On Termination and Divergence of Linear Programs

Mehran Hosseini

Linacre College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

Trinity 2021

To those who inspired it,
my parents and my brother.

Acknowledgements

There are no words that can express my gratitude towards my supervisors, Ben Worrell and Joël Ouaknine. I could not have asked for more during my DPhil at Oxford. During the last four years, I learned many things from both of you; I learned beyond academic skills; I learned how to be a better person.

I would also like to greatly thank Stefan Kiefer (Transfer, Confirmation, and Viva), Christoph Haase (Transfer), Paul Goldberg (Confirmation), and Thomas Brihaye (Viva), who assessed my progress during my DPhil, for their valuable comments, and for the time they dedicated to making it possible for me to be here writing the last lines of my thesis.

Next, I would like to thank Reino Niskanen for his feedback on my thesis and valuable collaboration during the last two years. I was also very fortunate to have had Alessandro, Mahsa, Shaull, George, Nikhil, Engel, Pavel, and Edon as my friends and colleagues.

I like to thank my extended family for their extensive support, especially during the lock-down. I also like to express my gratitude towards Sajjad, Mojtaba, and Mohammad, for their continuous support since my early years of my undergraduate studies at the Isfahan University of Technology.

Last but not least, I would like to deeply thank

my friends in computer science: Nathalie, Simin, Andrea, Elizabeth, Paul, Brian, Gareth, Damian, Khaza, Hosein, Francesco, Ada, Qiyi, Martin, Will, Min, Shadi, Dongxia, Andrius, Amir, Ninad, Milad, and Julian,

my friends from the Oxford University Iranian Society: Fatimah, Mahan, Hamideh, Saeed, Mehdi, Henry, Natsunu, and Kiana,

and my Linacre family: Xiaoyi, Oana, Farhana, Pete, Zuzana, Karrar, Luke, Peter, Alex, Omar, Joseph, Misha, Isabel, Nyree, Shahé, Ashley, Angad, Filip, Artur, Matthias, Louis, Vinayak, Huihui, Kai, Daniel, Sumedha, and CJ.

Finally, I am obliged to acknowledge that, without the generous funding of the European Research Council (grant AVS-ISS (648701)) I would have not been able to conduct the research that led to this thesis.

Abstract

The objective of this thesis is to shed some light on the boundaries of decidability by answering some of the central problems in the study of linear programs, and to provide an up-to-date survey of the latest results in this field.

In particular, we review some of the classical decision problems in the theory of linear recurrence sequences. Namely, we revisit the Skolem Problem, Positivity Problem, Ultimate Positivity Problem, and Absolute Divergence Problem. We then show that the Divergence Problem, the problem of deciding whether a given linear recurrence sequence diverges to infinity, is decidable for all linear recurrence sequences of order at most 5, and when the linear recurrence sequence is simple it is decidable up to order 8. Our results hold for both homogeneous and inhomogeneous linear recurrence sequences. As a by-product of our approach, we extend existing results on the Positivity Problem and Ultimate Positivity Problem for homogeneous linear recurrence sequences to inhomogeneous linear recurrence sequences. We further demonstrate why it is unlikely to improve these decidability boundaries to higher order linear recurrence sequences, by establishing reductions from long-lasting open problems in Diophantine Approximation.

Next, we answer a 15-year-old problem of Tiwari, which asks whether a given linear loop program with integer coefficients terminates over all its integer initial values. We use novel techniques to evade the obstacles in answering the Positivity and Ultimate Positivity Problems. In more detail, we exploit the freedom to choose the initial value to circumvent the need to solve "hard instances" of the Positivity Problem. Our algorithm decides, in double exponential space, whether a linear loop program with integer coefficients terminates over all integer initial values.

Finally, we summarise the state-of-the-art results in the field, and provide the reader with a landscape of some of the new and classical open problems

in the field. We also discuss some of the shortcomings of the current approaches, and provide direction for further research.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Program verification is a pivotal part of computer science. Nevertheless, as soon as one goes beyond basic models of computation, such as finite automata or push-down automata, program verification soon becomes nearly impossible; in fact, in its general form, program verification is undecidable as it encompasses the *Halting Problem* for *Turing machines*, the problem of deciding whether a given Turing machine terminates on a given input.

Determining boundaries of decidability and undecidability in program verification has drawn the attention of computer scientists for many decades. One class of programs that lies on this boundary is the class of deterministic *linear programs*, programs in which variables are updated by a *linear* or *affine* update function.

In particular, it takes very little beyond deterministic linear programs for problems such as the Termination Problem to become undecidable. For instance, if one permits polynomial updates of variables (as opposed to linear updates), deciding several properties of such programs, such as termination and finiteness of the reachable set are undecidable [66]. Even introducing *the slightest* non-determinism will take us to the realm of undecidability. Termination of counter machines [22] and piecewise linear programs [99, 19], as well as the matrix semi-group membership problem [64, 79, 10] are all examples of classes of non-deterministic linear programs for which termination is undecidable.

The goal of this thesis is to shed some light on the boundaries of decidability and undecidability through investigating two types of deterministic linear programs. We push some of the current decidability boundaries, and reveal some of the barriers to better understanding these programs.

Linear programs are one of the frequently-used building blocks of more complex programs used in science and engineering. Despite being one of the most well-studied families of program, and the numerous mathematical tools available for studying them,

many fundamental questions about linear programs remain open. We will focus on two types of linear programs in this thesis.

Chapter 3 is dedicated to the study of *Linear Recurrence Sequences (LRS)* over rational numbers. An LRS over rational numbers is a sequence $\mathbf{u} = \langle u_n \rangle_{n=0}^{\infty}$, defined by a recurrence relation

$$u_{n+k} = a_1 u_{n+k-1} + \cdots + a_{k-1} u_{n+1} + a_k u_n + a_{k+1},$$

where $a_1, \ldots, a_{k+1} \in \mathbb{Q}$ are constants. For the sake of brevity, in the rest of this thesis, we use LRS to refer to LRS over rational number, unless otherwise stated.

Linear recurrence sequences describe numerous natural phenomena, and are used in a wide range of scientific areas such as biology [58], economics [9], quantum computing [20, 37], etc. Perhaps, the most well-known example of LRS is the sequence

$$0, 1, 1, 2, 3, 5, 8, 13, \ldots$$

defined by the recurrence

$$f_{n+2} = f_{n+1} + f_n,$$

and initial conditions $f_0 = f_1 = 0$. This sequence is called the *Fibonacci Sequence* after the twelfth century Italian mathematician, Leonardo of Pisa [81]. Earlier records of studying the Fibonacci Sequence go back to the tenth and eleventh century by Persian mathematicians Al-Karaji [93, 85, 95] and Khayyám [34, 92, 49] in their study of Pascal's triangle. There is even evidence that the Fibonacci sequence was used in 200 BC India for enumerating possible patterns of Sanskrit poetry formed from syllables of two lengths [53, 40, 96].

Since the beginning of the twentieth century, due to their applications in sciences and the industry, more attention has been paid to the computational aspects of LRS. *Skolem Problem*, which asks whether an LRS $\mathbf{u}$ ever attains 0, is arguably the most famous open problem about LRS, having remained open since the 1930s [97].

Motivated by the applications in biology and economics, in Chapter 3, we will study the *Divergence Problem* for LRS [60, 8]. The Divergence Problem asks whether a given LRS $\mathbf{u}$ diverges to $+\infty$ and is equivalent to deciding divergence to $-\infty$. We will show that the Divergence Problem is decidable for low-order LRS. In fact, we will show that the Divergence problem is decidable for LRS of order at most 5, or, if the LRS is simple, of order at most 8 in polynomial time. Moreover, we provide fine-grained lower bounds on the rate of divergence. Furthermore, in Subsection 3.2.2, we show why it is unlikely to improve these lower-bounds, via reduction from some long-standing open problems in Diophantine approximations.

We also consider the *Positivity Problem*, the problem of deciding whether an LRS $\mathbf{u}$ is always positive, and the *Ultimate Positivity Problem*, the problem of deciding whether the LRS $\mathbf{u}$ is eventually always positive. In particular, We extend the decidability results as well as the lower bounds in [76, 77, 75] to inhomogeneous LRS.

Chapter 4 is devoted to the study of *single-path affine loop programs*. Single-path affine loop programs, or affine loops for short, are programs of the form

$$\mathsf{P} : \textit{while } (B\boldsymbol{x} > \boldsymbol{b}) \textit{ do } \boldsymbol{x} := A\boldsymbol{x} + \boldsymbol{c}\,.$$

When $\boldsymbol{b} = 0$ and $\boldsymbol{c} = 0$, the program is called *linear* or *homogeneous*. In the rest of this thesis, when we use the term "affine loops", we are referring to single-path affine loop programs.

Affine loops can be regarded as a different representation of LRS as we discuss this in Subsection 4.1.1. The Termination Problem of the loop P on a given input $\boldsymbol{x}$ is equivalent to the Positivity Problem for LRS. In fact, these two problems are inter-reducible in polynomial time (see Subsection 4.1.1).

