Termination of Linear Loops over the Integers

Mehran Hosseini
Department of Computer Science, University of Oxford, UK
mehran.hosseini@cs.ox.ac.uk

Joël Ouaknine
Max Planck Institute for Software Systems, Germany
Department of Computer Science, University of Oxford, UK
joel@mpi-sws.org

James Worrell
Department of Computer Science, University of Oxford, UK
jbw@cs.ox.ac.uk

Abstract

We consider the problem of deciding termination of single-path while loops with integer variables, affine updates, and affine guard conditions. The question is whether such a loop terminates on all integer initial values. This problem is known to be decidable for the subclass of loops whose update matrices are diagonalisable, but the general case has remained open since being conjectured decidable by Tiwari in 2004. In this paper we show decidability of determining termination for arbitrary update matrices, confirming Tiwari's conjecture. For the class of loops considered in this paper, the question of deciding termination on a specific initial value is a longstanding open problem in number theory. The key to our decision procedure is in showing how to circumvent the difficulties inherent in deciding termination on a fixed initial value.

2012 ACM Subject Classification Computing methodologies → Algebraic algorithms; Theory of computation → Logic and verification

Keywords and phrases Program Verification, Loop Termination, Linear Integer Programs, Affine While Loops

Digital Object Identifier 10.4230/LIPIcs.ICALP.2019.118

Category Track B: Automata, Logic, Semantics, and Theory of Programming

Funding *Mehran Hosseini*: Mehran Hosseini was supported by ERC grant AVS-ISS (648701).
Joël Ouaknine: Joël Ouaknine was supported by ERC grant AVS-ISS (648701) and by DFG grant 389792660 as part of TRR 248 (see `https://perspicuous-computing.science`).
James Worrell: James Worrell was supported by EPSRC Fellowship EP/N008197/1.

1 Introduction

Termination is a central problem in program verification. In this paper we study termination of *single-path linear loops*, i.e., programs of the form

$$\textit{while } (g_1(\boldsymbol{x}) > 0 \wedge \ldots \wedge g_m(\boldsymbol{x}) > 0) \textit{ do } \boldsymbol{x} := f(\boldsymbol{x}),$$

where $g_1, \ldots, g_m : \mathbb{R}^d \to \mathbb{R}$ and $f : \mathbb{R}^d \to \mathbb{R}^d$ are affine maps with integer coefficients. Here the loop body has a single control path that performs a simultaneous affine update of the program variables. Analysis of loops of this form, including acceleration and termination, is an important part of analysing more complex programs (see, e.g., [7, 14, 16]).

For a set $S \subseteq \mathbb{R}^d$, we say that the above loop *terminates on* S if it terminates on all initial vectors $\boldsymbol{x} \in S$. Despite the simplicity of single-path linear loops, the question of deciding termination has proven challenging (and termination already becomes undecidable if the loop body consists of a nondeterministic choice between two different linear updates). Tiwari [25] showed that termination of single-path linear loops is decidable over $\mathbb{R}^d$. Subsequently, Braverman [9], using a more refined analysis of the loop components, showed that termination is decidable over $\mathbb{Q}^d$ and noted that termination on $\mathbb{Z}^d$ can be reduced to termination on $\mathbb{Q}^d$ in the homogeneous case, i.e., when the update map f and guards $g_1, \ldots, g_m$ are linear. More recently, Ouaknine, Sousa-Pinto, and Worrell [18] have proven that termination over $\mathbb{Z}^d$ is decidable in the non-homogeneous case under the assumption that the update function f has the form $f(\boldsymbol{x}) = A\boldsymbol{x} + \boldsymbol{a}$ for A a diagonalisable integer matrix. Decidability of termination for non-homogeneous linear loops over $\mathbb{Z}^d$ was conjectured by Tiwari [25, Conjecture 1], but has remained open until now.

In this paper we give a procedure for deciding termination of the general class of single-path linear loops over the integers, i.e., we generalise the result of [18] by lifting the assumption of diagonalisability. Note that for this class of programs, the question of termination on a *given initial value* in $\mathbb{Z}^d$ (as opposed to termination over all of $\mathbb{Z}^d$) is equivalent to the *Positivity Problem* for linear recurrence sequences, i.e., the problem of whether all terms in a given integer linear recurrence sequence are positive. Decidability of the Positivity Problem is a longstanding open problem (going back at least as far as the 1970s [22, 24]), and results in [19] suggest that a solution to the problem will require significant breakthroughs in number theory. However, in considering termination over $\mathbb{Z}^d$ one can benefit from the freedom to choose the initial values of the loop variables. In the present paper we exploit this freedom in order to circumvent the need to solve "hard instances" of the Positivity Problem when deciding termination of linear loops. In particular, we avoid the use of sophisticated Diophantine-approximation techniques, such as the S-units theorem, that were employed in [19]. By eschewing such tools we lose all hope of obtaining an effective characterisation of the set of non-terminating points, as was done in the diagonalisable case in [19], but our methods nevertheless manage to solve the decision problem in the general case.

Among the tools we use are a circle of closely related results in the geometry of numbers, including Khinchine's flatness theorem, Kronecker's theorem on simultaneous Diophantine approximation, and the result of Khachiyan and Porkolab that it is decidable whether a convex semi-algebraic set contains an integer point. In tandem with these, from algebraic number theory, we use a result of Masser that allows to compute all algebraic relations among the eigenvalues of the update matrix of a given loop. Using this last result, we define a semi-algebraic subset of "non-termination candidates" such that the loop is non-terminating if and only if this set contains an integer point.

In this paper we focus on the foundational problem of providing complete methods to solve termination. Much effort has been devoted to scalable and pragmatic methods to prove termination for classes of programs that subsume linear loops. In particular, techniques to prove termination via synthesis of linear ranking functions [4, 5, 8, 10, 11, 20, 21] and their extension, multiphase linear ranking functions [6, 3], have been developed. Many of these techniques have been implemented in software verification tools, such as Microsoft's TERMINATOR [12]. Although these methods are capable of handling non-deterministic linear loops, they can only guarantee termination whenever ranking functions of a certain form exist.

2 Background

2.1 Convexity

The *affine hull* of $S \subseteq \mathbb{R}^d$ is the smallest affine set that contains S, where an affine set is the translation of a vector subspace of $\mathbb{R}^d$. The affine hull of S can be characterised as follows:

$$\operatorname{aff}(S) := \left\{ \sum_{i=1}^{k} \alpha_i \boldsymbol{x}_i \mid k > 0, \boldsymbol{x}_i \in S, \alpha_i \in \mathbb{R}, \sum_{i=1}^{k} \alpha_i = 1 \right\} .$$

The *convex hull* of $S \subseteq \mathbb{R}^d$ is the smallest convex set that contains S. The convex hull of S can be characterised as follows:

$$\operatorname{conv}(S) := \left\{ \sum_{i=1}^{k} \alpha_i \boldsymbol{x}_i \mid k > 0, \boldsymbol{x}_i \in S, \alpha_i \in \mathbb{R}_{\geq 0}, \sum_{i=1}^{k} \alpha_i = 1 \right\} .$$

Clearly $\operatorname{conv}(S) \subseteq \operatorname{aff}(S)$. The *relative interior* of a convex set $S \subseteq \mathbb{R}^d$ is its interior with respect to the restriction of the Euclidean topology to $\operatorname{aff}(S)$. We have the following easy proposition, characterising the relative interior.

