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.

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

\[ \text{while } (g_1(x) > 0 \land \ldots \land g_m(x) > 0) \text{ do } x := f(x), \]

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 \(x \in S\). 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 $f(x) = Ax + a$ 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:

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

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:

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

Clearly $\text{conv}(S) \subseteq \text{aff}(S)$. 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 $\text{aff}(S)$. We have the following easy proposition, characterising the relative interior.

▶ Proposition 1. Let $S = \{a_1, \ldots, a_n\} \subseteq \mathbb{R}^d$. If $u$ lies in the relative interior of $\text{conv}(S)$ then there exist $a_1, \ldots, a_n > 0$ such that $u = \sum_{i=1}^{n} a_i a_i$ and $\sum_{i=1}^{n} a_i = 1$.

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

$$(1 + n\varepsilon)u - \sum_{i=1}^{n} \varepsilon a_i \in \text{conv}(S).$$

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

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

$$\Lambda := \{z_1 v_1 + \cdots + z_r v_r : z_1, \ldots, z_r \in \mathbb{Z}\},$$

where $v_1, \ldots, v_r$ 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 $u \in \mathbb{R}^d$ to be

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

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

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 $\Lambda$ 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 $C \cap \mathbb{Z}^d \neq \emptyset$. 

ICALP 2019
2.2 Groups of Multiplicative Relations

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

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

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

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

where \( \gamma^v \) is defined to be \( \gamma_1^{v_1} \cdots \gamma_s^{v_s} \) for \( v \in \mathbb{Z}^s \), that is, exponentiation acts coordinate-wise. Since \( L(\gamma) \) 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.

\[\textbf{Theorem 4 (Masser).} \quad \text{The free Abelian group } L(\gamma) \text{ has a basis } v_1, \cdots, v_l \in \mathbb{Z}^s \text{ for which } \]

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

where \( H \) and \( D \) bound respectively the heights and degrees of all the \( \gamma_i \).

Membership of a tuple \( v \in \mathbb{Z}^s \) in \( L(\gamma) \) 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 \( L(\gamma) \) in polynomial space by brute-force search.

Corresponding to \( L(\gamma) \), we consider the following multiplicative subgroup of \( T^s \):

\[
T(\gamma) = \{ \mu \in T^s : \forall v \in L(\gamma), \mu^v = 1 \}.
\]

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

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

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

\[
\| n\theta - p - \psi \|_{\infty} \leq \varepsilon.
\]

We now arrive at the main result of the section:

\[\textbf{Theorem 6.} \quad \text{Let } \gamma \in T^s. \text{ Then the orbit } \{ \gamma^k : k \in \mathbb{N} \} \text{ is a dense subset of } T(\gamma). \]

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

\[
\| \gamma^k - \mu \|_{\infty} = \| e^{2\pi i (k\theta - p)} - e^{2\pi i \psi} \|_{\infty} \leq \| 2\pi (k\theta - p - \psi) \|_{\infty} \leq 2\pi \varepsilon. \]

\]
3 Termination Analysis via Spectral Theory

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

$$
\text{while } (g_1(x) > 0 \land \ldots \land g_m(x) > 0) \text{ do } x := f(x),
$$

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, $f(x) = Ax + a$ for $A \in \mathbb{Z}^{d \times d}$ and $a \in \mathbb{Z}^d$, and $g_i(x) = b^T_i x + c_i$ for $b_i, c_i \in \mathbb{Z}$ and $i = 1, \ldots, m$.

Note that

$$
\begin{pmatrix}
  f(x) \\
  1
\end{pmatrix} =
\begin{pmatrix}
  A & a \\
  0 & 1
\end{pmatrix}
\begin{pmatrix}
  x \\
  1
\end{pmatrix}
\quad \text{and} \quad
g_i(x) = (b^T_i c_i)
\begin{pmatrix}
  x \\
  1
\end{pmatrix}.
$$

for all $x \in \mathbb{R}^d$. We say that $f$ is non-degenerate if no quotient of two distinct eigenvalues of the update matrix $\begin{pmatrix}
  A & a \\
  0 & 1
\end{pmatrix}$ 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 $\lambda_i / \lambda_j$ 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 $f^L = f \circ \cdots \circ f$ 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:

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

This concludes the proof.