Therefore, the lower bounds for the Positivity Problem (See [76] and also Subsection 3.3.3) leave *little* hope for solving the Termination Problem for affine loops over a fixed initial value $\boldsymbol{x}$. This ineptness is, perhaps, best described by the ingenious mathematician, Terence Tao as "it is saying that we do no know how to decide the Halting Problem for "linear" automata!" [100].

The situation for the Universal Termination Problem for affine loops, however, is somewhat brighter. By studying the spectral space of the update matrix A, Tiwari showed that the Universal Termination Problem is decidable for affine loops [102] when the variable $\boldsymbol{x}$ ranges over all possible real initial values, in **PTIME**. Furthermore, he conjectured that the Universal Termination Problem for affine loops is decidable over rational numbers and integers [102].

Braverman, two years later, proved Tiwari's conjecture over rational numbers, and, when the loop is homogeneous over the integers. Further progress had to wait another eight years, when Ouaknine et al. showed that when the update matrix A is diagonalisable, universal termination over integers can be solved.

In Chapter 4, we fully settle Tiwari's conjecture by devising a procedure for deciding the Universal Termination Problem of affine loops over the integers, solving this 15-year-old open problem. To achieve this result, we make use of tools from geometry of numbers, algebraic geometry, algebraic number theory, Diophantine approximation, and real algebraic geometry (see Subsubsection 4.1 for a more in-detail summary of tools that we use in Chapter 4).

Chapter 2

Mathematical Background

In this chapter, we introduce several tools and notations that will be used throughout this thesis starting with introducing the notations used in Subsubsection 2.1. Sections 2.2, 2.3, 2.4, 2.6, and 2.5 will give a basic introduction to the results we use from linear algebra, number theory, logic, linear recurrence sequences, and real algebraic geometry, respectively.

2.1 Notations

We will, for the most part, follow the standard notations in mathematics and computer science. We use blackboard bold letters $\mathbb{C}, \mathbb{T}, \mathbb{R}, \mathbb{Q}$, and $\mathbb{Z}$ to denote the sets of complex numbers, unit complex numbers, real numbers, rational numbers, and integers, respectively. The symbol $\mathbb{N}$ is used to denote the set of non-negative integers $\{0, 1, 2, \ldots\}$. Note that some literature uses $\mathbb{N}$ to denote the set of positive integers. For a set S, $\bar{S}$ indicates either the algebraic closure or topological closure of the set S; the meaning will be clear from the context. To represent an infinite sequence $u_0, u_1, u_2, u_3, \ldots$, we use the notation $\langle u_n \rangle_{n=0}^{\infty}$.

For a ring R, we represent the set of univariable polynomials with coefficients in R with $R[x]$. The notation $\|\cdot\|$ is used to present either the length of a binary representation of a mathematical object or the Euclidean norm of a vector; in either case, the purpose should be clear from the context. We use the standard notation $|z|$ to denote the modulus of a complex number z. We use $\log(\cdot)$ to indicate the natural logarithm of real numbers, while $\mathrm{Log}(\cdot)$ is preserved for the principal branch of the complex natural logarithm.

For vector spaces V and W over a field $\mathbb{F}$, we use $\mathrm{Hom}(V, W)$ to indicate the vector space of linear maps from V to W. This should not be confused with the operator $\textsc{hom}(\cdot)$ that is used to homogenise linear recurrence sequences.

Let $x \in \mathbb{R}$ be any real number. We say that x is computable if there is an algorithm which, given any rational $\epsilon > 0$ as input, returns a rational number q such that $|q - x| < \epsilon$. Note that not all real number are computable because there are only countably many Turing machines over a given alphabet, whereas there are uncountably many real numbers. Chaitin's constant [29], as explained in [36], is one such number. Given $y \in \mathbb{R}$, the notation $[x]_y$ denotes the distance from x to the closest integer multiple of y.

We use italic letters such as x to refer to scalars (scalar variables), while we use bold italic letter such as $\boldsymbol{x}$ to refer to vectors (vector variables). We also use $\mathbf{0}$ to represent all zero vectors $(0, \ldots, 0)^\top$. Bold letters such as $\mathbf{u}$ are reserved for representing linear recurrences sequences.

We use the *Turing Machine* (*TM*) model of computation. Furthermore, we use the following conventional notations to indicate the complexity classes used throughout this thesis.

Notation	Description
PTIME	The class of all decision problems that are solvable in polynomial time using a TM
PSPACE	The class of all decision problems that are solvable in polynomial space using a TM
EXPSPACE	The class of all decision problems that are solvable in exponential space using a TM
2-EXPSPACE	The class of all decision problems that are solvable in double exponential space using a TM
NP	The class of all decision problems that are solvable in polynomial time using a non-deterministic TM
NP-Hard	The class of all decision problems that are at least as hard as the problems in **NP**
coNP	The class of all decision problems whose complement is solvable in **NP**
PosSLP	The class of all decision problems that are reducible in polynomial time to the following problem: *Given a division-free straight-line program*[1] *producing an integer N, decide whether $N > 0$*
$\mathbf{coNP^{PosSLP}}$	The class of all decision problems that are solvable in **coNP** with oracle access to **PosSLP**

Table 2.1: Complexity Classes Notations

[1] A *straight-line program* is a sequence of instructions corresponding to a sequential evaluation of an arithmetic circuit. An *arithmetic circuit* is a directed acyclic graph with input nodes labelled with the constants 0, 1 or with indeterminates $X_1, \ldots, X_k$ for some $k \in \mathbb{N}$. Internal nodes are labelled with one of the operations $+, -, *, \div$. If the program contains no $\div$ operation, it is said to be *division-free*.

2.2 Linear Algebra

We will extensively use tools from linear algebra throughout this thesis. We briefly present some of these tools in this section. An interested reader can find more details on matrix analysis and linear algebra in [67, chapter 7].

2.2.1 Cayley–Hamilton Theorem

For a given square matrix $A \in \mathbb{C}^{d\times d}$, *the characteristic polynomial* is defined as

$$\chi_A(x) = \det(xI_d - A),$$

where I_d is the identity matrix of size d. Note that χ_A is a polynomial of degree d.

Theorem 1 (Cayley–Hamilton)**.** *Given a square matrix $A \in \mathbb{C}^{d\times d}$, A satisfies its characteristic polynomial χ_A. In other words, $\chi_A(A) = 0$.*

The characteristic polynomial of A, χ_A, is not necessarily the lowest-degree polynomial that annihilates A. The unique monic polynomial that annihilates A and has the least degree is called *minimal polynomial* of A. We will denote the minimal polynomial of A as m_A.

2.2.2 Eigenvalues and Eigenvectors of a Matrix

The fundamental theorem of algebra states that every monic univariable polynomial $p(x) \in \mathbb{C}[x]$ can be written as a unique product (up to permutation) of monic linear terms [1, chapter 2]. Let A be any complex square matrix. By the fundamental theorem of algebra, we have

$$\chi_A(x) = (x - \lambda_1)^{n_1} \cdots (x - \lambda_s)^{n_s},$$

where λ_i is a root of χ_A of multiplicity n_i for all $1 \le i \le s$. Each λ_i is called an *eigenvalue* of the matrix A. We also say that a complex vector $\boldsymbol{v}_i$ is an *eigenvector* of A corresponding to λ_i if $A\boldsymbol{v}_i = \lambda_i \boldsymbol{v}_i$.

2.2.3 Linear Independence of Exponential Monomials

Let $\lambda_1, \ldots, \lambda_m \in \mathbb{C}$ be distinct complex numbers and $e_1, \ldots, e_m$ positive integers. Then the family of *exponential-polynomial* functions $p_{i,j} : \mathbb{N} \to \mathbb{C}$, for $j \in \{1, \ldots, m\}$ and $i \in \{0, \ldots, e_j - 1\}$, given by $p_{i,j}(n) = \binom{n}{i}\lambda_j^n$ is linearly independent over $\mathbb{C}$. Moreover if $p : \mathbb{N} \to \mathbb{C}$ is a $\mathbb{C}$-linear combination of the $p_{i,j}$, then p is identically zero if and only

if $p(n) = 0$ for $e_1 + \cdots + e_m$ consecutive values $n \in \mathbb{N}$. Both of the above facts can be proved using generalised Vandermonde determinants [42, Proposition 2.11]. We will use these facts in studying termination of integer linear loops in Subsection 4.2.2.

2.2.4 Jordan-Chevalley Decomposition

Theorem 2. *Let $L : V \to V$ be a linear operator on a d-dimensional complex vector space over a perfect field, i.e., any field $\mathbb{F}$ of characteristic 0 (such as $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$), or, prime characteristic p whose elements are all p-th powers. Then, there exist linear maps $S, N : V \to V$, with S diagonalisable and N nilpotent (with nilpotency index at most d), such that $L = S + N$ and $SN = NS$.*

For the proof and more details see [80, section 2.8].

2.2.5 Dual Space of a Vector Space

For a vector space V over a field $\mathbb{F}$, we define the *dual vector space* $V^* = \mathrm{Hom}(V, \mathbb{F})$ as the set of linear functions $\phi : V \to \mathbb{F}$ [80, section 1.14].