▶ **Proposition 1.** *Let $S = \{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n\} \subseteq \mathbb{R}^d$. If $\boldsymbol{u}$ lies in the relative interior of* $\operatorname{conv}(S)$ *then there exist $\alpha_1, \ldots, \alpha_n > 0$ such that $u = \sum_{i=1}^{n} \alpha_i \boldsymbol{a}_i$ and $\sum_{i=1}^{n} \alpha_i = 1$.*

Proof. Since $\boldsymbol{u}$ lies in the relative interior of $\operatorname{conv}(S)$, for $\varepsilon > 0$ sufficiently small we have that

$$(1 + n\varepsilon)u - \sum_{i=1}^{n} \varepsilon \boldsymbol{a}_i \in \operatorname{conv}(S) .$$

For such an ε there exist $\beta_1, \ldots, \beta_n \geq 0$ such that $(1 + n\varepsilon)u - \sum_{i=1}^{n} \varepsilon \boldsymbol{a}_i = \sum_{i=1}^{n} \beta_i \boldsymbol{a}_i$ and $\sum_{i=1}^{n} \beta_i = 1$. But then $\boldsymbol{u} = \sum_{i=1}^{n} \frac{\beta_i + \varepsilon}{1 + n\varepsilon} \boldsymbol{a}_i$. Defining $\alpha_i := \frac{\beta_i + \varepsilon}{1 + n\varepsilon}$ for $i \in \{1, \ldots, n\}$, the proposition is proved. ◀

A *lattice of rank* r in $\mathbb{R}^d$ is a set

$$\Lambda := \{z_1 \boldsymbol{v}_1 + \cdots + z_r \boldsymbol{v}_r : z_1, \ldots, z_r \in \mathbb{Z}\} ,$$

where $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r$ are linearly independent vectors in $\mathbb{R}^d$. Given a convex set $C \subseteq \mathbb{R}^d$, define the *width* of C along a vector $\boldsymbol{u} \in \mathbb{R}^d$ to be

$$\sup\{\boldsymbol{u}^\top (\boldsymbol{x} - \boldsymbol{y}) : \boldsymbol{x}, \boldsymbol{y} \in C\} .$$

Furthermore the *lattice width* of C is the infimum over all non-zero vectors $\boldsymbol{u} \in \Lambda$ of the width of C along $\boldsymbol{u}$.

The following result (see [2, Theorem 7.2.1]) captures the intuition that a convex set that contains no lattice point in its interior must be "thin" in some direction.

▶ **Theorem 2** (Flatness Theorem)**.** *Given a full-rank lattice Λ in $\mathbb{R}^d$ there exists W such that any convex set $C \subseteq \mathbb{R}^d$ of lattice width at least W contains a lattice point.*

Recall that $C \subseteq \mathbb{R}^d$ is said to be *semi-algebraic* if it is definable by a boolean combination of polynomial constraints $p(x_1, \ldots, x_d) > 0$, where $p \in \mathbb{Z}[x_1, \ldots, x_d]$.

▶ **Theorem 3** (Khachiyan and Porkolab [15])**.** *It is decidable whether a given convex semi-algebraic set $C \subseteq \mathbb{R}^d$ contains an integer point, that is, whether $C \cap \mathbb{Z}^d \neq \emptyset$.*

2.2 Groups of Multiplicative Relations

In this subsection we will introduce some concepts concerning groups of multiplicative relations among algebraic numbers.

Let $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$. We define the s-dimensional torus to be $\mathbb{T}^s$, considered as a group under component-wise multiplication. Given a tuple of algebraic numbers $\boldsymbol{\gamma} = (\gamma_1, \cdots, \gamma_s) \in \mathbb{T}^s$, the orbit $\{\boldsymbol{\gamma}^n : n \in \mathbb{N}\}$ is a subset of $\mathbb{T}^s$. In the following we characterise the topological closure of the orbit as an algebraic subset of $\mathbb{T}^s$.

The *group of multiplicative relations* of $\boldsymbol{\gamma} \in \mathbb{T}^s$ is defined as the following additive subgroup of $\mathbb{Z}^s$:

$$L(\boldsymbol{\gamma}) = \{\boldsymbol{v} \in \mathbb{Z}^s : \boldsymbol{\gamma}^{\boldsymbol{v}} = 1\},$$

where $\boldsymbol{\gamma}^{\boldsymbol{v}}$ is defined to be $\gamma_1^{v_1} \cdots \gamma_s^{v_s}$ for $\boldsymbol{v} \in \mathbb{Z}^s$, that is, exponentiation acts coordinate-wise. Since $L(\boldsymbol{\gamma})$ is a subgroup of $\mathbb{Z}^s$, it is a free Abelian group and hence has a finite basis. The following powerful theorem of Masser [17] gives bounds on the magnitude of the components of such a basis.

▶ **Theorem 4** (Masser). *The free Abelian group $L(\boldsymbol{\gamma})$ has a basis $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_l \in \mathbb{Z}^s$ for which*

$$\max_{1 \le i \le l, 1 \le j \le s} |v_{i,j}| \le (D \log H)^{O(s^2)},$$

where H and D bound respectively the heights and degrees of all the γ_i.

Membership of a tuple $\boldsymbol{v} \in \mathbb{Z}^s$ in $L(\boldsymbol{\gamma})$ can be computed in polynomial space, using a decision procedure for the existential theory of the reals. In combination with Theorem 4, it follows that we can compute a basis for $L(\boldsymbol{\gamma})$ in polynomial space by brute-force search.

Corresponding to $L(\boldsymbol{\gamma})$, we consider the following multiplicative subgroup of $\mathbb{T}^s$:

$$T(\boldsymbol{\gamma}) = \{\boldsymbol{\mu} \in \mathbb{T}^s : \forall \boldsymbol{v} \in L(\boldsymbol{\gamma}), \boldsymbol{\mu}^{\boldsymbol{v}} = 1\}.$$

If $\mathcal{B}$ is a basis of $L(\boldsymbol{\gamma})$, we can equivalently characterise $T(\boldsymbol{\gamma})$ as $\{\boldsymbol{\mu} \in \mathbb{T}^s : \forall \boldsymbol{v} \in \mathcal{B}, \boldsymbol{\mu}^{\boldsymbol{v}} = 1\}$. Crucially, this finitary characterisation allows us to represent $T(\boldsymbol{\gamma})$ as an algebraic set in $\mathbb{T}^s$.

We will use the following classical lemma of Kronecker on simultaneous Diophantine approximation to show that the orbit $\{\boldsymbol{\gamma}^n : n \in \mathbb{N}\}$ is a dense subset of $T(\boldsymbol{\gamma})$.

