nu(\lambda*, r*)$:

- If $\nu(\lambda^*, r^*) > 0$ then for sufficiently large k the sign of the loop condition (1) will be decided by the sign of $E_{\lambda^*,r^*}(k)$ i.e. it will be positive after some $k_0 \in \mathbb{N}$. We therefore need to check for termination till k_0. Such a value k_0 can be computed by using the upper bounds on $E_{\lambda,r}(k)$ given by $\sum_{j\in I_\lambda}(|a_{j,r}| + |b_{j,r}|)$ for $(\lambda, r) \neq (\lambda^*, r^*)$.

- If $\nu(\lambda^*, r^*) < 0$ then since the set $\{E_{\lambda,r}(k)|\ (k \in \mathbb{N}\}$ is dense there exists a sequence of natural numbers for which the corresponding sequence of evaluations of this expression converges to the infimum. Hence it will be negative eventually along this sequence and for sufficiently large k, due to this term's dominance, the loop will terminate.

- If $\nu(\lambda^*, r^*) = 0$ then we need to look at the infimum of the next dominant term (either a lower power of k, i.e. $\nu(\lambda^*, r_1)$ for $r_1 < r^*$ such that $E_{\lambda^*,r}(k) = 0$ for all $r_1 < r < r^*$, or the most dominant term of the eigenvalue with the next lower modulus, i.e. $\nu(\lambda_1, m_{\lambda_1})$). If this infimum is positive then we can find k_0 such that for $k > k_0$ the loop condition is always satisfied. The same inference can be drawn if we find a sequence of dominating terms each with infimum zero followed by a term with positive infimum. Note that even if the last term doesn't exist and we just have a series of zero infimums our program `P5` will not terminate because it terminates only when we have a negative value taken by the expression in the loop condition. But, in case this last term has a negative infimum then we cannot claim satisfiability/unstaisfiability of the loop condition.

If there is no real root of the dominant modulus, Braverman's theorem (Lemma 4 in [5]) asserts that the dominant term oscillates indefinitely around 0 and hence its infimum must be negative. This fact combined with Lemma 2.3 ensures that the loop will terminate. If there is a real dominant eigenvalue and no other complex dominant eigenvalues then the infimum of the coefficient of the dominant term is a constant. This is also non-zero (Lemma 2.3). Therefore, the loop termination problem is decidable for base matrices which either do not have a real dominant eigenvalue or have a real dominant eigenvalue with no other complex dominant eigenvalues. Also, if the base problem matrix is non-negative, then the corresponding homogenous linear recurrence has non-negative coefficients and hence its sufficient to check positivity of first few terms to ensure positivity of all other terms inductively. Note that a non-negative base problem matrix (which is always invertible and hence irreducible) always has a dominant real eigenvalue with possibly some more conjugate complex dominant eigenvalues given by $re^{\frac{2k\pi}{h}}$ for $0 \leq k \leq h-1$ where h is called the period of the matrix (Perron-Frobenius theorem for irreducible non-negative matrices [6]). For this problem case to arise, one needs a dominant real eigenvalue with atleast two complex dominant eigenvalues (since they occur in conjugate pairs), and a fourth term with negative infimum. This requires a base problem matrix of order atleast four. Therefore, our method gives a complete algorithm for deciding the termination problem for base problem matrices of order less than or equal to three.

Suppose we have a procedure to decide the sign of an expression of the form:

$$Re\left(k^m \sum_{j\in I} |\lambda_j|^k (a_j \cos k\theta_j + b_j \sin k\theta_j)\right) = |\lambda|^k k^m \sum_{j\in I} (a_j \cos k\theta_j + b_j \sin k\theta_j) \tag{3}$$

where $a_j, b_j \in \mathbb{R}$ are constant algebraic numbers and $\theta_j = arg(\lambda_j) \in [0, 2\pi)$. Then we can decide the positivity of the loop condition (1) in all cases except those characterized by zero infimum for the coefficients of first few terms followed by a negative infimum for the next dominant term.

3.1 Finding infimum and supremum of the coefficient of dominant term

We solve the following problem:

Given $a_j, b_j \in \mathbb{R}$(algebraic numbers) and $\theta_j \in [0, 2\pi)$, $1 \leq j \leq n$ as arguments of some algebraic numbers, define

$$f(k) = \sum_{j=1}^{n} (a_j \cos k\theta_j + b_j \sin k\theta_j)$$

and find the infimum of the set $\{f(k) | k \in \mathbb{N} \cup \{0\}\}$.