2.2.6 Adjoint of a Linear Map

For a linear map $\theta : \mathbb{F}^d \to \mathbb{F}^{d'}$, where $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, and $\mathbb{F}^d$ and $\mathbb{F}^{d'}$ are equipped with their standard inner products, we define the *adjoint* of θ as follows. We can write θ as a $d' \times d$ matrix and define the adjoint $\theta^* = \bar{\theta}^\top$, i.e., θ^* is the conjugate transpose of θ. In case $\mathbb{F} = \mathbb{R}$, conjugation has no effect, so $\theta^* = \theta^\top$. Note that since θ^* is a $d \times d'$ matrix, it corresponds to a linear map $\theta^* : \mathbb{F}^{d'} \to \mathbb{F}^d$. This matrix adjoint satisfies the crucial property

$$\boldsymbol{v}^\top \theta \boldsymbol{u} = (\theta^* \boldsymbol{v})^\top \boldsymbol{u},$$

for all $\boldsymbol{u} \in \mathbb{F}^d$ and $\boldsymbol{v} \in \mathbb{F}^{d'}$ [80, section 3.5].

2.3 Number Theory

2.3.1 Algebraic Numbers

A complex number α is *algebraic* if it is a root of a polynomial $p \in \mathbb{Z}[x]$. The *defining polynomial* of α, denoted p_α, is the unique polynomial of the least degree that vanishes at α, and whose coefficients do not have common factors other than ± 1. The *degree* and the *height* of α are the degree and the height (i.e., the maximum absolute value of the coefficients) of p_α, respectively. An algebraic number α can be represented by

a polynomial that has α as a root, along with an approximation of α by a complex number with rational real and imaginary parts. We denote by $\|\alpha\|$ the representation length of α. Basic arithmetic operations as well as equality testing and comparisons for algebraic numbers can be carried out in polynomial time (see [23, 31] for efficient algorithms).

2.3.2 Logarithm Forms

The following lemma from [76] is a consequence of the celebrated lower bound for linear forms in logarithms due to Baker and Wüstholz [6].

Lemma 3. *There exists $D \in \mathbb{N}$ such that, for all algebraic numbers $\lambda, \zeta \in \mathbb{C}$ of modulus 1, and for all $n \geq 2$, if $\lambda^n \neq \zeta$, then $|\lambda^n - \zeta| > \frac{1}{n^{(\|\lambda\|+\|\zeta\|)^D}}$.*

2.3.3 Asymptotic Analysis of Arithmetic of Algebraic Numbers

We have the following simple lemma from [76].

Proposition 4. *Let $a \geq 2$ and $\epsilon \in (0,1)$ be real numbers. Let $B \in \mathbb{Z}[x]$ have degree at most a^{D_1} and height at most $2^{a^{D_2}}$, and assume that $1/\epsilon \leq 2^{a^{D_3}}$ for some $D_1, D_2, D_3 \in \mathbb{N}$. Then there is $D_4 \in \mathbb{N}$ depending only on D_1, D_2, D_3 such that for all $n \geq 2^{a^{D_4}}$, $\frac{1}{B(n)} > (1-\epsilon)^n$.*

2.3.4 Groups of Multiplicative Relations of Algebraic Numbers

In this subsection we will introduce some concepts concerning groups of multiplicative relations among algebraic numbers. These groups occur frequently in studying linear recurrence sequences (for instance see subsubsection 3.2.1.2).

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 $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_s) \in \mathbb{T}^s$, the orbit $\{\boldsymbol{\gamma}^n : n \in \mathbb{N}\}$, where $\boldsymbol{\gamma}^n$ is defined to be $(\gamma_1^n, \ldots, \gamma_s^n)$, 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 [65] gives bounds on the magnitude of the components of such a basis.

Theorem 5 (Masser)**.** *The free Abelian group $L(\boldsymbol{\gamma})$ has a basis $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_l \in \mathbb{Z}^s$ 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 time, using exponentiation by repeated squaring method. In combination with Theorem 5, it follows that we can compute a basis for $L(\boldsymbol{\gamma})$ in polynomial space by brute-force search, i.e., by trying all possible linearly independent $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_l \in \mathbb{Z}^s$ such that

$$\max_{1 \le i \le l, 1 \le j \le s} |v_{i,j}| \le (D \log H)^{O(s^2)}, \text{ and } \boldsymbol{v} \in L(\boldsymbol{\gamma}).$$

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 6. *Let $\boldsymbol{\theta}, \boldsymbol{\psi} \in \mathbb{R}^s$. Suppose that for all $\boldsymbol{v} \in \mathbb{Z}^s$, if $\boldsymbol{v}^\top \boldsymbol{\theta} \in \mathbb{Z}$ then also $\boldsymbol{v}^\top \boldsymbol{\psi} \in \mathbb{Z}$, 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 7. *Let $\boldsymbol{\gamma} \in \mathbb{T}^s$. Then the orbit $\{\boldsymbol{\gamma}^k : k \in \mathbb{N}\}$ 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 $\boldsymbol{v}^\top \boldsymbol{\theta} \in \mathbb{Z}$. 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 $\|k\boldsymbol{\theta} - \boldsymbol{p} - \boldsymbol{\psi}\|_\infty \leq \varepsilon$. Whence

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

□

2.3.5 Transcendental Numbers

A complex number α that is not algebraic is called *transcendental*. Real transcendental numbers constitute the majority of real numbers; In fact, the set of algebraic numbers is countable and has Lebesgue measure zero.

Despite their abundance on the real line, many of the properties of the transcendental numbers are still unknown. However, there are some results that connect the transcendental numbers to the better-known algebraic numbers. We will use one such theorem, which was independently discovered by Gelfond and Schneider, in Subsection 3.3.3.

Theorem 8 (Gelfond-Schneider)**.** *If α and β are algebraic numbers with $\alpha \neq 0, 1$, and β irrational, then any value of α^β is a transcendental number.*

2.3.6 Diophantine Approximation

For any $x \in \mathbb{R}$, the *Lagrange constant* (or *homogeneous Diophantine approximation constant*) of x is defined as

$$L_\infty(x) = \inf\{c \in \mathbb{R} : |x - \frac{n}{m}| \leq \frac{c}{m^2} \text{ for infinitely many } m, n \in \mathbb{Z}\}.$$

We also define the *(homogeneous Diophantine) approximation type* of x as

$$L(x) = \inf\{c \in \mathbb{R} : |x - \frac{n}{m}| \leq \frac{c}{m^2} \text{ for some } m, n \in \mathbb{Z}\}.$$

Khinchin showed in 1926 that almost all real numbers (in the measure-theoretic sense) have Lagrange constant and type equal to zero. Yet real numbers with non-zero Lagrange constant constitute an uncountable class known as the *badly approximable* numbers. The Lagrange constant and type of a real number x are closely linked to the continued fraction expansion of x, a fact which enabled Euler to prove that all algebraic numbers of degree 2 are badly approximable.

An old observation of Dirichlet shows that every real number has Lagrange constant at most 1. This bound was improved to $1/\sqrt{5}$ by Hurwitz in 1891, who also showed

that this bound is achieved by the golden ratio. Markov proved in 1879 that every transcendental real number x has $L_\infty(x) \in [0, 1/3]$. Considerable further work has been devoted to the study of the Lagrange spectrum, which records the possible values taken on by Lagrange constants—see, e.g., [35]. Despite this, nothing further is known about the Lagrange constant or type of the vast majority of transcendental numbers; for example, it is a long-standing open problem as to whether $L_\infty(\pi)$ is $0, 1/3$, or some value in between. See [71] for comprehensive references and [5, 87, 91] for detailed explanations.

2.3.7 Geometry of Numbers

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:

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

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:

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

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

Proposition 9. *Let $S = \{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n\} \subseteq \mathbb{R}^d$. If $\boldsymbol{u}$ lies in the relative interior of $\mathrm{conv}(S)$ 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 $\mathrm{conv}(S)$, for $\varepsilon > 0$ sufficiently small we have that

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

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

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

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 [7, 51]) captures the intuition that a convex set that contains no lattice point in its interior must be "thin" in some direction.

Theorem 10 (Flatness Theorem)**.** *Given a full-rank lattice Λ in $\mathbb{R}^d$ there exists W such that any convex set $C \subseteq \mathbb{R}^d$ that has non-empty interior and lattice width at least W contains a lattice point in its interior.*

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 11 (Khachiyan and Porkolab [50])**.** *It is decidable whether a given convex semi-algebraic set $C \subseteq \mathbb{R}^d$ contains an integer point; that is, whether $C \cap \mathbb{Z}^d \neq \emptyset$.*

2.4 Logic

2.4.1 The First-Order Theory of the Reals

A sentence in the first-order theory of the reals is of the form

$$Q_1 x_1 \cdots Q_m x_m \phi(x_1, \ldots, x_m)$$

where each Q_i is a quantifier ($\exists$ or $\forall$), each x_i is a real valued variable, and ϕ is a Boolean combination of atomic predicates of the form $p(x_1, \ldots, x_m) \sim 0$ for some $p \in \mathbb{Z}[x_1, \ldots, x_m]$ and $\sim \in \{>, =\}$. The *degree* (resp. *height*) of a first-order formula is defined to be the maximum of the degrees (resp. heights) of all the polynomials appearing in the formulae. The first-order theory of the reals admits quantifier elimination, a famous result due to Tarski [101], whose procedure unfortunately has non-elementary complexity. In this thesis we consider only the case where the number of variables is uniformly bounded. Hence we can invoke the following result due to Renegar [86].