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

$$
P : \text{ while } (g(x) > 0) \text{ do } x \leftarrow f(x) \text{ end}
$$

with a single guard function $g(x) = b^T x + c$ and with non-degenerate update function $f(x) = Ax + a$, 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 $x \in \mathbb{R}^d$ is terminating if there exists $n$ such that $g(f^n(x)) \leq 0$. We say that $x$ is eventually non-terminating if the sequence $\langle g(f^n(x)) : n \in \mathbb{N} \rangle$ is ultimately positive, i.e., there exists $N$ such that for all $n \geq N$ $g(f^n(x)) > 0$. Clearly there exists $z \in \mathbb{Z}^d$ that is non-terminating if and only if there exists $z \in \mathbb{Z}^d$ 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 $\begin{pmatrix}
  A & a \\
  0 & 1
\end{pmatrix}$ and let $k_{\max}$ be the maximum multiplicity over all these eigenvalues.
Define a linear preorder on \( I := \{0, \ldots, k_{\text{max}} - 1\} \times \{1, \ldots, s\} \) by \((i_1, j_1) \preceq (i_2, j_2)\) if either (i) \(|\lambda_{j_1}| < |\lambda_{j_2}|\) or (ii) \(|\lambda_{j_1}| = |\lambda_{j_2}|\) and \(i_1 \leq i_2\). Write \((i_1, j_1) \prec (i_2, j_2)\) if \((i_1, j_1) \preceq (i_2, j_2)\) and \((i_2, j_2) \not\sim (i_1, j_1)\). Then we have

\[
(i_1, j_1) \prec (i_2, j_2) \iff \lim_{n \to \infty} \left( \frac{n}{i} \right)|\lambda_{j_1}|^n = 0,
\]

that is, the preorder \(\preceq\) characterises the asymptotic order of growth in absolute value of the terms \(\left(\frac{n}{i}\right)|\lambda_{j_1}|^n\) for \((i, j) \in I\). This preorder moreover induces an equivalence relation \(\approx\) on \(I\) where \((i_1, j_1) \approx (i_2, j_2)\) if \((i_1, j_1) \preceq (i_2, j_2)\) and \((i_2, j_2) \preceq (i_1, j_1)\).

The following closed-form expression for \(g(f^n(\mathbf{x}))\) 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 \(\mathbf{x} \in \mathbb{R}^d\) and all \(n \geq d\) we have

\[
g(f^n(\mathbf{x})) = \sum_{(i,j) \in I} \binom{n}{i} \lambda_{ij}^n h_{i,j}(\mathbf{x}).
\]

**Proof.** By the Jordan-Chevalley decomposition we can write \(\begin{pmatrix} A & a \\ 0 & 1 \end{pmatrix} = P^{-1}DP + N\), where \(D\) is diagonal, \(N\) is nilpotent, \(P = \text{invertible}, P^{-1}DP\) 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 \(D_1, \ldots, D_s\). Then for all \(n \in \mathbb{N}\) with \(n \geq d\) we have

\[
g(f^n(\mathbf{x})) = (b^\top c) \left(\begin{pmatrix} A & a \\ 0 & 1 \end{pmatrix} \right)^n \left(\begin{pmatrix} x \\ 1 \end{pmatrix}\right)
\]

\[
= (b^\top c) (P^{-1}DP + N)^n \left(\begin{pmatrix} x \\ 1 \end{pmatrix}\right)
\]

\[
= (b^\top c) \sum_{i=0}^{d} \binom{n}{i} P^{-1}D^{n-1}PN^i \left(\begin{pmatrix} x \\ 1 \end{pmatrix}\right)
\]