Dealing with the rational multiples of π:

We can get rid of the values taken by rational angles since there are only finitely many possible tuples of values for the sines and cosines of their multiples. For any rational angle $\phi = \frac{2p\pi}{q}$, $gcd(p, q) = 1$, $\cos k\phi$ and $\sin k\phi$ can take only finitely many values namely the set $\{\cos \frac{2pk\pi}{q} | 0 \leq k < q\} \cup \{\sin \frac{2pk\pi}{q} | 0 \leq k < q\}$. So for m rational angles $\phi_i = \frac{2p_i\pi}{q_i}$, $gcd(p_i, q_i) = 1$, if $\mathcal{L} = lcm(q_1, q_2, ..., q_m)$ then there are atmost $\mathcal{L}$ tuples of values taken by $k\bar{\phi} = k(\phi_1, \phi_2, ..., \phi_m)$ (Chinese Remainder Theorem).

We first divide angles in $f(k)$ as rational and irrational as follows: (ϕ_j are rational and θ_i are irrationals)

$$f(k) = \sum_{j=1}^{m} (a'_j \cos k\phi_j + b'_j \sin k\phi_j) + \sum_{i=1}^{n} (a_j \cos k\theta_j + b_j \sin k\theta_j)$$

Also, for each tuple of values taken by these angles we have a constant value taken by the combination of their cosines in the function $f(k)$. We divide $\mathbb{N}$ into classes corresponding to each possible value for the tuple of angles. Each class corresponds to a remainder modulo $\mathcal{L}$.

$S_f = \{\sum_{j=1}^{m} (a'_j \cos k\phi_j + b'_j \sin k\phi_j) | k \in \mathbb{N}\}$ and $\mathbb{N} = \cup_{i=0}^{\mathcal{L}-1} (\mathcal{L}\mathbb{N} + i)$

S_f is finite (as shown above) since ϕ_j are all rational angles. For each feasible tuple of values taken by $k\bar{\phi}$ with all rational angles, we associate a constant(the combination of values taken by their cosines and sines in the left side summation) to the leftover expression comprising of only irrational angles.

$f_j(k) = \delta_j + \sum_{i=1}^{m} (a_i \cos k\theta_i + b_i \sin k\theta_i)$ for $k \in \mathcal{L}\mathbb{N} + j$

for $0 \leq j < \mathcal{L}$, $\delta_j \in S_f$ (sum corresponsing to this class).

Dealing with dependent irrational angles:

We first look at a lemma from [9]:

Lemma 3.1. *For irrational angles $\theta_1, \theta_2, ..., \theta_n$ such that the set $\{\theta_i | 1 \leq i \leq n\}$ is rationally independent i.e. for any set of rational numbers $\{r_i | 1 \leq i \leq n\}$ the linear combination $\sum_{i=1}^{n} \frac{r_i}{2\pi}\theta_i \notin \mathbb{Q}$, the set $\{k\bar{\theta}\}_{k\in\mathbb{N}}$ is dense in $\mathcal{W}_n = [0, 2\pi)^n$.*

Corollary 3.2. *For $a \in \mathbb{N}$,$b \in \mathbb{N} \cup \{0\}$, and irrational angles $\theta_1, \theta_2, ..., \theta_n$ which are rationally independent, the set $\{k\bar{\theta}\}_{k\in(a\mathbb{N}+b)}$ is dense in $\mathcal{W}_n = [0, 2\pi)^n$.*

Proof. Given any point $\bar{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_n) \in \mathcal{W}_n$, we find a sequence $\{k_m\bar{\theta}\}_{m\in\mathbb{N}}$ in $\{k\bar{\theta}\}_{k\in\mathbb{N}}$ (Lemma 3.3) that converges to the point $(\frac{\alpha_1 - b\theta_1}{a}, \frac{\alpha_2 - b\theta_2}{a}, ..., \frac{\alpha_n - b\theta_n}{a})$ which in turn provides us with a sequence $\{(ak_m + b)\bar{\theta}\}_{m\in\mathbb{N}}$ in $\{k\bar{\theta}\}_{k\in(a\mathbb{N}+b)}$ which converges to $\bar{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_n)$. □

Now, we try to impose the conditions of lemma 3.3 for the given irrational angles in the expression for $f_j(k)$. We proceed as follows:

Consider the set($\mathcal{S}_\theta$) of all angles in the expression $f(k)$.