Theorem 12 (Renegar)**.** *Let $M \in \mathbb{N}$ be fixed. Let $\tau(\boldsymbol{y})$ be a formula of the first-order theory of the reals. Assume that the number of (free and bound) variables in $\tau(\boldsymbol{y})$ is bounded by M. Denote the degree of $\tau(\boldsymbol{y})$ by d and the number of atomic predicates in $\tau(\boldsymbol{y})$ by n.*

There is a polynomial time (polynomial in $\|\tau(\boldsymbol{y})\|$) procedure which computes an equivalent quantifier-free formula

$$\chi(\boldsymbol{y}) = \bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} h_{i,j}(\boldsymbol{y}) \sim_{i,j} 0,$$

where each $\sim_{i,j}$ is either $>$ or $=$, with the following properties:

1. *Each of I and J_i (for $1 \leq i \leq I$) is bounded by $(n+d)^{O(1)}$.*
2. *The degree of $\chi(\boldsymbol{y})$ is bounded by $(n+d)^{O(1)}$.*
3. *The height of $\chi(\boldsymbol{y})$ is bounded by $2^{\|\tau(\boldsymbol{y})\|(n+d)^{O(1)}}$.*

2.5 Foundations of Linear Recurrence Sequences

We now turn to present three results regarding the asymptotic analysis of linear recurrence sequences. We postpone the formal definition of a linear recurrence sequence to Subsubsection 3.1. Nevertheless, we state some of the basic terminology and well-known results here.

Remember from Chapter 1 that a linear recurrence sequence is a sequence $\mathbf{u} = \langle u_n \rangle_{n=0}^{\infty}$ such there exist a positive integer k and numbers $a_1, \ldots, a_{k+1}$ such that

$$u_{n+k} = a_1 u_{n+k-1} + \cdots + a_{k-1} u_{n+1} + a_k u_n + a_{k+1}$$

In Subsubsection 3.1, we explain that associated to the LRS $\mathbf{u}$, there exist algebraic numbers $\lambda_1, \ldots, \lambda_m$, called characteristic roots of $\mathbf{u}$. If all of these characteristic roots have multiplicity one, then $\mathbf{u}$ is called simple, and if the ratio of no two characteristic roots is a root of unity, then $\mathbf{u}$ is called non-degenerate.

Every LRS $\mathbf{u}$ has an *exponential polynomial* representation [42]. In other words, the n-th term of the LRS $\mathbf{u}$ can be expressed as

$$u_n = \sum_{i=1}^{m} C_i(n) \lambda_i^n, \tag{2.1}$$

where $C_1, \ldots, C_m \in \mathbb{C}[n]$, the ring of polynomials over the variable n with coefficients in $\mathbb{C}$. If $\langle u_n \rangle_{n=0}^{\infty} \subseteq \mathbb{R}$, then its complex characteristic roots appear in conjugate pairs, and

$$u_n = \sum_{i=1}^{m_1} A_i(n)\lambda_i^n + \sum_{i=1}^{m_2} \left(C_i(n)\lambda_i^n + \overline{C_i(n)}\,\overline{\lambda_i}^n \right), \tag{2.2}$$

with $A_1, \ldots, A_{m_1} \in \mathbb{R}[n]$ and $C_1, \ldots, C_m \in \mathbb{C}[n]$. Conversely, any infinite sequences that has an exponential representation of the form (2.1) or (2.2) is an LRS [42].

The following result due to Braverman [26] enables us to reason about the complex part of the exponential polynomials i.e., polynomials of the form $\sum_{i=1}^{m} p_i(n)\lambda_i^n$ for $\lambda_1, \ldots, \lambda_m \in \mathbb{C}$.

Lemma 13 (Complex Units Lemma)**.** *Let $\zeta_1, \zeta_2, \ldots, \zeta_m \in \mathbb{T} \setminus \{1\}$ be distinct complex numbers (where $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$), and let $\alpha_1, \alpha_2, \ldots, \alpha_m \in \mathbb{C} \setminus \{0\}$. Set $z_n := \sum_{k=1}^{m} \alpha_k \zeta_k^n$. Then there exists $c < 0$ such that for infinitely many n, $\mathrm{Re}\,(z_n) < c$.*

In particular, Lemma 13 immediately implies that a linear recurrence sequence without a positive real dominant characteristic root can not be always positive, be eventually always positive, or diverge to ∞. We will use this in Subsection 3.2.1 to obtain effective divergence upper bounds for LRS.

Finally, the following proposition from [77] allows us to bound the growth rate of the low-order terms in the exponential polynomial of a linear recurrence sequence.

Proposition 14. *Consider a linear recurrence sequence $\mathbf{u} = \langle u_n \rangle_{n=0}^{\infty}$ of bounded order, with dominant modulus ρ, and write*

$$\frac{u_n}{\rho^n} = A(n) + \sum_{i=1}^{m} \left(C_i(n)\lambda_i^n + \overline{C_i(n)}\,\overline{\lambda_i}^n \right) + r(n),$$

where A is a real polynomial, C_i are non-zero complex polynomials, $\rho\lambda_i$ and $\rho\overline{\lambda_i}$ are conjugate pairs of non-real dominant roots of $\mathbf{u}$, and r is an exponentially decaying function.

We can compute in polynomial time $\epsilon \in (0,1)$ and $N \in \mathbb{N}$ such that

$$\begin{aligned} &\frac{1}{\epsilon} = 2^{\|\mathbf{u}\|^{O(1)}}, \\ &N = 2^{\|\mathbf{u}\|^{O(1)}}, \\ &\text{for all } n > N, |r(n)| < (1-\epsilon)^n. \end{aligned}$$

We use the following well-known homogenisation result frequently in Chapter 3. The construction and the proof of Proposition 15 can be found in Subsection 3.3.1.

Proposition 15. *Let* $\mathbf{u} = \langle u_n \rangle_{n=0}^{\infty}$ *satisfy an inhomogeneous linear recurrence of order* k*. Then* $\mathbf{u}$ *satisfies a homogeneous recurrence of order* $k+1$*.*

For an inhomogeneous LRS $\mathbf{u}$ of order k, we refer to the corresponding homogeneous representation obtained as per Proposition 15 as the *homogenisation* of $\mathbf{u}$, denoted $\textsc{hom}(\mathbf{u})$.

2.6 Real Algebraic Geometry

In this subsection, we will state some zero-dimensionality lemmata from [74] that we will use to study divergence of linear recurrence sequences in Subsection 3.2.1.

2.6.1 Zero-Dimensionality Lemmata

Lemma 16. *Let* $a_1, \ldots, a_m \in \mathbb{R}$ *and* $\phi_1, \ldots, \phi_m \in \mathbb{R}$ *be two collections of* m *real numbers, for* $m \geq 1$*, with each of the* a_i *non-zero, and let* $l_1, \ldots l_m \in \mathbb{Z}$ *be integers. Define* $f, g : \mathbb{R}^m \to \mathbb{R}$ *by setting* $f(x_1, \ldots, x_m) = \sum_{i=1}^{m} a_i \cos(x_i + \phi_i)$ *and* $g(x_1, \ldots, x_m) = \sum_{i=1}^{m} l_i x_i$*. Assume that* $g(x_1, \ldots, x_m)$ *is not of the form* $l(x_i \pm x_j)$ *for some non-zero* $l \in \mathbb{Z}$ *and indices* $i \neq j$*. Let* $\psi \in \mathbb{R}$*.*

Then the function f*, subject to the constraint* $g(x_1, \ldots, x_m) = \psi$*, achieves its minimum only finitely many times over the domain* $[0, 2\pi)^m$*.*

Lemma 17. *Let* $\langle u_n \rangle$ *be a non-degenerate simple linear recurrence sequence with dominant characteristic roots* $\rho \in \mathbb{R}$ *and* $\gamma_1, \bar{\gamma}_1, \ldots, \gamma_m, \bar{\gamma}_m \in \mathbb{C} \setminus \mathbb{R}$*. Write* $\lambda_i = \gamma_i / \rho$ *for* $1 \leq i \leq m$*, and let* $L = \{(v_1, \ldots, v_m) \in \mathbb{Z}^m : \lambda_1^{v_1} \cdots \lambda_m^{v_m} = 1\}$*. Let* $\{\boldsymbol{\ell}_1, \ldots, \boldsymbol{\ell}_{m-1}\}$ *be a basis for* L *of cardinality* $m-1$*, and write* $\boldsymbol{\ell}_j = (\ell_{j,1}, \ldots, \ell_{j,m})$ *for* $1 \leq j \leq m-1$*. Let*

$$M = \begin{pmatrix} l_{1,1} & l_{1,2} & \cdots & l_{1,m-1} & l_{1,m} \\ l_{2,1} & l_{2,2} & \cdots & l_{2,m-1} & l_{2,m} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ l_{m-1,1} & l_{m-1,2} & \cdots & l_{m-1,m-1} & l_{m-1,m} \end{pmatrix} \tag{2.3}$$