▶ **Lemma 5.** *Let $\boldsymbol{\theta}, \boldsymbol{\psi} \in \mathbb{R}^s$. Suppose that for all $\boldsymbol{v} \in \mathbb{Z}^s$, if $\boldsymbol{v}^T\boldsymbol{\theta} \in \mathbb{Z}$ then also $\boldsymbol{v}^T\boldsymbol{\psi} \in \mathbb{Z}$, i.e., all integer relations among the coordinates of $\boldsymbol{\theta}$ also hold among those of $\boldsymbol{\psi}$ (modulo $\mathbb{Z}$). Then, for each $\varepsilon > 0$, there exist $\boldsymbol{p} \in \mathbb{Z}^s$ and a non-negative integer n such that*

$$\|n\boldsymbol{\theta} - \boldsymbol{p} - \boldsymbol{\psi}\|_\infty \le \varepsilon.$$

We now arrive at the main result of the section:

▶ **Theorem 6.** *Let $\boldsymbol{\gamma} \in \mathbb{T}^s$. Then the orbit $\left\{\boldsymbol{\gamma}^k : k \in \mathbb{N}\right\}$ is a dense subset of $T(\boldsymbol{\gamma})$.*

Proof. Let $\boldsymbol{\theta} \in \mathbb{R}^s$ be such that $\boldsymbol{\gamma} = e^{2\pi i \boldsymbol{\theta}}$ (with exponentiation operating coordinate-wise). Notice that $\boldsymbol{\gamma}^{\boldsymbol{v}} = 1$ if and only if $\boldsymbol{v}^T\boldsymbol{\theta} \in \mathbb{Z}$. If $\boldsymbol{\mu} \in T(\boldsymbol{\gamma})$, we can likewise define $\boldsymbol{\psi} \in \mathbb{R}^s$ to be such that $\boldsymbol{\mu} = e^{2\pi i \boldsymbol{\psi}}$. Then the premises of Kronecker's lemma apply to $\boldsymbol{\theta}$ and $\boldsymbol{\psi}$. Thus, given $\varepsilon > 0$, there exist a non-negative integer k and $\boldsymbol{p} \in \mathbb{Z}^s$ such that $\|k\boldsymbol{\theta} - \boldsymbol{p} - \boldsymbol{\psi}\|_\infty \le \varepsilon$. Whence

$$\|\boldsymbol{\gamma}^k - \boldsymbol{\mu}\|_\infty = \|e^{2\pi i (k\boldsymbol{\theta} - \boldsymbol{p})} - e^{2\pi i \boldsymbol{\psi}}\|_\infty \le \|2\pi(k\boldsymbol{\theta} - \boldsymbol{p} - \boldsymbol{\psi})\|_\infty \le 2\pi\varepsilon.$$

◀

3 Termination Analysis via Spectral Theory

The general form of a simple linear loop in dimension d is as follows:

$$\textit{while } (g_1(\boldsymbol{x}) > 0 \wedge \ldots \wedge g_m(\boldsymbol{x}) > 0) \textit{ do } \boldsymbol{x} := f(\boldsymbol{x}),$$

where $g_1, \ldots, g_m : \mathbb{R}^d \to \mathbb{R}$ and $f : \mathbb{R}^d \to \mathbb{R}^d$ are affine functions. We assume that f and $g_1, \ldots, g_m$ have integer coefficients, that is, $f(\boldsymbol{x}) = A\boldsymbol{x} + \boldsymbol{a}$ for $A \in \mathbb{Z}^{d\times d}$ and $\boldsymbol{a} \in \mathbb{Z}^d$, and $g_i(\boldsymbol{x}) = \boldsymbol{b}_i^\top \boldsymbol{x} + c_i$ for $\boldsymbol{b}_i \in \mathbb{Z}^d$, $c_i \in \mathbb{Z}$ and $i = 1, \ldots, m$.

Note that

$$\begin{pmatrix} f(\boldsymbol{x}) \\ 1 \end{pmatrix} = \begin{pmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \boldsymbol{x} \\ 1 \end{pmatrix} \text{ and } g_i(\boldsymbol{x}) = (\boldsymbol{b}_i^\top \; c_i) \begin{pmatrix} \boldsymbol{x} \\ 1 \end{pmatrix}. \tag{1}$$

for all $\boldsymbol{x} \in \mathbb{R}^d$. We say that f is *non-degenerate* if no quotient of two distinct eigenvalues of the update matrix $\begin{pmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{pmatrix}$ is a root of unity.

▶ **Proposition 7.** *The termination problem for simple linear loops on integers is reducible to the special case of the problem for non-degenerate update functions.*

Proof. Consider a simple linear loop, as described above, whose update matrix has distinct eigenvalues $\lambda_1, \ldots, \lambda_s$. Let L be the least common multiple of the orders of the roots of unity appearing among the quotients λ_i/λ_j for $i \neq j$. It is known that $L = 2^{O(d\sqrt{\log d})}$ [13, Subsection 1.1.9]. The update matrix corresponding to the affine map $f^L = \underbrace{f \circ \cdots \circ f}_{L}$ has eigenvalues $\lambda_1^L, \ldots, \lambda_s^L$ and hence is non-degenerate. Moreover the original loop terminates if and only if the following loop terminates:

$$\textit{while } \bigwedge_{i=0}^{L-1} \left(g_1(f^i(\boldsymbol{x})) > 0 \wedge \ldots \wedge g_m(f^i(\boldsymbol{x})) > 0\right) \textit{ do } \boldsymbol{x} := f^L(\boldsymbol{x}),$$

This concludes the proof. ◀

In the rest of this section and in the next section we focus on the case of a loop

$$\mathsf{P}: \textit{ while } (g(\boldsymbol{x}) > 0) \textit{ do } x \leftarrow f(\boldsymbol{x}) \textit{ end} \tag{2}$$

with a single guard function $g(\boldsymbol{x}) = \boldsymbol{b}^\top \boldsymbol{x} + c$ and with non-degenerate update function $f(\boldsymbol{x}) = A\boldsymbol{x} + \boldsymbol{a}$, with both maps having integer coefficients. We show that a spectral analysis of the matrix underlying the loop update function suffices to classify almost all initial values of the loop as either terminating or eventually non-terminating. Towards the end of the section we isolate a class of so-called *critical* initial values that are not amenable to this analysis. We show how to deal with such points in Section 4.

With respect to the loop P we say that $\boldsymbol{x} \in \mathbb{R}^d$ is *terminating* if there exists n such that $g(f^n(\boldsymbol{x})) \leq 0$. We say that $\boldsymbol{x}$ is *eventually non-terminating* if the sequence $\langle g(f^n(\boldsymbol{x})) : n \in \mathbb{N}\rangle$ is *ultimately positive*, i.e., there exists N such that for all $n \geq N$ $g(f^n(\boldsymbol{x})) > 0$. Clearly there exists $\boldsymbol{z} \in \mathbb{Z}^d$ that is non-terminating if and only if there exists $\boldsymbol{z} \in \mathbb{Z}^d$ that is eventually non-terminating. Thus we can regard the problem of deciding termination on $\mathbb{Z}^d$ as that of searching for an eventually non-terminating point.

Let $\lambda_1, \ldots, \lambda_s$ be the non-zero eigenvalues of $\begin{pmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{pmatrix}$ and let $k_{\max}$ be the maximum multiplicity over all these eigenvalues.