We retrieve an angle from $\mathcal{S}_\theta$, say, θ_0 and check its rational dependence with other angles in $\mathcal{S}_\theta - \{\theta_0\}$. If we get any such dependence $p_0\theta_0 = \sum_{i=1}^{k} p_i\theta_i$ for $p_i \in \mathbb{Z} - \{0\}$ then we do the following:

(1) Remove all the angles θ_i from $\mathcal{S}_\theta$ for $0 \leq i \leq k$, and write $\theta_i = p_0\psi_i$ for $1 \leq i \leq k$ and $\theta_0 = \sum_{i=1}^{k} p_i\psi_i$ in the expression for $f_j(k)$.

(2) Add the angles $\{\psi_i\}_{1\leq i\leq k}$ in $\mathcal{S}_\theta$.

We repeat this process as long as we may proceed. At the end of this process we will have expressions in angles which are irrational multiples of 2π as well as they are rationally independent.

Let $\mathcal{S}_\theta = \{\phi_1, \phi_2, ..., \phi_m\}$ after the above mentioned procedure is complete.

$$f_j(k) = \delta_j + \sum_{i=1}^{l}\left(c_{ij}\cos\left(k\sum_{j=1}^{m} p_{ij}\phi_i\right) + d_{ij}\sin\left(k\sum_{j=1}^{m} p_{ij}\phi_i\right)\right)$$

Note that $\cos(a_1 + a_2 + ... + a_n)$ and $\sin(a_1 + a_2 + ... + a_n)$ can be written as a multivariate polynomial in $\cos a_i$ and $\sin a_i$. Also, $\cos p\theta$ can be written as a polynomial of degree p in $\cos\theta$ and $\sin p\theta$ can be written as product of $\sin\theta$ and a polynomial of degree $(p-1)$ in $\cos\theta$. Therefore, we can write $f_j(k) - \delta_j$ as a multivariate polynomial $P_j(x_1, ..., x_m, y_1, ..., y_m)$ in $x_i = \cos k\phi_i$ and $y_i = \sin k\phi_i$. Since $\{\phi_i\}_{i=1}^{m}$ satisfies the conditions of Lemma 3.3 and since the set $\{k\bar{\phi}\}_{k\in(\mathcal{L}\mathbb{N}+j)}$ is dense in $[0, 2\pi)^m$ (Corollary 3.4), it follows that computing the infimum is the same as solving the following polynomial optimization problem

minimize $P_j(x_1, ..., x_m, y_1, ..., y_m)$

with constraints: $x_i^2 + y_i^2 = 1$ for all $1 \leq i \leq m$

This problem can be seen as solving multiple polynomial equations in several variables (obtained from the gradients with lagrange multipliers). The minimum can be obtained as a solution of a regular chain of polynomials which corresponds to an algebraic value for the minimum. If the minimum value obtained from solving this polynomial optimization problem (as done in [13], [14]) is m_j then $I_j = \inf_{k\in(\mathcal{L}\mathbb{N}+j)} f_j(k) = \delta_j + m_j$. Hence, the overall infimum of the given expression is $I = \min_{1\leq j\leq\mathcal{L}} I_j$.

Example. Consider the order reduced problem given by:

$$b = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad c = \begin{pmatrix} 2354848 \\ 185008 \\ 1608 \\ 388 \\ 73 \end{pmatrix} \quad A = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ -216 & 0 & 1 & 0 & 0 \\ 3456 & 0 & 0 & 1 & 0 \\ -8192 & 0 & 0 & 0 & 1 \\ 1048576 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and characteristic polynomial $c_A(x) = (x-16)(x^2-4x+256)(x^2+18x+256)$. The eigenvalues are $16, 16e^{i\phi}, 16e^{-i\phi}$ (roots of $x^2-4x+256=0$), $16e^{i\theta}$ and $16e^{-i\theta}$ (roots of $x^2+18x+256=0$).