\[
= (b^\top c) \sum_{i=0}^{d} \binom{n}{i} P^{-1}(\lambda_{1}^{n-1}D_1 + \cdots + \lambda_{s}^{n-1}D_s)PN^i \left(\begin{pmatrix} x \\ 1 \end{pmatrix}\right) \quad (\text{since } N^{d+1} = 0)
\]

\[
= \sum_{j=1}^{s} \lambda_{j}^{n} \sum_{i=0}^{d} \binom{n}{i} \lambda_{j}^{-i}(b^\top c)P^{-1}D_jPN^i \left(\begin{pmatrix} x \\ 1 \end{pmatrix}\right)
\]

\[
= \sum_{j=1}^{s} \sum_{i=0}^{d} \binom{n}{i} \lambda_{j}^{n} h_{i,j}(\mathbf{x}),
\]

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 \(\gamma_i = \frac{\lambda_i}{N_0}\) for \(i = 1, \ldots, s\), that is, we obtain the \(\gamma_i\) by normalising the eigenvalues to have length 1. Recall from Section 2.2 the definition of the group \(L(\gamma)\) of multiplicative relations that hold among \(\gamma_1, \ldots, \gamma_s\), viz.,

\[
L(\gamma) = \{(n_1, \ldots, n_s) \in \mathbb{Z}^s : \gamma_1^{n_1} \cdots \gamma_s^{n_s} = 1\}.
\]
Recall also that we have $T(\gamma) \subseteq T^*$, given by
\[ T(\gamma) = \{ (\mu_1, \ldots, \mu_s) \in T^* : \mu_1^{n_1} \cdots \mu_s^{n_s} = 1 \text{ for all } (n_1, \ldots, n_s) \in L(\gamma) \} . \]

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 $\rho_E$.

Given an $\approx$-equivalence class $E$, define $\Phi_E : \mathbb{R}^d \times T(\gamma) \rightarrow \mathbb{R}$ by
\[ \Phi_E(x, \mu) = \sum_{(i,j) \in E} h_{i,j}(x) \mu_j . \]

From the above definition of $\Phi_E$ we have
\[ \sum_{(i,j) \in E} \binom{n}{i} \lambda_j^n h_{i,j}(x) = \binom{n}{i_E} \rho_E^n \Phi_E(x, \gamma^n) . \]

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

We say that an equivalence class $E$ of $I$ is dominant for $x \in \mathbb{R}^d$ if $E$ is the equivalence class of the maximal indices $(i,j)$ for which $h_{i,j}(x)$ is non-zero. Equivalently, $E$ is dominant for $x$ if $E$ is the maximal equivalence class such that $\Phi_E(x, \cdot)$ is not identically zero on $T(\gamma)$. (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 $x \in \mathbb{R}^d$ can be derived from properties of $\Phi_E(x, \cdot)$.

\begin{proposition}
Consider the loop $P$ in (2). Let $x \in \mathbb{R}^d$ and let $E$ be an $\approx$-equivalence class that is dominant for $x$. Then
\begin{enumerate}
    \item If $\inf_{\mu \in T(\gamma)} \Phi_E(x, \mu) > 0$ then $x$ is eventually non-terminating for $P$.
    \item If $\inf_{\mu \in T(\gamma)} \Phi_E(x, \mu) < 0$ then $x$ is terminating for $P$.
\end{enumerate}
\end{proposition}

\begin{proof}
By Proposition 8 and Equation (5) we have that for all $n \geq d$,
\[ g(f^n(x)) = \sum_{(i,j) \in E} \binom{n}{i} \lambda_j^n h_{i,j}(x) = \binom{n}{i_E} \rho_E^n \Phi_E(x, \gamma^n) + \sum_{(i,j) \in I \setminus E} \binom{n}{i} \lambda_j^n h_{i,j}(x) . \]

Moreover by the dominance of $E$ we have that
\[ \lim_{n \to \infty} \binom{n}{i} \rho_E^n = 0 \]