Define a linear preorder on $I := \{0,\dots,k_{\max}-1\}\times\{1,\dots,s\}$ by $(i_1,j_1) \preccurlyeq (i_2,j_2)$ if either (i) $|\lambda_{j_1}| < |\lambda_{j_2}|$ or (ii) $|\lambda_{j_1}| = |\lambda_{j_2}|$ and $i_1 \le i_2$. Write $(i_1,j_1) \prec (i_2,j_2)$ if $(i_1,j_1) \preccurlyeq (i_2,j_2)$ and $(i_2,j_2) \not\preccurlyeq (i_1,j_1)$. Then we have

$$(i_1,j_1) \prec (i_2,j_2) \text{ iff } \lim_{n\to\infty} \frac{\binom{n}{i_1}|\lambda_{j_1}|^n}{\binom{n}{i_2}|\lambda_{j_2}|^n} = 0\,,$$

that is, the preorder $\preccurlyeq$ characterises the asymptotic order of growth in absolute value of the terms $\binom{n}{i}\lambda_j^n$ for $(i,j)\in I$. This preorder moreover induces an equivalence relation $\approx$ on I where $(i_1,j_1)\approx(i_2,j_2)$ iff $(i_1,i_1)\preccurlyeq(i_2,j_2)$ and $(i_2,i_2)\preccurlyeq(i_1,j_1)$.

The following closed-form expression for $g(f^n(\boldsymbol{x}))$ will be the focus of the subsequent development.

▶ **Proposition 8.** *There is a set of affine functions $h_{i,j} : \mathbb{R}^d \to \mathbb{C}$ such that for all $\boldsymbol{x}\in\mathbb{R}^d$ and all $n \ge d$ we have*

$$\boldsymbol{g}(f^n(\boldsymbol{x})) = \sum_{(i,j)\in I} \binom{n}{i} \lambda_j^n\, h_{i,j}(\boldsymbol{x})\,.$$

Proof. By the Jordan-Chevalley decomposition we can write $\begin{pmatrix} A & \boldsymbol{a} \\ 0 & 1\end{pmatrix} = P^{-1}DP+N$, where D is diagonal, N is nilpotent, P is invertible, $P^{-1}DP$ and N commute, and all matrices have algebraic coefficients. Moreover we can write $D = \lambda_1 D_1 + \cdots + \lambda_s D_s$ for appropriate idempotent diagonal matrices $D_1,\dots,D_s$. Then for all $n\in\mathbb{N}$ with $n\ge d$ we have

$$\begin{aligned}
g(f^n(\boldsymbol{x})) &= (\boldsymbol{b}^\top\ c)\begin{pmatrix} A & \boldsymbol{a} \\ 0 & 1\end{pmatrix}^n \begin{pmatrix}\boldsymbol{x}\\ 1\end{pmatrix} \\
&= (\boldsymbol{b}^\top\ c)(P^{-1}DP+N)^n \begin{pmatrix}\boldsymbol{x}\\ 1\end{pmatrix} \\
&= (\boldsymbol{b}^\top\ c)\sum_{i=0}^{n}\binom{n}{i} P^{-1}D^{n-i}PN^i \begin{pmatrix}\boldsymbol{x}\\ 1\end{pmatrix} \\
&= (\boldsymbol{b}^\top\ c)\sum_{i=0}^{d}\binom{n}{i} P^{-1}(\lambda_1^{n-i}D_1+\cdots+\lambda_s^{n-i}D_s)PN^i \begin{pmatrix}\boldsymbol{x}\\ 1\end{pmatrix} \qquad (\text{since } N^{d+1}=0) \\
&= \sum_{j=1}^{s}\lambda_j^n \sum_{i=0}^{d}\binom{n}{i} \underbrace{\lambda_j^{-i}(\boldsymbol{b}^\top\ c)P^{-1}D_jPN^i\begin{pmatrix}\boldsymbol{x}\\ 1\end{pmatrix}}_{h_{i,j}(\boldsymbol{x})} \qquad (3) \\
&= \sum_{j=1}^{s}\sum_{i=0}^{d}\binom{n}{i}\lambda_j^n h_{i,j}(\boldsymbol{x})\,,
\end{aligned}$$

where for $(i,j)\in I$ the affine function $h_{i,j}$ is defined in Line (3). Clearly each function $h_{i,j}$ is a complex-valued affine function on $\mathbb{R}^d$ with algebraic coefficients. ◀

Define $\gamma_i = \frac{\lambda_i}{|\lambda_i|}$ for $i=1,\dots,s$, that is, we obtain the γ_i by normalising the eigenvalues to have length 1. Recall from Section 2.2 the definition of the group $L(\boldsymbol{\gamma})$ of multiplicative relations that hold among $\gamma_1,\dots,\gamma_s$, *viz.*,

$$L(\boldsymbol{\gamma}) = \{(n_1,\dots,n_s)\in\mathbb{Z}^s : \gamma_1^{n_1}\cdots\gamma_s^{n_s} = 1\}\,.$$

Recall also that we have $T(\boldsymbol{\gamma}) \subseteq \mathbb{T}^s$, given by

$$T(\boldsymbol{\gamma}) = \{(\mu_1, \dots, \mu_s) \in \mathbb{T}^s : \mu_1^{n_1} \cdots \mu_s^{n_s} = 1 \text{ for all } (n_1, \dots, n_s) \in L(\boldsymbol{\gamma})\} .$$

Given an $\approx$-equivalence class $E \subseteq I$, note that for all $(i_1, j_1), (i_2, j_2) \in E$ we have $i_1 = i_2$ and $|\lambda_{j_1}| = |\lambda_{j_2}|$. Thus E is determines a common multiplicity, which we denote i_E, and a set of eigenvalues that all have the same absolute value, which we denote ρ_E.

Given an $\approx$-equivalence class E, define $\Phi_E : \mathbb{R}^d \times T(\boldsymbol{\gamma}) \to \mathbb{R}$ by[1]

$$\Phi_E(\boldsymbol{x}, \boldsymbol{\mu}) = \sum_{(i,j) \in E} h_{i,j}(\boldsymbol{x}) \mu_j . \tag{4}$$

From the above definition of Φ_E we have

$$\sum_{(i,j) \in E} \binom{n}{i} \lambda_j^n h_{i,j}(\boldsymbol{x}) = \binom{n}{i_E} \rho_E^n \Phi_E(\boldsymbol{x}, \boldsymbol{\gamma}^n) . \tag{5}$$

for all $\boldsymbol{x} \in \mathbb{R}^d$ and all $n \in \mathbb{N}$.

We say that an equivalence class E of I is *dominant* for $\boldsymbol{x} \in \mathbb{R}^d$ if E is the equivalence class of the maximal indices (i, j) for which $h_{i,j}(\boldsymbol{x})$ is non-zero. Equivalently, E is dominant for $\boldsymbol{x}$ if E is the maximal equivalence class such that $\Phi_E(\boldsymbol{x}, \cdot)$ is not identically zero on $T(\boldsymbol{\gamma})$. (The equivalence of these two characterisations follows from the linear independence of the functions $\binom{n}{i} \lambda_j^n$ for $(i, j) \in E$.)