The loop inequality expression reduces to $16^k\,(33+20(\cos k\phi + \cos k\theta))$ where θ and ϕ are irrational angles. If they were also independent (i.e. their ratio was irrational) then the infimum of dominant term's coefficient will be -17 but in this case their ratio is rational with $\frac{\theta}{\phi} = \frac{3}{2}$. Let $\theta = 3\psi$ and $\psi = 2\psi$ (ψ also being irrational). Now, the expression becomes $16^k\left(33+20(4\cos^3\psi + 2\cos^2\psi - 3\cos\psi - 1)\right) = 16^k(80\cos^3\psi + 40\cos^2\psi - 60\cos\psi + 13)$. The minimum value taken by the polynomial $80x^3+40x^2-60x+13$ for $x \in [-1,1]$ is positive (approximately 0.3164618) and hence the expression will always remain positive.

3.2 Base problem of Order 4 and the hard instance

We consider the base problem $\pi(n,b,c,A)$ of order $n=4$. Let $c_A(x)$ be the characteristic (or minimal) polynomial of the matrix A. We factorize $c_A(x)$ over $\mathbb{Z}$. Note that if $c_A(x)$ has no real dominant eigenvalue then using Braverman's theorem we can show that the loop will always terminate since the dominant term oscillates around zero. Let n_d be the number of dominant roots of $c_A(x)$ counting multiplicities. We take cases based on the value of n_d. We assume that there is a real dominant root r. We also assume that $r > 0$ because otherwise we can break the problem into two problems: corresponding to the even and odd iterations which will ensure that dominant real root is positive.

Case 1: $n_d = 1$. Clearly $r \geq 1$ (since the product of all roots is an integer). If $r = 1$, then $|s| = 1$ for any root s of $c_A(x)$ but this implies that all four roots are dominant which is a contradiction. If $r > 1$ then the dominant term just a constant times a power of r. The sign of the constant coefficient will decide the termination eventually.

Case 2: $n_d = 2$. The other root must be $-r$ since any other complex root will occur in pairs. Now, the dominant term is of the form $(c_1 r^k + c_2(-r)^k)$. Clearly, the sign of $min(c_1+c_2, c_1-c_2)$ will decide termination eventually.

Case 3: $n_d = 4$. The dominant term is a power of r multiplied by an expression of the form (3). The loop terminates iff infimum of the expression is negative dominant modulus or zero.

Case 4: $n_d = 3$. This is the most interesting case. Let ϕ and $\bar{\phi}$ be the other two complex dominant roots i.e. $|\phi| = r$. The characteristic polynomial looks like $c_A(x) = (x^2 - tx + r^2)(x-r)(x-s)$ where $r,s,t \in \mathbb{Z}$ with $|t| < 2r$ and $|s| < r$. This is the only case which can potentially cause a problem in deciding termination. If $\phi = |r|e^{i\theta_1}$ then the termination condition looks like $(a_1 \sin k\theta_1 + b_1 \cos k\theta_1 + c_1)r^k + c_2 s^k \leq 0$. The problem may arise when θ_1 is an irrational multiple of π and infimum of the expression $(a_1 \sin k\theta_1 + b_1\cos k\theta_1 + c_1)$ is zero i.e. $c_1 = \sqrt{a_1^2 + b_1^2}$) and $c_2 < 0$. In all other cases termination is decidable since the infimum will be non-zero.

We also present a concrete example capturing the problem case:

$$b = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad c = \begin{pmatrix} 1873 \\ 27 \\ 73 \\ 15 \end{pmatrix} \quad A = \begin{pmatrix} 14 & 1 & 0 & 0 \\ -121 & 0 & 1 & 0 \\ 776 & 0 & 0 & 1 \\ -1536 & 0 & 0 & 0 \end{pmatrix}$$

$c_A(x) = (x^2-3x+64)(x-8)(x-3)$, $\cos\theta = \frac{3}{16}$ and the termination condition being $8^{k+1}(1+\cos k\theta) - 3^k = 8^{k+1}(1+\cos k\theta - \frac{1}{8}\left(\frac{3}{8}\right)^k) \leq 0$ which reduces to a yet unsolved problem: deciding positivity of the expression of the form $(1+\cos k\theta - \beta\alpha^k)$ with $|\alpha| < 1$, $\beta > 0$ and θ being an irrational multiple of π. This hard instance corresponds to the hard instance of the open problem of deciding positivity of linear homogenous recurrences of order 4. Braverman in [5] pointed out this problem case but didn't give any characterization for the problem instances which can be solved. On the other hand, [9] gives a characterization for some solvable cases but doesn't give any justification for whether the hard instances are limitations of their method or is it something more fundamental that may turn out to be a hard problem in other areas of mathematics. We resolve this gap by showing that the hard problem instance given by Braverman corresponds to the cases where the algorithm in [9] fails. In addition, this corresponds to an as-yet open problem of deciding positivity of linear recurrences ([7]).