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

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

\end{proof}

\footnote{That the function $\Phi_E$ is real-valued follows from the fact that if eigenvalues $\lambda_{j_1}$ and $\lambda_{j_2}$ are complex conjugates then $\gamma_{j_1}$ and $\gamma_{j_2}$ are also complex conjugates, as are $h_{i,j_1}(z)$ and $h_{i,j_2}(z)$ (see the proof of Proposition 8).}
We turn now to Item 2. By assumption there exists \( \varepsilon > 0 \) and an open subset \( U \) of \( T(\gamma) \) such that \( \Phi_E(x, \mu) < -\varepsilon \) for all \( \mu \in U \). Moreover by density of \( \{ \gamma^n : n \in \mathbb{N} \} \) in \( T(\gamma) \) there exist infinitely many \( n \) such that \( \gamma^n \in U \). Exactly as in Case 1 we can now use the dominance of \( E \) to conclude that \( g(f^n(x)) < 0 \) for sufficiently large \( n \) such that \( \gamma^n \in U \) and hence \( x \) is terminating.

Given \( z \in \mathbb{Z}^d \), since \( T(\gamma) \) is an algebraic subset of \( \mathbb{T}^s \), the number \( \inf_{\mu \in T(\gamma)} \Phi_E(z, \mu) \) 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 \( z \). Indeed, let us define \( z \in \mathbb{R}^d \) to be critical if \( \inf_{\mu \in E} \Phi_E(z, \mu) = 0 \), where \( E \) is the dominant equivalence class for \( z \). Then neither clause in the above proposition suffices to resolve termination of the loop \( P \) in (2) on such a \( z \). 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 \( x \in \mathbb{R}^d \) is critical then \( f(x) \) should also be critical. This, and more, follows from the following proposition.

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

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

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

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

\[
(b^Tc) \begin{pmatrix} A & a \\ 0 & 1 \end{pmatrix}^{n+1} \begin{pmatrix} x \\ 1 \end{pmatrix} = \sum_{(i,j) \in I} \tilde{h}_{i,j}(x) \binom{n+1}{i} \lambda_j^n \tag{9}
\]

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

\[
\sum_{(i,j) \in I} \tilde{h}_{i,j}(x) \binom{n}{i} \lambda_j^n = \sum_{(i,j) \in I} h_{i,j}(x) \binom{n+1}{i} \lambda_j^{n+1} = \sum_{(i,j) \in I} h_{i,j}(x) \left( \binom{n}{i} + \binom{n}{i-1} \right) \lambda_j^n.
\]
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 \( \mathbb{C}^N \) (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 \( \bar{h}_{i,j} = \lambda, h_{i,j} = \rho E \gamma_j h_{i,j} \) for all \((i, j) \in E \); likewise we have that \( E \) is dominant for \( f(x) \). 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 \( z \in \mathbb{R}^d \) is critical then there exists a positive integer \( M \) such that for all \( n \geq M \), all points in the relative interior of \( \text{conv}(\{f^d(z), f^{d+1}(z), \ldots, f^n(z)\}) \) are eventually non-terminating.

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

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

By Proposition 1, for all \( n \geq M \) and all points \( x \) lying in the relative interior of \( \text{conv}(\{f^d(z), f^{d+1}(z), \ldots, f^n(z)\}) \), there exist \( \alpha_d, \ldots, \alpha_n > 0 \) such that \( \sum_{i=d}^n \alpha_i = 1 \) and \( x = \sum_{i=d}^n \alpha_i f^i(z) \). Since \( \Phi_E \) is an affine map in its first variable, it follows that \( \Phi_E(x, \cdot) = \sum_{i=d}^n \alpha_i \Phi_E(f^i(z), \cdot) \) is strictly positive on \( T(\gamma) \). Hence \( x \) 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 \( z_* \in \mathbb{Z}^d \), we show that for \( n \) sufficiently large, the set

\[
\text{conv}(\{f^d(z_*), f^{d+1}(z_*), \ldots, f^n(z_*)\})
\]

contains an integer point in its relative interior.