Let $a_1, \ldots, a_m \in \mathbb{R}$ *and* $\phi_1, \ldots, \phi_m$ *be two collections of* m *real numbers, with each of the* a_i *non-zero, and let* $\boldsymbol{q} = (q_1, \ldots, q_{m-1}) \in \mathbb{Z}^{m-1}$ *be a column vector of* $m-1$ *integers. Let us further write* $\boldsymbol{x} = (x_1, \ldots, x_m)$ *to denote a column vector of* m *real-valued variables.*

Then the function $f(x_1, \ldots, x_m) = \sum_{i=1}^{m} a_i \cos(x_i + \phi_i)$*, subject to the constraint* $M\boldsymbol{x} = 2\pi\boldsymbol{q}$*, achieves its minimum at only finitely many points over the domain* $[0, 2\pi)^m$*.*

Chapter 3

Linear Recurrence Sequences

3.1 Introduction

Linear recurrence sequences (LRS), such as the Fibonacci numbers, permeate a wide range of scientific fields, from economics and theoretical biology to computer science and mathematics. In computer-aided verification, for example, LRS techniques play a key rôle in the termination analysis of a large class of simple while loops—see [78] for a short survey on this topic. Likewise, the ergodic behaviour of Markov chains in probability theory [2], or the stability of supply-and-demand price equilibria in laggy markets in economics (the so-called 'cobweb model') [8] can be analysed through an examination of the asymptotic behaviour of certain types of LRS; in particular, instability of price equilibria corresponds precisely to *divergence* of the associated LRS.

In this chapter, we undertake a systematic and fine-grained analysis of the growth behaviour of rational linear recurrence sequences from the point of view of effectiveness and complexity. In order to describe our main results, we first require some preliminary definitions. A sequence of real numbers $\mathbf{u} = \langle u_n \rangle_{n=0}^{\infty}$ is said to satisfy a *linear recurrence of order* k if there are real numbers $a_1, \ldots, a_{k+1}$ such that

$$u_{n+k} = a_1 u_{n+k-1} + \cdots + a_{k-1} u_{n+1} + a_k u_n + a_{k+1} \tag{3.1}$$

for all $n \in \mathbb{N}$. Such a recurrence is said to be *homogeneous* if $a_{k+1} = 0$ and *inhomogeneous* if $a_{k+1} \neq 0$. We shall refer to $\mathbf{u}$ as a(n) (in)homogeneous LRS of order k, or an LRS of (in)homogeneous degree k, interchangebly. The *characteristic polynomial* of the recurrence is

$$p(x) := x^k - a_1 x^{k-1} - \cdots - a_{k-1} x - a_k \,.$$

The zeros of p are called the *characteristic roots*. A characteristic root of maximum modulus is said to be *dominant* and its modulus is the *dominant modulus*. The *multiplicity* of a characteristic root γ is the maximal $m \in \mathbb{N}$ such that $(x-\gamma)^m$ divides $p(x)$.

An LRS is said to be *rational* if it consists of rational numbers, *integral* if it consists of integers, and *algebraic* if it consists of algebraic numbers. In the rest of this chapter, we will assume that all LRS are rational unless stated otherwise. An LRS is *simple* if all of its characteristic roots have multiplicity 1, and is *non-degenerate* if no ratio of two distinct characteristic roots is a root of unity.[1]

3.1.1 A Survey of Existing Literature

3.1.1.1 Skolem Problem

Skolem Problem, named after Thoralf Skolem, is arguably the most well-known open problem in study of LRS. It asks whether a given LRS $\mathbf{u} = \langle u_n \rangle_{n=0}^{\infty}$ ever attains 0 for some $n \in \mathbb{N}$.

Example 18. Let $\mathbf{u} = \langle u_n \rangle_{n=0}^{\infty}$ be the LRS defined by the recurrence relation

$$u_{n+3} = 2u_{n+2} + 5u_{n+1} - 6u_n,$$

and the initial values $594, -264, 2442$. We have that $u_4 = 2 \times 2442 + 5 \times (-264) - 6 \times 594 = 0$. Therefore, the sequence $\mathbf{u}$ attains 0 for $n = 4$. □

Even though the algorithmic decision issues in the 1930s had not yet acquired the importance they have today, Skolem Problem is regarded to have remained open since the publication of Skolem's original paper [97]. Lipton has called this persistent openness of decidability of the Skolem Problem as a "mathematical embarrassment" [59], and Tao has described it as "faintly outrageous" [100].

Now Let us start by stating a fundamental results about the zeros of LRS that we will be using on multiple occasions later on in this chapter.

Theorem 19 (Skolem-Mahler-Lech)**.** *Let $\langle u_n \rangle_{n=0}^{\infty}$ be a linear recurrence sequence over the reals. Its set of zeros $\{n : u_n = 0\}$ consists of a finite set F, along with a finite number (possibly zero) of arithmetic progressions $A_1 \cup \cdots \cup A_l$.*

[1] For most practical purposes—and certainly for all of the computational tasks considered in this chapter—LRS can be assumed to be non-degenerate, since any degenerate LRS can be effectively decomposed into a finite number of non-degenerate LRS; moreover this reduction can be carried out in polynomial time for rational LRS of bounded order [38, 77].

The celebrated Skolem-Mahler-Lech Theorem is named after Thoralf Skolem, who proved the theorem for sequences of rational numbers [97], Kurt Mahler, who proved it for sequences of algebraic numbers [61, 62], and Christer Lech, who proved it for sequences whose elements belong to any field of characteristics 0 [56], all using p-adic methods.

All proofs of the Skolem-Mahler-Lech Theorem are, however, ineffective as they achieve the result in a *non-constructive* manner [73]. In more detail, although one can effectively obtain all the arithmetic progressions $A_1, \ldots, A_l$ using a result of Berstel and Mignotte [18], no effective method of calculating the finite set F has been found as of now. As pointed by Terrence Tao "it is faintly outrageous that this problem is still open; it is saying that we do not know how to decide the halting problem even for 'linear' automata!" [100].

Decidability of the Skolem Problem for higher order LRS, however, turns out to be significantly harder. Nevertheless, significant progress has been made by imposing restrictions on LRS, most notably, by considering only low-order LRS. Orders 1 and 2 are considered folklore and are fairly straightforward. Let $\mathbf{u} = \langle u \rangle_{n=0}^{\infty}$ be an LRS of order at most 2 that is not the zero sequence $\langle 0 \rangle_{n=0}^{\infty}$. Without loss of generality, we can assume that the LRS $\mathbf{u}$ is non-degenerate (cf. Proposition 56). Remember from Subsubsection 2.5 that $\mathbf{u}$ can be written as

$$u_n = a_1\lambda_1^n + a_2\lambda_2^n, \ \forall n \in \mathbb{N},$$

where λ_1 and λ_2 are the characteristic roots of $\mathbf{u}$, and a_1 and a_2 are algebraic numbers. If $a_1 = 0$ or $a_2 = 0$ (i.e., when the order of $\mathbf{u}$ is 1), then $u_n \neq 0$ for all $n \in \mathbb{N}$. Otherwise, there are two possible scenarios:

- $|\lambda_1| = |\lambda_2| = \rho$. In this case, since $\mathbf{u}$ is non-degenerate, λ_1 and λ_2 are both complex algebraic numbers and are conjugate pairs that are not $\pm i$. Let $\gamma \in \mathbb{C}$ be such that have that $\lambda_1 = \rho\gamma = \bar{\lambda}_2$. Then, there exists some algebraic number $a \in \mathbb{C}$ such that $u_n = \rho^n(a\gamma^n + \bar{a}\bar{\gamma}^n)$. Now we have that

$$\begin{aligned} & u_n = 0 \\ \Leftrightarrow \quad & a\gamma^n = -\bar{a}\bar{\gamma}^n \\ \Leftrightarrow \quad & -\frac{a}{\bar{a}} = \left(\frac{\bar{\gamma}}{\gamma}\right)^n. \end{aligned}$$

  By [42, Proposition 2.7], the later is decidable. Therefore, in this case we can solve the Skolem Problem.

- $|\lambda_1| > |\lambda_2|$. In this case, we have that $u_n = a_1\lambda_1^n + a_2\lambda_2^n$. It can be easily seen that whenever
$$n > N = \frac{\log|a_2| - \log|a_1|}{\log|\lambda_1| - \log|\lambda_2|},$$
then $|a_1\lambda_1^n| > |a_2\lambda_2^n|$, and hence, $u_n \neq 0$. Therefore, to decide whether $\mathbf{u}$ ever attains 0, we only need to check whether $u_n = 0$ for $0 \leq n \leq N$. Thus, we observe that the Skolem Problem is decidable for homogeneous LRS of order at most 2.

Vereshchagin [104] as well as Mignotte, Shorey, and Tijdeman [69] independently showed the decidability for orders 3 and 4. Both proofs make heavy use of p-adic techniques, Galois theory, and Baker's Theorem on linear sums of logarithms, for which Baker was award the Fields Medal in 1970. An enthusiastic reader can learn more on Baker's results in Waldschmidt's book [105], on p-adic numbers in [41], and on Galois theory in [63, Chapter 24].