3.3 Finding infimum and supremum of the coefficient of dominant term

We solve the following problem:

Given $a_j, b_j \in \mathbb{R}$(algebraic numbers) and $\theta_j \in [0, 2\pi)$, $1 \leq j \leq n$ as arguments of some algebraic numbers, define

$$f(k) = \sum_{j=1}^{n} (a_j \cos k\theta_j + b_j \sin k\theta_j)$$

and find the infimum of the set $\{f(k) | k \in \mathbb{N} \cup \{0\}\}$.

Dealing with the rational multiples of π:

We can get rid of the values taken by rational angles since there are only finitely many possible tuples of values for the sines and cosines of their multiples. For any rational angle $\phi = \frac{2p\pi}{q}$, $gcd(p, q) = 1$, $\cos k\phi$ and $\sin k\phi$ can take only finitely many values namely the set $\{\cos\frac{2pk\pi}{q} | 0 \leq k < q\} \cup \{\sin\frac{2pk\pi}{q} | 0 \leq k < q\}$. So for m rational angles $\phi_i = \frac{2p_i\pi}{q_i}$, $gcd(p_i, q_i) = 1$, if $\mathcal{L} = lcm(q_1, q_2, ..., q_m)$ then there are atmost $\mathcal{L}$ tuples of values taken by $k\vec{\phi} = k(\phi_1, \phi_2, ..., \phi_m)$ (Chinese Remainder Theorem).

We first divide angles in $f(k)$ as rational and irrational as follows: (ϕ_j are rational and θ_i are irrationals)

$$f(k) = \sum_{j=1}^{m} (a'_j \cos k\phi_j + b'_j \sin k\phi_j) + \sum_{i=1}^{n} (a_j \cos k\theta_j + b_j \sin k\theta_j)$$

Also, for each tuple of values taken by these angles we have a constant value taken by the combination of their cosines in the function $f(k)$. We divide $\mathbb{N}$ into classes corresponding to each possible value for the tuple of angles. Each class corresponds to a remainder modulo $\mathcal{L}$.

$S_f = \{\sum_{j=1}^{m} (a'_j \cos k\phi_j + b'_j \sin k\phi_j) | k \in \mathbb{N}\}$ and $\mathbb{N} = \cup_{i=0}^{\mathcal{L}-1} (\mathcal{L}\mathbb{N} + i)$

S_f is finite (as shown above) since ϕ_j are all rational angles. For each feasible tuple of values taken by $k\bar{\phi}$ with all rational angles, we associate a constant(the combination of values taken by their cosines and sines in the left side summation) to the leftover expression comprising of only irrational angles.

$f_j(k) = \delta_j + \sum_{i=1}^{m}(a_i \cos k\theta_i + b_i \sin k\theta_i)$ for $k \in \mathcal{L}\mathbb{N} + j$

for $0 \le j < \mathcal{L}$, $\delta_j \in S_f$ (sum corresponsing to this class).

Dealing with dependent irrational angles:

We first look at a lemma from [9]:

Lemma 3.3. *For irrational angles $\theta_1, \theta_2, ..., \theta_n$ such that the set $\{\theta_i | 1 \le i \le n\}$ is rationally independent i.e. for any set of rational numbers $\{r_i | 1 \le i \le n\}$ the linear combination $\sum_{i=1}^{n} \frac{r_i}{2\pi}\theta_i \notin \mathbb{Q}$, the set $\{k\bar{\theta}\}_{k\in\mathbb{N}}$ is dense in $\mathcal{W}_n = [0, 2\pi)^n$.*