The following proposition shows how information about termination of the loop P on an initial value $\boldsymbol{x} \in \mathbb{R}^d$ can be derived from properties of $\Phi_E(\boldsymbol{x}, \cdot)$.

▶ **Proposition 9.** *Consider the loop P in (2). Let $\boldsymbol{x} \in \mathbb{R}^d$ and let E be an $\approx$-equivalence class that is dominant for $\boldsymbol{x}$. Then*

1. *If $\inf_{\boldsymbol{\mu} \in T(\boldsymbol{\gamma})} \Phi_E(\boldsymbol{x}, \boldsymbol{\mu}) > 0$ then $\boldsymbol{x}$ is eventually non-terminating for P.*
2. *If $\inf_{\boldsymbol{\mu} \in T(\boldsymbol{\gamma})} \Phi_E(\boldsymbol{x}, \boldsymbol{\mu}) < 0$ then $\boldsymbol{x}$ is terminating for P.*

Proof. By Proposition 8 and Equation (5) we have that for all $n \geq d$,

$$\begin{aligned} g(f^n(\boldsymbol{x})) &= \sum_{(i,j) \in I} \binom{n}{i} \lambda_j^n h_{i,j}(\boldsymbol{x}) \\ &= \binom{n}{i_E} \rho_E^n \Phi_E(\boldsymbol{x}, \boldsymbol{\gamma}^n) + \sum_{(i,j) \in I \setminus E} \binom{n}{i} \lambda_j^n h_{i,j}(\boldsymbol{x}) . \end{aligned} \tag{6}$$

Moreover by the dominance of E we have that

$$\lim_{n \to \infty} \frac{\binom{n}{i} |\lambda_j|^n}{\binom{n}{i_E} \rho_E^n} = 0 \tag{7}$$

for all $(i, j) \in I \setminus E$ such that $h_{i,j}(\boldsymbol{x}) \neq 0$.

We first prove Item 1. By assumption, in this case there exists $\varepsilon > 0$ such that $\Phi_E(\boldsymbol{x}, \boldsymbol{\mu}) \geq \varepsilon$ for all $\boldsymbol{\mu} \in T(\boldsymbol{\gamma})$. Together with Equation (7), this shows that the asymptotically dominant term in Equation (6) has positive sign. It follows that $g(f^n(\boldsymbol{x}))$ is positive for n sufficiently large and hence $\boldsymbol{x}$ is eventually non-terminating.

[1] That the function Φ_E is real-valued follows from the fact that if eigenvalues λ_{j_1} and λ_{j_2} are complex conjugates then γ_{j_1} and γ_{j_2} are also complex conjugates, as are $h_{i,j_1}(\boldsymbol{z})$ and $h_{i,j_2}(\boldsymbol{z})$ (see the proof of Proposition 8).

We turn now to Item 2. By assumption there exists $\varepsilon > 0$ and an open subset U of $T(\boldsymbol{\gamma})$ such that $\Phi_E(\boldsymbol{x}, \boldsymbol{\mu}) < -\varepsilon$ for all $\boldsymbol{\mu} \in U$. Moreover by density of $\{\boldsymbol{\gamma}^n : n \in \mathbb{N}\}$ in $T(\boldsymbol{\gamma})$ there exist infinitely many n such that $\boldsymbol{\gamma}^n \in U$. Exactly as in Case 1 we can now use the dominance of E to conclude that $g(f^n(\boldsymbol{x})) < 0$ for sufficiently large n such that $\boldsymbol{\gamma}^n \in U$ and hence $\boldsymbol{x}$ is terminating. ◀

Given $\boldsymbol{z} \in \mathbb{Z}^d$, since $T(\boldsymbol{\gamma})$ is an algebraic subset of $\mathbb{T}^s$, the number $\inf_{\boldsymbol{\mu} \in T(\boldsymbol{\gamma})} \Phi_E(\boldsymbol{z}, \boldsymbol{\mu})$ is algebraic and its sign can be decided. Note however that Proposition 9 does not completely resolve the question of termination with respect to guard g from a given initial value $\boldsymbol{z}$. Indeed, let us define $\boldsymbol{z} \in \mathbb{R}^d$ to be *critical* if $\inf_{\boldsymbol{\mu} \in E} \Phi_E(\boldsymbol{z}, \boldsymbol{\mu}) = 0$, where E is the dominant equivalence class for $\boldsymbol{z}$. Then neither clause in the above proposition suffices to resolve termination of the loop P in (2) on such a $\boldsymbol{z}$. Indeed the question of whether such a point is eventually non-terminating is equivalent to the *Ultimate Positivity Problem* for linear recurrence sequences: a longstanding and notoriously difficult open problem in number theory, only known to be decidable up to order 4 [1, 19]. Fortunately in the setting of deciding loop termination we can sidestep such difficult questions. The following section is devoted to handling critical points. The idea is to show that if there is a critical initial value then there is another initial value that is eventually non-terminating and moreover whose eventual non-termination can be established by Proposition 9.

4 Analysis of Critical Points

In this section we continue to analyse termination of the loop P, as given in (2) in the previous section, and refer to the notation established therein.

4.1 Transition Invariance of Critical Points

Intuitively critical points are those for which it is difficult to determine eventual non-termination. One should therefore expect that if $\boldsymbol{x} \in \mathbb{R}^d$ is critical then $f(\boldsymbol{x})$ should also be critical. This, and more, follows from the following proposition.

▶ **Proposition 10.** *Let $\boldsymbol{x} \in \mathbb{R}^d$ and let $E \subseteq I$ be an equivalence class that is dominant for $\boldsymbol{x}$. Then E is also dominant for $f(\boldsymbol{x})$ and for all $\boldsymbol{\mu} \in T(\boldsymbol{\gamma})$ we have $\Phi_E(f(\boldsymbol{x}), \boldsymbol{\mu}) = \rho_E \, \Phi_E(\boldsymbol{x}, \boldsymbol{\gamma}\boldsymbol{\mu})$, where the product $\boldsymbol{\gamma}\boldsymbol{\mu}$ is defined pointwise.*

Proof. By definition we have $\Phi_E(\boldsymbol{x}, \boldsymbol{\mu}) = \sum_{(i,j) \in E} h_{i,j}(\boldsymbol{x}) \mu_j$, where the $h_{i,j}$ satisfy

$$(\boldsymbol{b}^\top \ c) \begin{pmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{pmatrix}^n \begin{pmatrix} \boldsymbol{x} \\ 1 \end{pmatrix} = \sum_{(i,j) \in I} h_{i,j}(\boldsymbol{x}) \binom{n}{i} \lambda_j^n \tag{8}$$

for all $n \geq d$. Likewise we have $\Phi_E(f(\boldsymbol{x}), \boldsymbol{\mu}) = \sum_{(i,j) \in S} \widetilde{h}_{i,j}(\boldsymbol{x}) \mu_j$, where the $\widetilde{h}_{i,j}$ satisfy

$$(\boldsymbol{b}^\top \ c) \begin{pmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{pmatrix}^{n+1} \begin{pmatrix} \boldsymbol{x} \\ 1 \end{pmatrix} = \sum_{(i,j) \in I} \widetilde{h}_{i,j}(\boldsymbol{x}) \binom{n}{i} \lambda_j^n \,. \tag{9}$$