Halava *et al.*, in 2005, published a paper [42] containing a detailed history of Skolem Problem, and a decision procedure for Skolem Problem for order 5 LRS. Unfortunately, however, the proof is incorrect as acknowledged by the authors. The case that the paper fails to handle is when an LRS $\mathbf{u} = \langle u_n \rangle_{n=0}^{\infty}$ has five distinct characteristic roots; four of which, $\gamma_1, \gamma_2, \bar{\gamma}_1, \bar{\gamma}_2$, are complex and of the same magnitude, and another one, r, of strictly smaller magnitude. The positioning of eigenvalues of one such LRS is depicted in Figure 3.1.

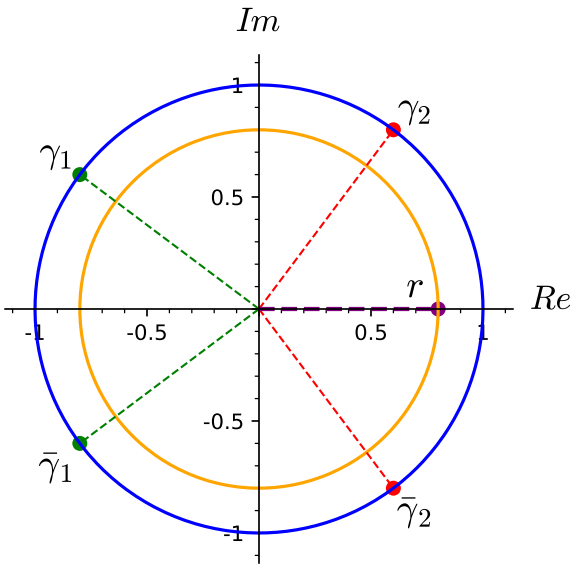

Figure 3.1: Eigenvalues $\gamma_1, \gamma_2, \bar{\gamma}_1, \bar{\gamma}_2$, and r of an open instance of Skolem Problem.

The general exponential form of $\mathbf{u}$ can be expressed as

$$\begin{aligned} u_n &= A\gamma_1^n + \bar{A}\bar{\gamma}_1^n + B\gamma_2^n + \bar{B}\bar{\gamma}_2^n + cr^n \\ &= \rho^n(a\cos(n\theta_1 + \phi_1) + b\cos(n\theta_2 + \phi_2)) + cr^n, \end{aligned}$$

where ρ is the magnitude of γ_1, θ_1 and θ_2 are the arguments of γ_1 and γ_2 respectively, a, b, and c are real algebraic numbers such that $a = |A|, b = |B|$, and ϕ_1 and ϕ_2 are the arguments of two algebraic numbers, all of which can be effectively calculated. As of now, if $|a| \neq |b|$, there does not seem to be any decision procedure for deciding whether $u_n = 0$ for some n.

We can summarise the above results on Skolem Problem in the following theorems

Theorem 20 (Decidability result from [104, 42])**.** *Skolem problem is decidable for homogeneous LRS of order* 4*.*

Theorem 21 (Complexity result from [21])**.** *Skolem problem is* **NP-Hard***.*

A recent approach taken towards the Skolem Problem is by limiting the indices under study. Kenison *et al.* considered the following specialisation of the Skolem problem: given an LRS $\mathbf{u} = \langle u_n \rangle_{n=0}^{\infty}$ and $c \in \mathbb{Z}^+$, decide whether there exists $n \in \mathbb{Z}^+$ of the form $n = \ell p^k$, with $k, \ell \leq c$, and p any prime number, such that $u_n = 0$ [48]. They, in fact, showed that it can be decided if such an n exists whenever one further assumes $v_\ell \neq 0$, where $\langle v_n \rangle_{n=0}^{\infty}$ is the LRS obtained by replacing $C_i(n)$ in (2.1) by $C_i(0)$.

3.1.1.2 Positivity Problem

After the Skolem Problem, The *Positivity* problem is probably the most studied problem about LRS. An LRS $\langle u_n \rangle_{n=0}^{\infty}$ defined by an equation of the form (3.1) is *positive* if $u_n \geq 0$ for all $n \geq 0$.

Example 22. Let $\mathbf{u}$ be the same LRS as in Example 18. Since $u_2 = -264$, $\mathbf{u}$ is not positive. □

Surprisingly, the Skolem Problem can be reduced to the Positivity Problem: we have $u_n = 0$ if and only if $u_n^2 \leq 0$, and the pointwise multiplication of two LRS is again an LRS. In the worst case, this reduction allows reducing an instance of the Skolem Problem of order k to an instance of the Positivity Problem of order k^2. An immediate consequence of the reduction is that the Positivity Problem is **NP-Hard**, inheriting **NP-Hardness** from the Skolem Problem.

In light of the above reduction, the Positivity Problem can be considered as open since 1930s. Nonetheless, the earliest explicit references of the Positivity Problem can be found in papers of Salomaa [89] and Soittola [98] from 1970s. The first decidability result on the Positivity Problem for order two homogeneous LRS was only established in 2006, a witness to the resilience of the Positivity Problem [43]. Order three had to wait longer until 2009 [54].

The biggest breakthrough happened in 2014, when Ouaknine and Worrell, pushed the decidability boundaries to order 5 homogeneous LRS [76], and showed that solving the Positivity Problem for order 6 will entail major breakthroughs in mathematics, and hence, is hard. They also showed that, when the homogeneous LRS is simple one can decide Positivity Problem up to order 9 [75].

Now, We will briefly summarise the results on Positivity Problem.

Positivity Problem Upper Bounds: The following theorems are from [76] and [75], respectively.

Theorem 23 (Upper Bounds from [76])**.** *Positivity is decidable for homogeneous LRS of order* 5 *or less with complexity in* $\mathbf{coNP^{PosSLP}}$*.*

Theorem 24 (Upper Bounds from [75])**.** *Positivity is decidable for simple homogeneous LRS of order* 9 *or less with complexity in* $\mathbf{coNP^{PosSLP}}$*.*

Positivity Problem Lower Bound: In Subsection 3.3.3, we will formalise the definition of hardness used in the following theorem.

Theorem 25 (Positivity Lower Bounds from [76])**.** *Positivity for LRS of order at least* 6 *is hard with respect to the problem of computing the approximation type of certain transcendental numbers.*

The lowest-order homogeneous LRS for which the Positivity Problem is open are of order 6, and have 3 eigenvalues of the same modulus, each of which of multiplicity 2 (cf. Subsection 3.2.2). By normalisation via dividing by modulus, we can further assume that all of these eigenvalues have modulus 1. Moreover, since we are only considering real LRS, all complex eigenvalues appear in pairs. Figure 3.2 shows the positioning of eigenvalues of such an LRS.

3.1.1.3 Ultimate Positivity Problem

An LRS $\mathbf{u} = \langle u_n \rangle_{n=0}^{\infty}$ defined by an equation of the form 3.1 is *ultimately positive* if for some $N \in \mathbb{N}$ we have that $u_n \geq 0$ for all $n \geq N$. Similarly to the Positivity Problem, the *Ultimate Positivity Problem* is the problem of deciding given an LRS $\mathbf{u}$ if it is ultimately positive. The variant of Ultimate Positivity Problem that, further, asks for effective computation of such N is known as *Effective Ultimate Positivity Problem*.

Example 26. Let $\mathbf{u}$ be the same LRS as in Example 18. Using the recurrence relation for $\mathbf{u}$, we have that its characteristic polynomial is

$$x^3 - 2x^2 - 5x + 6 = (x - 3)(x + 2)(x - 1).$$

Hence the characteristic roots of $\mathbf{u}$ are $\lambda_1 = 3, \lambda_2 = -2$ and $\lambda_3 = 1$. Therefore, we have that

$$u_n = 99\lambda_1^n + 352\lambda_2^n + 143\lambda_3^n.$$

We observe that the term $99\lambda_1^n$ dominates the other terms, and thus, $\mathbf{u}$ is ultimately positive. In fact, it can be easily seen that $u_n \geq 0$ for $n \geq 4$. □

The Ultimate Positivity Problem, in the first glance, might seem to be more straightforward than the Positivity Problem. Even though in some variations of the Ultimate Positivity Problem, such as the Ultimate Positivity Problem for simple LRS, there are better decidability and complexity upper bounds, that does not seem to be the cause in general. In fact, if one can solve the Effective Ultimate Positivity Problem, the decidability of the Positivity Problem directly follows.

In the early 1980s, Burke and Webb showed that Ultimate Positivity is decidable for homogeneous LRS of order 2 [27], and nine years later Nagasaka and Shiue [70] showed the same for LRS of order 3 that have repeated characteristic roots. In 2009, Laohakosol and Tangsupphathawat proved that both Positivity and Ultimate Positivity are decidable for homogeneous integer LRS of order 3 [55].

Most recently, Ouaknine and Worrell showed that Ultimate Positivity is solvable for homogeneous LRS of order at most 5 [76], and when the LRS is simple, for arbitrary orders [77]. They also showed that deciding Ultimate Positivity is hard for homogeneous LRS of order 6 by means of reduction from long-standing hard open problems in mathematics (cf. subsubsection 3.1.1.2).