Corollary 3.4. *For $a \in \mathbb{N}$,$b \in \mathbb{N} \cup \{0\}$, and irrational angles $\theta_1, \theta_2, ..., \theta_n$ which are rationally independent, the set $\{k\bar{\theta}\}_{k\in(a\mathbb{N}+b)}$ is dense in $\mathcal{W}_n = [0, 2\pi)^n$.*

Proof. Given any point $\bar{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_n) \in \mathcal{W}_n$, we find a sequence $\{k_m\bar{\theta}\}_{m\in\mathbb{N}}$ in $\{k\bar{\theta}\}_{k\in\mathbb{N}}$ (Lemma 3.3) that converges to the point $(\frac{\alpha_1 - b\theta_1}{a}, \frac{\alpha_2 - b\theta_2}{a}, ..., \frac{\alpha_n - b\theta_n}{a})$ which in turn provides us with a sequence $\{(ak_m + b)\bar{\theta}\}_{m\in\mathbb{N}}$ in $\{k\bar{\theta}\}_{k\in(a\mathbb{N}+b)}$ which converges to $\bar{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_n)$. ☐

Now, we try to impose the conditions of lemma 3.3 for the given irrational angles in the expression for $f_j(k)$. We proceed as follows:

Consider the set($\mathcal{S}_\theta$) of all angles in the expression $f(k)$.

We retrieve an angle from $\mathcal{S}_\theta$, say, θ_0 and check its rational dependence with other angles in $\mathcal{S}_\theta - \{\theta_0\}$. If we get any such dependence $p_0\theta_0 = \sum_{i=1}^{k} p_i\theta_i$ for $p_i \in \mathbb{Z} - \{0\}$ then we do the following:

(1) Remove all the angles θ_i from $\mathcal{S}_\theta$ for $0 \le i \le k$, and write $\theta_i = p_0\psi_i$ for $1 \le i \le k$ and $\theta_0 = \sum_{i=1}^{k} p_i\psi_i$ in the expression for $f_j(k)$.

(2) Add the angles $\{\psi_i\}_{1\le i\le k}$ in $\mathcal{S}_\theta$.

We repeat this process as long as we may proceed. At the end of this process we will have expressions in angles which are irrational multiples of 2π as well as they are rationally independent.

Let $\mathcal{S}_\theta = \{\phi_1, \phi_2, ..., \phi_m\}$ after the above mentioned procedure is complete.

$$f_j(k) = \delta_j + \sum_{i=1}^{l}\left(c_{ij}\cos\left(k\sum_{j=1}^{m} p_{ij}\phi_i\right) + d_{ij}\sin\left(k\sum_{j=1}^{m} p_{ij}\phi_i\right)\right)$$

Note that $\cos(a_1 + a_2 + ... + a_n)$ and $\sin(a_1 + a_2 + ... + a_n)$ can be written as a multivariate polynomial in $\cos a_i$ and $\sin a_i$. Also, $\cos p\theta$ can be written as a polynomial of degree p in $\cos\theta$ and $\sin p\theta$ can be written as product of $\sin\theta$ and a polynomial of degree $(p-1)$ in $\cos\theta$. Therefore, we can write $f_j(k) - \delta_j$ as a multivariate polynomial $P_j(x_1, ..., x_m, y_1, ..., y_m)$ in $x_i = \cos k\phi_i$ and $y_i = \sin k\phi_i$. Since $\{\phi_i\}_{i=1}^{m}$ satisfies the conditions of Lemma 3.3 and since the set $\{k\bar{\phi}\}_{k\in(\mathcal{L}\mathbb{N}+j)}$ is dense in $[0, 2\pi)^m$ (Corollary 3.4), it follows that computing the infimum is the same as solving the following polynomial optimization problem

minimize $P_j(x_1, ..., x_m, y_1, ..., y_m)$

with constraints: $x_i^2 + y_i^2 = 1$ for all $1 \le i \le m$

This problem can be seen as solving multiple polynomial equations in several variables (obtained from the gradients with lagrange multipliers). The minimum can be obtained as a solution of a regular chain of polynomials which corresponds to an algebraic value for the minimum. If the minimum value obtained from solving this polynomial optimization problem (as done in [13], [14]) is m_j then $I_j = \inf_{k \in (\mathcal{L}\mathbb{N}+j)} f_j(k) = \delta_j + m_j$. Hence, the overall infimum of the given expression is $I = \min_{1 \le j \le \mathcal{L}} I_j$.