Combining Equations (8) and (9) we have the for all $n \geq d$,

$$\begin{aligned} \sum_{(i,j) \in I} \widetilde{h}_{i,j}(\boldsymbol{x}) \binom{n}{i} \lambda_j^n &= \sum_{(i,j) \in I} h_{i,j}(\boldsymbol{x}) \binom{n+1}{i} \lambda_j^{n+1} \\ &= \sum_{(i,j) \in I} h_{i,j}(\boldsymbol{x}) \left[\binom{n}{i} + \binom{n}{i-1} \right] \lambda_j \lambda_j^n \,. \end{aligned}$$

Now the collection of functions $n \mapsto \binom{n}{i}\lambda_j^n$ for $(i,j) \in I$ is linearly independent in the vector space $\mathbb{C}^{\mathbb{N}}$ (see, e.g., [23, Lemma 9.6]). Equating the coefficients of the functions $\binom{n}{i}\lambda_j^n$ for $(i,j) \in E$ in the above equation we have $\widetilde{h}_{i,j} = \lambda_j h_{i,j} = \rho_E \gamma_j h_{i,j}$ for all $(i,j) \in E$; likewise we have that E is dominant for $f(\boldsymbol{x})$. The proposition follows. ◀

The next lemma shows that the existence of a critical point entails the existence of an eventually non-terminating point.

▶ **Lemma 11.** *If $\boldsymbol{z} \in \mathbb{R}^d$ is critical then there exists a positive integer M such that for all $n \geq M$, all points in the relative interior of* $\operatorname{conv}(\{f^d(\boldsymbol{z}), f^{d+1}(\boldsymbol{z}), \dots, f^n(\boldsymbol{z})\})$ *are eventually non-terminating.*

Proof. Given an arbitrary $\boldsymbol{\mu} \in T(\boldsymbol{\gamma})$ we claim that there exists $n \geq d$ for which we have $\Phi_E(f^n(\boldsymbol{z}), \boldsymbol{\mu}) > 0$. If this were not the case then for all $n \geq d$ we would have $\Phi_E(f^n(\boldsymbol{z}), \boldsymbol{\mu}) = \Phi_E(\boldsymbol{z}, \boldsymbol{\xi}^n \boldsymbol{\mu}) = 0$. But by Theorem 6, the set $\{\boldsymbol{\xi}^n \boldsymbol{\mu} : n \geq d\}$ is dense in $T(\boldsymbol{\gamma})$ and hence we would have that $\Phi_E(\boldsymbol{z}, \cdot)$ is identically 0 on $T(\boldsymbol{\gamma})$, contradicting the dominance of E.

For each $n \in \mathbb{N}$, the set $C_n = \{\boldsymbol{\mu} \in T(\boldsymbol{\gamma}) : \Phi_E(f^n(\boldsymbol{z}), \boldsymbol{\mu}) > 0\}$ is an open subset of $T(\boldsymbol{\gamma})$. Moreover, by the analysis above, the collection $\{C_n : n \geq d\}$ is an open cover of $T(\boldsymbol{\gamma})$. Thus by compactness of $T(\boldsymbol{\gamma})$ there exists $M \in \mathbb{N}$ such that $C_d, C_{d+1}, \cdots, C_M$ is a finite cover of $T(\boldsymbol{\gamma})$.

By Proposition 1, for all $n \geq M$ and all points $\boldsymbol{x}$ lying in the relative interior of $\operatorname{conv}(\{f^d(\boldsymbol{z}), f^{d+1}(\boldsymbol{z}), \dots, f^n(\boldsymbol{z})\})$, there exist $\alpha_d, \dots, \alpha_n > 0$ such that $\sum_{i=d}^n \alpha_i = 1$ and $\boldsymbol{x} = \sum_{i=d}^n \alpha_i f^i(\boldsymbol{z})$. Since Φ_E is an affine map in its first variable, it follows that $\Phi_E(\boldsymbol{x}, \cdot) = \sum_{i=d}^n \alpha_i \Phi_E(f^i(\boldsymbol{z}), \cdot)$ is strictly positive on $T(\boldsymbol{\gamma})$. Hence $\boldsymbol{x}$ is eventually non-terminating by Proposition 9. ◀

4.2 Integer Non-Terminating Points from Critical Points

Lemma 11 shows how to derive the existence of non-terminating points from the existence of a critical point. In this subsection we refine this analysis to derive the existence of *integer* non-terminating points. In particular, fixing an initial value $\boldsymbol{z}_* \in \mathbb{Z}^d$, we show that for n sufficiently large, the set

$$\operatorname{conv}(\{f^d(\boldsymbol{z}_*), f^{d+1}(\boldsymbol{z}_*), \dots, f^n(\boldsymbol{z}_*)\})$$

contains an integer point in its relative interior.

Define $V := \operatorname{Aff}(\{f^n(\boldsymbol{z}_*) : n \geq d\})$ and let the vector subspace $V_0 \subseteq \mathbb{R}^d$ be the unique translate of V containing the origin. Write d_0 for the dimension of V_0 (equivalently the dimension of V).

▶ **Proposition 12.** *For all non-zero integer vectors $\boldsymbol{v} \in V_0$ the set $\{|\boldsymbol{v}^\top f^n(\boldsymbol{z}_*)| : n \geq d\}$ is unbounded.*

Proof. Consider the sequence $x_n := \boldsymbol{v}^\top f^n(\boldsymbol{z}_*) = \begin{pmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{pmatrix}^n \begin{pmatrix} \boldsymbol{z}_* \\ 1 \end{pmatrix}$. If this sequence were constant then $\boldsymbol{v}$ would be orthogonal to V_0, contradicting the fact that $\boldsymbol{v}$ is non-zero. Since the sequence is non-constant, integer-valued, and satisfies a non-degenerate linear recurrence of order at most $d+1$ (see, e.g., [13, Subsection 1.1.12]), by the Skolem-Mahler-Lech Theorem we have that $\{|\boldsymbol{v}^\top f^n(\boldsymbol{z}_*)| : n \geq d\}$ is unbounded (see the discussion of growth of linear recurrence in [13, Section 2.2]).[2] ◀

▶ **Proposition 13.** *There exists M such that for all $n \geq M$ the set*

$$\mathrm{conv}(\{f^d(\boldsymbol{z}_*), f^{d+1}(\boldsymbol{z}_*), \ldots, f^n(\boldsymbol{z}_*)\})$$

contains an integer point in its relative interior.

Proof. Since V_0 is spanned by integer vectors, $\Lambda := V_0 \cap \mathbb{Z}^d$ is a lattice of rank d_0 in $\mathbb{R}^d$. Define $C := \mathrm{conv}(\{f^n(\boldsymbol{z}_*) : n \geq d\}) \subseteq V$ and $C_0 := C - f^d(\boldsymbol{z}_*) \subseteq V_0$.