Let us briefly summarise the latest results on the Ultimate Positivity Problem for homogeneous LRS.

Ultimate Positivity Problem Upper Bounds: The following results are from [76] and [77].

Theorem 27 (Upper Bounds from [76])**.** *Ultimate Positivity is decidable for homogeneous LRS of order* 5 *or less with complexity in* **PTIME**.

Theorem 28 (Upper Bounds from [77])**.** *Ultimate Positivity is decidable for simple homogeneous LRS of any order with complexity in* **PTIME**.

Theorem 29 (Upper Bounds from [76])**.** *Effective Ultimate Positivity is solvable for simple homogeneous LRS of order 9 or less with complexity in* **PTIME**.

Ultimate Positivity Problem Lower Bounds: Theorem 30 uses a notion of hardness introduced in [76], which we shall explain later in Subsection 3.3.3.

Theorem 30 (Ultimate Positivity Lower Bounds from [76])**.** *Ultimate Positivity for LRS of order at least* 6 *is hard with respect to the problem of computing the Lagrange constant of certain transcendental numbers.*

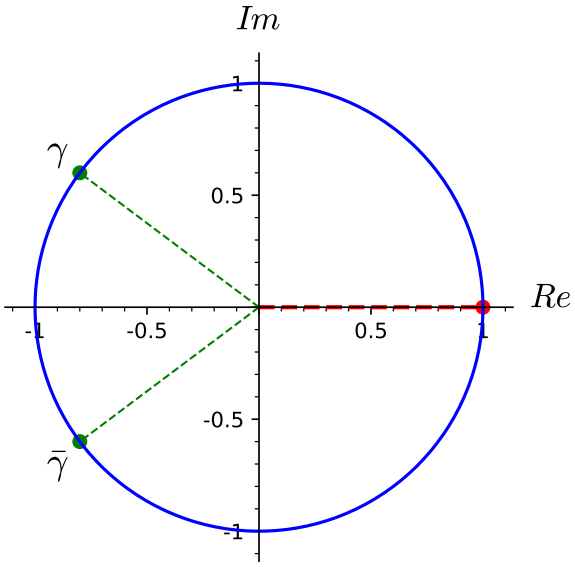

Figure 3.2: Eigenvalues $1, \gamma, \bar{\gamma}$ (each of multiplicity 2) of a hard instance of Positivity and Ultimate Positivity Problems.

Even though the reductions for Positivity and Ultimate Positivity are from different problems, hard instances of both problems have similar number of distinct eigenvalues and with the same multiplicity, as presented in Figure 3.2 (cf. Subsection 3.2.2).

3.1.1.4 Absolute Divergence

We say that an LRS $\mathbf{u}$ *diverges in absolute value to* ∞ if $\lim_{n\to\infty} |u_n| = \infty$ (technically speaking: for all $T \in \mathbb{N}$, there exists $N \in \mathbb{N}$ such that, for all $n \geq N$, we have $|u_n| \geq T$).

The celebrated Skolem-Mahler-Lech theorem (Theorem 19), implies that all non-degenerate integral LRS attain any particular value only finitely often, and, therefore, are absolutely divergent. This statement is however *non-effective* in a very basic sense: given a finite representation of a non-degenerate integral LRS $\mathbf{u}$, there is no known algorithm to compute a bound N such that $u_n \neq 0$ for $n \geq N$. It is also worth pointing out that the divergence assertion fails in general for non-integral LRS.

The question of the so-called *rate of absolute divergence* for non-degenerate integral LRS was subsequently extensively studied; see [38, Sec. 2.4] for an account of some of the key results accumulated over the last several decades. To begin with, a fairly straightforward fact is the following: if $\mathbf{u}$ is an algebraic LRS of order k with dominant modulus ρ, then there is an effectively computable constant a such that, for all $n \geq 1$, $|u_n| \leq a\rho^n n^k$. In the 1970s, a conjecture was formulated to the effect that any non-degenerate integral LRS has, essentially, the maximal possible growth rate (see the next theorem for a precise statement). The conjecture was finally settled positively independently by Evertse [39] and by van der Poorten and Schlickewei [103]:

Theorem 31. *For any non-degenerate algebraic LRS* $\mathbf{u}$ *of dominant modulus* $\rho > 1$*, and any* $\varepsilon > 0$*, there exists a constant* N *such that, for all* $n \geq N$*, we have* $|u_n| \geq \rho^{(1-\varepsilon)n}$.

This is a highly non-trivial result making use of deep number-theoretic tools concerning bounds on the sum of S-units. Unfortunately, the proof is not effective, in the sense that given $\varepsilon > 0$, it does not provide estimates for the corresponding value of N. This effectiveness issue is described as "an important open problem" in [38], where it is furthermore suggested that any progress on the matter would likely hinge upon substantial improvements of deep number-theoretic results, such as Roth's theorem, the prospects of which currently appear to be remote.

Nevertheless—and in particular for algorithmic applications in computer science—effectiveness is of central importance. The sharpest known results in this vein are due to Mignotte [68] as well as Shorey and Stewart [94], capping a long line of work in this area:

Theorem 32. *For any homogeneous non-degenerate integral LRS* $\mathbf{u}$ *of order at most* 3 *with dominant modulus* ρ*, there are effective constants* a, d *and* N *such that, for all* $n \geq N$*, we have* $|u_n| \geq \frac{a\rho^n}{n^d}$.

However, when there are more than 4 dominant eigenvalues, the absolute divergence problem remains open. The placement of eigenvalues of an LRS for which the Absolute Divergence Problem is open is demonstrated in Figure 3.3.

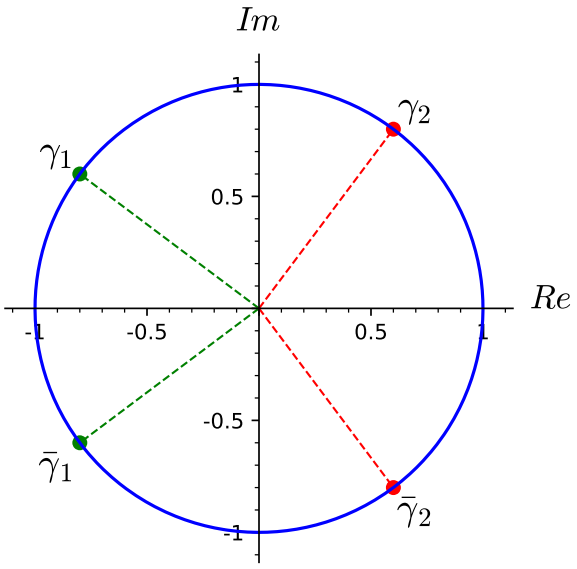

Figure 3.3: Eigenvalues $\gamma_1, \gamma_2, \bar{\gamma}_1, \bar{\gamma}_2$ of an open instance of Absolute Divergence Problem.

3.2 Divergence

We say that an LRS $\mathbf{u}$ *diverges to* ∞ if $\lim_{n\to\infty} u_n = \infty$ (technically speaking: for all $T \in \mathbb{N}$, there exists $N \in \mathbb{N}$ such that, for all $n \geq N$, we have $u_n \geq T$).

For most problems in computer science and automated verification, such as the analysis of the long-run behaviour of dynamical systems or the termination of linear while loops, the primary notion of *divergence* is clearly much more relevant than that of 'divergence in absolute value'. In view of the above results, however, one might expect that little could be said about effective rates of divergence. Somewhat surprisingly, divergence does turn out to be significantly more tractable than absolute divergence, in that it can be solved for a broader class of recurrences. At a high level, the main results of this chapter can now be summarised as follows:

Given a rational LRS $\mathbf{u}$, homogeneous or inhomogeneous, either of order at most 5, or, if the LRS is simple, of order at most 8, we can carry out the following tasks in polynomial time:

- decide if $\mathbf{u}$ diverges to ∞ or not; and
- in divergent instances, provide effective fine-grained lower bounds on the rate of divergence of $\mathbf{u}$.

The precise statements can be found in Theorems 33 and 34. The most obvious contrast in comparison with Theorem 32 is the higher order of LRS that can be handled effectively (5 and 8 versus 3). It is also worth noting, however, that our results apply more generally to rational (as opposed to integral) LRS, and that we can handle inhomogeneous sequences at no cost—this is remarkable in that the folklore wisdom usually broadly equates inhomogeneous LRS of order k with homogeneous LRS of order $k+1$ (this assertion, as well as the manner in which we circumvent it, are made precise in the main body of the chapter).

Finally, let us point out that our analysis of divergence rates relies, among others, on improvements to results concerning the positivity and ultimate positivity of LRS, which were originally developed in [76, 77, 75]. As a by-product, therefore, stronger results on the Positivity and Ultimate Positivity Problems—notably dealing with inhomogeneous LRS—can be found in the present chapter, in particular in the form of Theorems 41 and 42.