Example. Consider the order reduced problem given by:

$$b = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad c = \begin{pmatrix} 2354848 \\ 185008 \\ 1608 \\ 388 \\ 73 \end{pmatrix} \quad A = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ -216 & 0 & 1 & 0 & 0 \\ 3456 & 0 & 0 & 1 & 0 \\ -8192 & 0 & 0 & 0 & 1 \\ 1048576 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and characteristic polynomial $c_A(x) = (x-16)(x^2-4x+256)(x^2+18x+256)$. The eigenvalues are $16, 16e^{i\phi}, 16e^{-i\phi}$ (roots of $x^2-4x+256=0$), $16e^{i\theta}$ and $16e^{-i\theta}$ (roots of $x^2+18x+256=0$).

The loop inequality expression reduces to $16^k\,(33+20(\cos k\phi + \cos k\theta))$ where θ and ϕ are irrational angles. If they were also independent (i.e. their ratio was irrational) then the infimum of dominant term's coefficient will be -17 but in this case their ratio is rational with $\frac{\theta}{\phi} = \frac{3}{2}$. Let $\theta = 3\psi$ and $\psi = 2\psi$ (ψ also being irrational). Now, the expression becomes $16^k \left(33 + 20(4\cos^3\psi + 2\cos^2\psi - 3\cos\psi - 1)\right) = 16^k(80\cos^3\psi + 40\cos^2\psi - 60\cos\psi + 13)$. The minimum value taken by the polynomial $80x^3+40x^2-60x+13$ for $x \in [-1,1]$ is positive (approximately 0.3164618) and hence the expression will always remain positive.

4 Decidable operations on algebraic numbers

We have seen how to find infimum of an expression of the form (3). In the process, we assumed the following two decision problems on algebraic numbers:

- Given an alegbraic number, deciding if its argument is rational.
- Given a set of algebraic numbers, deciding if their arguments are rationally independent.

We assume the computable number data structure for algebraic numbers which maintains the minimal polynomial corresponding to the algebraic number with a suitably precise approximation which can distinguish this number from other roots of this minimal polynomial and a procedure to find the number to an arbitrary precision as discussed in [4] and [10]. It follows that we can construct computable number datastructures for sum, product, quotient of two algebraic numbers and modulus of an algebraic number. We can also compare two algebraic numbers check if they are conjugates. Hence, we can justify establishing an order on the absolute values of the roots of characteristic equation and checking for algebraic coefficients in a polynomial to be zero and evaluating polynomial functions of algebraic numbers.

Consider the following result from [3].

Theorem 4.1. *Given non-zero algebraic numbers $\alpha, \beta_1, ..., \beta_k$ the set*

$$S = \{(j_1, j_2, ..., j_k) | \alpha\beta_1^{j_1}\beta_2^{j_2}...\beta_k^{j_k} = 1\}$$

is either empty or is an affine lattice with rank at most k and a small description. Moreover, it is decidable in polynomial time whether it is empty, and if not, to compute a small description in terms of an off-set vector v and a small basis.

Both decision problems can be reduced to some simpler version of this theorem.

- Checking if an angle is rational, is same as checking if given θ(argument of an algebraic number $\alpha = e^{i\theta}$ obtained from division of an eigenvalue and its modulus which is also an algebraic number) $\exists\ k$ such that $\alpha^k = e^{ik\theta} = 1$.

- Checking if a set of irrational angles is rationally independent is same as checking if given θ_i (irrational arguments of algebraic units β_i) $\exists\ k_i \in \mathbb{Z}$ for $1 \leq i \leq n$such that $\beta_1^{k_1}\beta_2^{k_2}...\beta_n^{k_n} = 1$ which is a simple reformulation of the theorem.

5 Future Work and Conclusion

Our approach can potentially decide termination on a finite set of points. For convex sets, non-termination of the program on the boundary points ensures non-termination on all interior points but the same is not true for temrination. The next step would be to characterize infinite sets of points for the termination problem. One possible solution to this problem might come from the solution to the following problem:

Given a monic polynomial over integers $p(x) = x^n - \sum_{i=0}^{n-1} \alpha_i x^i$, does there exist a monic polynomial $q(x)$ of degree m such that $p(x)q(x) = x^{m+n} - \sum_{i=0}^{m+n-1} \beta_i x^i$ with $\beta_i \geq 0$ for $0 \leq i \leq m+n$.