Let $\theta : \mathbb{R}^d \to \mathbb{R}^{d_0}$ be a linear map that takes V_0 bijectively onto $\mathbb{R}^{d_0}$ and whose kernel is the orthogonal complement of V_0. Then $\theta(\Lambda)$ is a lattice in $\mathbb{R}^{d_0}$ of full rank. We claim that the lattice width of $\theta(C_0)$ with respect to $\theta(\Lambda)$ is infinite. Indeed for any non-zero vector $\boldsymbol{v} \in \theta(\Lambda)$ we have

$$\boldsymbol{v}^\top(\theta(f^n(\boldsymbol{z}_*)) - \theta(f^d(\boldsymbol{z}_*))) = (\theta^*\boldsymbol{v})^\top(f^n(\boldsymbol{z}_*) - f^d(\boldsymbol{z}_*)), \tag{10}$$

where $\theta^* : \mathbb{R}^{d_0} \to \mathbb{R}^d$ is the adjoint map of θ. But $\theta^*\boldsymbol{v}$ is a non-zero rational vector in V_0 and hence Proposition 12 entails that the absolute value of (10) is unbounded as n runs over $\mathbb{N}$. This proves the claim.

By Theorem 2 we have that $\theta(C_0)$ contains a point of $\theta(\Lambda)$ in its relative interior and hence C_0 contains a point of Λ (necessarily an integer point) in its relative interior. We conclude that C also contains an integer point in its relative interior. ◀

We summarise Sections 3 and 4 with a theorem characterising when a loop with a single guard is terminating.

▶ **Theorem 14.** *The loop P, given in (2), is non-terminating on $\mathbb{Z}^d$ if and only if there exists $\boldsymbol{z} \in \mathbb{Z}^d$ and an $\approx$-equivalence class E such that (i) E is dominating for $\boldsymbol{z}$ and (ii) $\inf_{\boldsymbol{\mu} \in T(\boldsymbol{\gamma})} \Phi_E(\boldsymbol{z}, \boldsymbol{\mu}) \geq 0$.*

Proof. If no such $\boldsymbol{z}$ exists then the loop is terminating by Proposition 9(2). Conversely, if such a $\boldsymbol{z}$ exists then by Lemma 11 and Proposition 13 there exists $\boldsymbol{z}' \in \mathbb{Z}^d$ such that $\inf_{\boldsymbol{\mu} \in T(\boldsymbol{\gamma})} \Phi_E(\boldsymbol{z}', \boldsymbol{\mu}) > 0$ (and with E still dominating for $\boldsymbol{z}'$.) Such a point is eventually non-terminating by Proposition 9(1). ◀

We postpone the question of the effectiveness of the above characterisation until we handle loops with multiple guards, in Section 5.

---

[2] The above argument actually establishes that $\langle x_n : n \in \mathbb{N}\rangle$ diverges to infinity in absolute value. We briefly sketch a more elementary proof of mere unboundedness. If the sequence $\langle x_n : n \in \mathbb{N}\rangle$ were bounded then by van der Waerden's Theorem, for all m it would contain a constant subsequence of the form $x_\ell, x_{\ell+p}, \ldots, x_{\ell+mp}$ for some $\ell, p \geq 1$. In particular, if $m = d$ then since every infinite subsequence $y_n := x_{\ell+pn}$ satisfies a linear recurrence of order at most $d+1$, $\langle x_n : n \in \mathbb{N}\rangle$ would have an infinite constant subsequence $\langle x_{\ell+pn} : n \in \mathbb{N}\rangle$. If $p = 1$ then $\langle x_n : n \in \mathbb{N}\rangle$ is constant and if $p > 1$ then by [23, Lemma 9.11] $\langle x_n : n \in \mathbb{N}\rangle$ is degenerate.

5 Multiple Guards

Now we are ready to present our decision procedure for a general linear loop program

$$\mathsf{Q} \, : \, \textit{while } (g_1(\boldsymbol{x}) > 0 \wedge \ldots \wedge g_m(\boldsymbol{x}) > 0) \textit{ do } \boldsymbol{x} := f(\boldsymbol{x}) \,, \tag{11}$$

with multiple guards. Associated to the loop Q we consider m single-guard loops with a common update function:

$$\mathsf{Q}_i \, : \, \textit{while } (g_i(\boldsymbol{x}) > 0) \textit{ do } \boldsymbol{x} := f(\boldsymbol{x}) \,,$$

for $i = 1, \ldots, m$. Clearly Q is non-terminating if and only if there exists $\boldsymbol{z} \in \mathbb{Z}^d$ such that each loop Q_i is non-terminating on $\boldsymbol{z}$. As we now explain, we can decide the existence of such a point following the proof of Theorem 14.

Let $\lambda_1, \ldots, \lambda_s$ be the distinct non-zero eigenvalues of the matrix corresponding to the update function f in the loop Q. As before, write $\gamma_j = \frac{\lambda_j}{|\lambda_j|}$ for $j = 1, \ldots, s$. For $i = 1, \ldots, m$, denote by $\Phi_E^{(i)} : \mathbb{R}^d \times T(\boldsymbol{\gamma}) \to \mathbb{R}$ the function associated to loop Q_i and $\approx$-equivalence class E as defined by (4). Given $\approx$-equivalence classes $E_1, \ldots, E_m$, we define $W_{E_1,\ldots,E_m} \subseteq \mathbb{R}^d$ to be the set of $\boldsymbol{\gamma} \in \mathbb{R}^d$ such that the following hold for $i = 1, \ldots, m$:

- E_i is dominant for $\boldsymbol{x}$ in loop Q_i, that is, $\Phi_{E_i}^{(i)}(\boldsymbol{x}, \cdot) \not\equiv 0$ and $\Phi_E^{(i)}(\boldsymbol{x}, \cdot) \equiv 0$ for all $E_i \prec E$.
- $\inf\limits_{\boldsymbol{\mu} \in T(\boldsymbol{\gamma})} \Phi_{E_i}^{(i)}(\boldsymbol{x}, \boldsymbol{\mu}) \geq 0$.

▶ **Proposition 15.** *Loop Q is non-terminating if and only if there exist $\approx$-equivalence classes $E_1, \ldots, E_m$ such that $W_{E_1,\ldots,E_m}$ contains an integer point.*

Proof. Suppose that Q fails to terminate on $\boldsymbol{z} \in \mathbb{Z}^d$. Then each loop Q_i also fails to terminate on $\boldsymbol{z} \in \mathbb{Z}^d$. Thus if E_i is the dominant equivalence class for $\boldsymbol{z}$ in program Q_i, for $i = 1, \ldots, m$, applying Proposition 9(2) we get that $\boldsymbol{z} \in W_{E_1,\ldots,E_m}$.

Conversely, suppose $\boldsymbol{z} \in W_{E_1,\ldots,E_m}$ for some $\approx$-equivalence classes $E_1, \ldots, E_m$. Then, by Lemma 11 and Proposition 13, there is an integer point $\boldsymbol{z}' \in \operatorname{conv}(\{f^n(\boldsymbol{z}) : n \geq d\})$ such that $\inf\limits_{\boldsymbol{\mu} \in T(\boldsymbol{\gamma})} \Phi_{E_i}^{(i)}(\boldsymbol{z}', \boldsymbol{\mu}) > 0$ for $i = 1, \ldots, m$. By Proposition 9(1), each loop Q_i fails to terminate on $\boldsymbol{z}'$ and hence also Q is non-terminating on $\boldsymbol{z}'$. ◀

Proposition 15 leads to the following procedure for deciding termination of a given linear loop Q, as shown in (11).