Define \( V := \text{Aff}(\{f^n(z_*) : n \geq d\}) \) 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 \( v \in V_0 \) the set \( \{|v^\top f^n(z_*)| : n \geq d\} \) is unbounded.

**Proof.** Consider the sequence \( x_n := v^\top f^n(z_*) = \begin{pmatrix} A & a \\ 0 & 1 \end{pmatrix}^n \begin{pmatrix} z_* \\ 1 \end{pmatrix} \). If this sequence were constant then \( v \) would be orthogonal to \( V_0 \), contradicting the fact that \( v \) 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 \( \{ v^T f^n(z_*) \} : n \geq d \) is unbounded (see the discussion of growth of linear recurrence in [13, Section 2.2]).

\[ \textbf{Proposition 13.} \text{ There exists } M \text{ such that for all } n \geq M \text{ the set} \]

\[ \text{conv}(\{ f^d(z_*), f^{d+1}(z_*), \ldots, f^n(z_*) \}) \]

\textit{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 \( C := \text{conv}(\{ f^n(z_*): n \geq d \}) \subseteq V \) and \( C_0 := C - f^d(z_*) \subseteq V_0 \).

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 \( v \in \theta(\Lambda) \) we have

\[ v^T(\theta(f^n(z_*)) - \theta(f^d(z_*))) = (v^* v) f^n(z_*) - f^d(z_*) \text{,} \tag{10} \]

where \( \theta^* : \mathbb{R}^{d_0} \to \mathbb{R}^d \) is the adjoint map of \( \theta \). But \( \theta^* v \) 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 \( \Lambda \) (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.

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

**Proof.** If no such \( z \) exists then the loop is terminating by Proposition 9(2). Conversely, if such a \( z \) exists then by Lemma 11 and Proposition 13 there exists \( z' \in \mathbb{Z}^d \) such that

\[ \inf_{\mu \in T(\gamma)} \Phi_E(z', \mu) > 0 \text{ (and with } E \text{ still dominating for } z'). \]

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 \( x_{\ell \cdot p}, x_{\ell \cdot p + 1}, \ldots, x_{\ell \cdot p + m} \) for some \( \ell, p \geq 1 \). In particular, if \( m = d \) then since every infinite subsequence \( y_n := x_{\ell \cdot p n} \) satisfies a linear recurrence of order at most \( d + 1 \), \( \langle y_n : n \in \mathbb{N} \rangle \) would have an infinite constant subsequence \( \langle x_{\ell \cdot p n} : n \in \mathbb{N} \rangle \). 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

\[ Q : \text{while } (g_1(x) > 0 \land \ldots \land g_m(x) > 0) \text{ do } x := f(x), \]

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

\[ Q_i : \text{while } (g_i(x) > 0) \text{ do } x := f(x), \]

for \( i = 1, \ldots, m \). Clearly \( Q \) is non-terminating if and only if there exists \( z \in \mathbb{Z}^d \) such that each loop \( Q_i \) is non-terminating on \( z \). 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 \( \Phi_{E_i}^{(i)} : \mathbb{R}^d \times T(\gamma) \to \mathbb{R} \) 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 \( \gamma \in \mathbb{R}^d \) such that the following hold for \( i = 1, \ldots, m \):

- \( E_i \) is dominant for \( z \) in loop \( Q_i \), that is, \( \Phi_{E_i}^{(i)}(z, \cdot) \neq 0 \) and \( \Phi_{E_i}^{(i)}(z, \cdot) \equiv 0 \) for all \( E_i \approx E \).
- \( \inf_{\mu \in T(\gamma)} \Phi_{E_i}^{(i)}(z, \mu) \geq 0 \).

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

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

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 \( \approx \) among eigenvalues.
3. Compute a basis of the group of multiplicative relations \( L(\gamma) \).
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 \( L(\gamma) \) reduces to checking a finite collection of multiplicative relations among algebraic numbers. Given a basis of \( L(\gamma) \) 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.
118:12 Termination of Linear Loops over the Integers

References