If the characteristic polynomial of the matrix A can be extended in this manner, we can ensure that $\boldsymbol{c}^T A^{m+n+k}\boldsymbol{b} = \sum_{i=0}^{m+n-1} \beta_i \boldsymbol{c}^T A^{i+k}\boldsymbol{b}$ with $\beta_i \geq 0$ for $0 \leq i \leq m+n$ and hence it is sufficient to ensure that $c^T A^j b > 0$ for $0 \leq j \leq m+n-1$ which will form a potentially infinite convex set of possibilities for $\boldsymbol{b}$ given a vector $\boldsymbol{c}$ and a matrix A, so as to ensure that $c^T A^k b > 0$ for all $k \geq 0$ by induction.

Another possible generalization of this framework of linear termination of programs will be to include non-linear (polynomial) transformations or non-deterministic choices between various linear transformations inside the loop with linear considitonals. As shown in [1] the problem with linear conditional is undecidable. Similar to extension of the Orbit problem to ABC problem, we would like to investigate the decidability of termination of a linear loop with a non-deterministic choice between two linear transformations which commute with each other i.e. $\exists\ i, j \in \mathbb{N} \cup \{0\}$ $\wedge$ $\boldsymbol{c}^T A^i B^j \boldsymbol{b} \leq 0$. This problem can be solved using the approach we took in this paper even though simultaeneous JNF decomposition is not possible, generating functions can be used to get an expression for the loop inequality as used in [9] but again the problem case remains the same: an open problem in the context of deciding positivity for linear recurrences.

References

[1] Termination of Linear Programs (2004), Ashish Tiwari, In CAV2004: Computer Aided Verification, volume 3114 of LNCS

[2] R. Kannan and R.Lipton, The orbit problem is decidable, STOC 1980, 252-261.

[3] The Complexity of the A B C Problem Resolved , Jin-Yi Cai , Richard J. Lipton , Yechezkel Zalcstein, Technical Report, SUNY Buffalo 1994(www.cse.buffalo.edu/tech-reports/94-17.ps)

[4] Computing Jordan Normal Forms Exactly for Commuting Matrices in Polynomial Time, Jin-yi Cai, Technical Report, SUNY Buffalo 1994(www.cse.buffalo.edu/tech-reports/94-16.ps)

[5] Termination of integer linear programs (2006), Mark Braverman, 2006. In CAV2006: Computer Aided Verification, volume 4144 of LNCS

[6] M. Boyle, Notes on the Perron-Frobenius Theory of Nonnegative Matrices, http://www.math.umb.edu/mmb.

[7] Vichian Laohakosol and Pinthira Tangsupphathawat. 2009. Positivity of third order linear recurrence sequences. Discrete Appl. Math. 157, 15 (August 2009), 3239-3248.

[8] Vesa Halava, Tero Harju, Mika Hirvensalo, Positivity of second order linear recurrent sequences, Discrete Applied Mathematics, Volume 154, Issue 3, 1 March 2006, Pages 447-451, ISSN 0166-218X

[9] Bican Xia and Zhihai Zhang. 2010. Termination of linear programs with nonlinear constraints. Journal of Symbolic Computation 45, 11 (November 2010), 1234-1249.

[10] Oliver Aberth 1968, Analysis in the Computable Number Field, Journal of the Association for Computing Machinery (JACM), vol 15, iss 2, pp 276-299.

[11] Zhongqin Bi, Meijing Shan, "Termination Analysis of Linear Programs with Conditionals," Advanced Computer Theory and Engineering, International Conference on, pp. 450-456, 2008

[12] Prasolov, Viktor Vasilevich, Problems and Theorems in Linear algebra, Translations of Mathematical Mono- graphs, Volume 134, American Mathematical Society, 1994

[13] Hagglof, K., Lindberg, P.O. and Stevenson, L. (1995), Computing global minima to polynomial optimization problems using Grobner bases. Journal of Global Optimization, 7(2), 115-125.

[14] Caviness, B. F. and Johnson, J. R., editors. Quantifier Elimination and Cylindrical Algebraic Decomposition. Springer Verlag, Berlin/Heidelberg, 1998.