1. Compute the eigenvalues of the matrix corresponding to the loop update function, as given in (1).
2. Compute the dominance preorder $\preccurlyeq$ among eigenvalues.
3. Compute a basis of the group of multiplicative relations $L(\boldsymbol{\gamma})$.
4. Return "non-terminating" if some set $W_{E_1,\ldots,E_m}$ contains an integer point and otherwise return "terminating".

In terms of effectiveness, Steps 1 and 2 can be accomplished via standard symbolic computations with algebraic numbers. (We refer to [18] for a detailed treatment in a very similar setting.) By Theorem 4, computing a basis of $L(\boldsymbol{\gamma})$ reduces to checking a finite collection of multiplicative relations among algebraic numbers. Given a basis of $L(\boldsymbol{\gamma})$ we can directly obtain representations of each set $W_{E_1,\ldots,E_m}$ as semi-algebraic subsets of $\mathbb{R}^d$. Finally, since $W_{E_1,\ldots,E_m}$ is convex, we can decide the existence of an integer point in each set $W_{E_1,\ldots,E_m}$ using Theorem 3.

We have thus established the main result of the paper:

▶ **Theorem 16.** *There is a procedure to decide termination of single-path linear loops (of the form specified in* (11)*) over the integers.*

References

1. Shaull Almagor, Brynmor Chapman, Mehran Hosseini, Joël Ouaknine, and James Worrell. Effective Divergence Analysis for Linear Recurrence Sequences. In *29th International Conference on Concurrency Theory, CONCUR 2018, September 4-7, 2018, Beijing, China*, pages 42:1–42:15, 2018.
2. Alexander I. Barvinok. Lattice Points and Lattice Polytopes. In *Handbook of Discrete and Computational Geometry, Second Edition.*, pages 153–176. Chapman and Hall/CRC, 2004.
3. Amir M. Ben-Amram, Jesús Doménech, and Samir Genaim. Multiphase-Linear Ranking Functions and their Relation to Recurrent Sets. *CoRR*, abs/1811.07340, 2018. `arXiv:1811.07340`.
4. Amir M. Ben-Amram and Samir Genaim. On the linear ranking problem for integer linear-constraint loops. In *The 40th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '13, Rome, Italy - January 23 - 25, 2013*, pages 51–62, 2013.
5. Amir M. Ben-Amram and Samir Genaim. Ranking Functions for Linear-Constraint Loops. *J. ACM*, 61(4):26:1–26:55, 2014.
6. Amir M. Ben-Amram and Samir Genaim. On Multiphase-Linear Ranking Functions. In *Computer Aided Verification - 29th International Conference, CAV 2017, Heidelberg, Germany, July 24-28, 2017, Proceedings, Part II*, pages 601–620, 2017.
7. Bernard Boigelot. On iterating linear transformations over recognizable sets of integers. *Theor. Comput. Sci.*, 309(1-3):413–468, 2003.
8. Aaron R. Bradley, Zohar Manna, and Henny B. Sipma. Termination Analysis of Integer Linear Loops. In *CONCUR 2005 - Concurrency Theory, 16th International Conference, CONCUR 2005, San Francisco, CA, USA, August 23-26, 2005, Proceedings*, pages 488–502, 2005.
9. Mark Braverman. Termination of Integer Linear Programs. In *Computer Aided Verification, 18th International Conference, CAV 2006, Seattle, WA, USA, August 17-20, 2006, Proceedings*, pages 372–385, 2006.
10. Hong Yi Chen, Shaked Flur, and Supratik Mukhopadhyay. Termination proofs for linear simple loops. *STTT*, 17(1):47–57, 2015.
11. Michael Colón and Henny Sipma. Synthesis of Linear Ranking Functions. In *Tools and Algorithms for the Construction and Analysis of Systems, 7th International Conference, TACAS 2001 Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2001 Genova, Italy, April 2-6, 2001, Proceedings*, pages 67–81, 2001.
12. Byron Cook, Andreas Podelski, and Andrey Rybalchenko. Termination proofs for systems code. In *Proceedings of the ACM SIGPLAN 2006 Conference on Programming Language Design and Implementation, Ottawa, Ontario, Canada, June 11-14, 2006*, pages 415–426, 2006.
13. Graham Everest, Alfred J. van der Poorten, Igor E. Shparlinski, and Thomas Ward. *Recurrence Sequences*, volume 104 of *Mathematical surveys and monographs.* American Mathematical Society, 2003.
14. Bertrand Jeannet, Peter Schrammel, and Sriram Sankaranarayanan. Abstract acceleration of general linear loops. In *The 41st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '14, San Diego, CA, USA, January 20-21, 2014*, pages 529–540. ACM, 2014.
15. Leonid Khachiyan and Lorant Porkolab. Computing Integral Points in Convex Semi-algebraic Sets. In *38th Annual Symposium on Foundations of Computer Science, FOCS '97, Miami Beach, Florida, USA, October 19-22, 1997*, pages 162–171, 1997.
16. Zachary Kincaid, Jason Breck, John Cyphert, and Thomas W. Reps. Closed forms for numerical loops. *PACMPL*, 3(POPL):55:1–55:29, 2019.
17. David W Masser. Linear relations on algebraic groups. *New Advances in Transcendence Theory*, pages 248–262, 1988.
18. Joël Ouaknine, João Sousa Pinto, and James Worrell. On Termination of Integer Linear Loops. In *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2015, San Diego, CA, USA, January 4-6, 2015*, pages 957–969, 2015.

19 Joël Ouaknine and James Worrell. Positivity Problems for Low-Order Linear Recurrence Sequences. In *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2014, Portland, Oregon, USA, January 5-7, 2014*, pages 366–379, 2014.

20 Andreas Podelski and Andrey Rybalchenko. A Complete Method for the Synthesis of Linear Ranking Functions. In *Verification, Model Checking, and Abstract Interpretation, 5th International Conference, VMCAI 2004, Venice, Italy, January 11-13, 2004, Proceedings*, pages 239–251, 2004.

21 Andreas Podelski and Andrey Rybalchenko. Transition Invariants. In *19th IEEE Symposium on Logic in Computer Science (LICS 2004), 14-17 July 2004, Turku, Finland, Proceedings*, pages 32–41, 2004.

22 G. Rozenberg and A. Salomaa. *Cornerstones of Undecidability*. Prentice Hall, 1994.

23 Arto Salomaa and Matti Soittola. *Automata-Theoretic Aspects of Formal Power Series*. Texts and Monographs in Computer Science. Springer, 1978.

24 M. Soittola. On D0L Synthesis Problem. In A. Lindenmayer and G. Rozenberg, editors, *Automata, Languages, Development*. North-Holland, 1976.

25 Ashish Tiwari. Termination of Linear Programs. In *Computer Aided Verification, 16th International Conference, CAV 2004, Boston, MA, USA, July 13-17, 2004, Proceedings*, pages 70–82, 2004.