Recall from Theorem 31 that an LRS $\mathbf{u}$ with dominant modulus ρ necessarily diverges in absolute value if $\rho > 1$. More precisely, if $\rho > 1$ then given $\varepsilon > 0$ there exists a threshold N such that $|u_n| > \rho^{(1-\varepsilon)n}$ for all $n > N$. However this result is *ineffective*—it is not known how to compute N given $\mathbf{u}$ and ε.

In this section we derive *effective* divergence bounds for sequences that diverge to ∞ (i.e., sequences that both diverge in absolute value and that are ultimately positive). The bounds on divergence have the following form: for a divergent sequence $\mathbf{u}$ with dominant modulus $\rho = 1$ we aim to show that for every $n > N$, $u_n > an^d$ for effective constants $a > 0, d \in \mathbb{N}$, and $N \in \mathbb{N}$. In case of a dominant modulus $\rho > 1$ we aim to show that for every $n > N$, $u_n > \frac{a\rho^n}{n^d}$ for effective constants $a > 0, d \in \mathbb{N}$, and $N \in \mathbb{N}$. Henceforth we refer to bounds of these respective forms as *divergence bounds*.[2]

[2]Note that not only do we seek effective divergence bounds, but also that these bounds are asymptotically tighter than the bounds from Theorem 31 since for any fixed $d > 0$, it is clear that $a\rho^n/n^d$ eventually dominates $\rho^{(1-\varepsilon)n}$ for any $\varepsilon > 0$.

In Subsection 3.2.1, we show how to compute effective divergence bounds of LRS up to certain orders. Then in Subsection 3.2.2, we provide hardness results for the decidability of divergence.

3.2.1 Effective Divergence Upper Bounds

3.2.1.1 Effective Divergence Analysis of LRS

Let us begin by proving the following theorem:

Theorem 33. *There is a polynomial-time procedure that given a rational LRS* $\mathbf{u} = \langle u_n \rangle_{n=0}^{\infty}$ *of order at most 5 decides whether it diverges and, in case of divergence, outputs divergence bounds. In particular, in case of divergence, we find* $d, N \in \mathbb{N}$ *and* $a, \rho > 0$ *such that*

$$u_n \geq a n^d \rho^n$$

for all $n \geq N$.

Proof. We initially prove Theorem 33 for homogeneous LRS. We then show how to handle the inhomogeneous case, using Proposition 37.

Consider an LRS $\mathbf{u} = \langle u_n \rangle_{n=0}^{\infty}$ of order $k \leq 5$ with dominant modulus ρ, and let $\varepsilon > 0$ be a rational number. First, we note that without loss of generality, we can assume $\mathbf{u}$ is non-degenerate, as we may decompose a degenerate sequence and recast analysis at lower orders. In fact, $\mathbf{u}$ can be partitioned in polynomial time into at most 2520 non-degenerate LRS of the same order or less, q.v. the proof of Proposition 56 [76, section 2], [106, Corollary 3.3]. We also note that if $\rho < 1$, then $|u_n| \to 0$ as $n \to \infty$, and in particular the sequence does not diverge. Thus, we may assume $\rho \geq 1$.

By Lemma 13, if $\mathbf{u}$ does not have a real positive dominant root, then there are infinitely many $n \in \mathbb{N}$ such that $u_n < 0$, and therefore, $u_n \not\to \infty$. Thus, we may assume a real positive dominant root. Note that all other dominant roots must be complex, and come in conjugate pairs, since if $-\rho$ were a root, then $\mathbf{u}$ would be degenerate.

Writing u_n as an exponential polynomial and dividing by ρ^n, we have

$$\frac{u_n}{\rho^n} = A(n) + \sum_{i=1}^{m} \left(C_i(n)\lambda_i^n + \overline{C_i(n)}\,\overline{\lambda_i}^n \right) + r(n) \tag{3.2}$$

where A is a real polynomial, C_i are non-zero complex polynomials, $\rho\lambda_i$ and $\rho\overline{\lambda_i}$ are conjugate pairs of non-real dominant roots of $\mathbf{u}$, and r is an exponentially decaying function (possibly identically zero). We can assume that either $A \not\equiv 0$ or $m \neq 0$.

Indeed, otherwise we can consider the LRS $\langle \rho^n r(n) \rangle_{n=0}^{\infty}$, which is of lower order than $\mathbf{u}$.

We proceed to decide divergence by a case analysis of Equation (3.2).

Case 1 ($\rho = 1$): Note that in this case, $\frac{u_n}{\rho^n} = u_n$. If $A(n)$ is a constant, then it does not affect the divergence of $\mathbf{u}$. We claim that $u_n \not\to \infty$. Indeed, by Lemma 13, the expression $\sum_{i=1}^{m} \left(C_i(n)\lambda_i^n + \overline{C_i(n)\lambda_i}^n \right)$ becomes negative infinitely often (regardless of whether C_i are constants or polynomials), whereas the effect of $r(n)$ is exponentially decreasing. Thus, $\mathbf{u}$ does not diverge.

If $A(n)$ is not a constant, then $m \leq 1$. If $m = 0$, then clearly $u_n \to \infty$ if and only if the leading coefficient of $A(n)$ is positive. Otherwise, if $m = 1$, then C_1 is a constant, and thus $|C_1\lambda_1^n + \overline{C_1\lambda_1}^n| \leq 2|C_1|$, and again $u_n \to \infty$ if and only if the leading coefficient of $A(n)$ is positive.

Recall that since $\rho = 1$, then if $\mathbf{u}$ diverges, there exist $N, k \in \mathbb{N}$ such that $u_n \geq n^k$ for all $n > N$. We now show how to effectively compute N and k.

From Proposition 14, we can compute in polynomial time $\varepsilon \in (0, 1)$ and $N_1 \in \mathbb{N}$ such that $r(n) < (1-\varepsilon)^n < 1$ for all $n > N_1$. We thus have that $u_n \geq A(n) - |C_1| - 1$, and we can easily compute $N_2 \in \mathbb{N}$ and $a \in \mathbb{Q}$ (depending on the coefficients of $A(n)$) such that for all $n > N_2$ we have $A(n) - |C_1| - 1 \geq an^k$, where k is the degree of $A(n)$, namely 1 or 2. Taking $N = \max\{N_1, N_2\}$, we conclude this case.

Case 2 ($\rho > 1$ and there exists a non-constant C_i): In this case, $m = 1$, C_1 is linear, and $A(n)$ is constant. Let C_1 have leading coefficient $b \neq 0$. By Lemma 13, there exists $\varepsilon > 0$ such that $b\lambda^n + \overline{b\lambda}^n < -\varepsilon$ infinitely often. Then $C_1(n)\lambda_1^n + \overline{C_1(n)\lambda_1}^n$ (and hence u_n) is unbounded below, so $u_n \not\to \infty$.

Case 3 ($\rho > 1$ and every C_i is a nonzero constant): In this case, $m \leq 2$. In the following, we set $m = 2$, as the cases where $m < 2$ are similar and slightly simpler.[3]

Let $L = \{(v_1, v_2) \in \mathbb{Z}^2 : \lambda_1^{v_1}\lambda_2^{v_2} = 1\}$, and let $\{\boldsymbol{\ell}_1, \ldots, \boldsymbol{\ell}_p\}$ be a basis for L of cardinality p. Write $\boldsymbol{\ell}_q = (\ell_{q,1}, \ell_{q,2})$ for $1 \leq q \leq p$. From Theorem 5, such a basis can be computed in polynomial time, and moreover, each $\ell_{q,j}$ may be assumed to have magnitude polynomial in $\|\mathbf{u}\|$.

Consider the set $\mathbb{T} = \{(z_1, z_2) \in \mathbb{C}^2 : |z_1| = |z_2| = 1 \text{ and for each } 1 \leq q \leq p, z_1^{\ell_{q,1}} z_2^{\ell_{q,2}} = 1\}$.

[3]One may notice that taking $m = 2$ means that some of the cases we handle actually require order 6, e.g., when $A(n)$ is linear and $m = 2$. Still, the analysis covers all possible cases of order 5.

Define $h : \mathbb{T} \to \mathbb{R}$ by setting $h(z_1, z_2) = \sum_{i=1}^{2}(C_i z_i + \overline{C_i}\overline{z_i})$, so that for every $n \in \mathbb{N}$, $\frac{u_n}{\rho^n} = A(n) + h(\lambda_1^n, \lambda_2^n) + r(n)$. Recall that the set $\{(\lambda_1^n, \lambda_2^n) : n \in \mathbb{N}\}$ is a dense subset of $\mathbb{T}$. Since h is continuous, it follows that $\inf\{h(\lambda_1^n, \lambda_2^n) : n \in \mathbb{N}\} = \min h|_{\mathbb{T}} = \mu$ for some $\mu \in \mathbb{R}$.

We now claim that μ is an algebraic number, computable in polynomial time, with $\|\mu\| = \|\mathbf{u}\|^{O(1)}$. We can represent μ via the following formula $\tau(y)$:

$$\exists(\zeta_1, \zeta_2) \in \mathbb{T} : \ [h(\zeta_1, \zeta_2) = y \wedge \forall(z_1, z_2) \in \mathbb{T}, y \leq h(z_1, z_2)].$$

Note that $\tau(y)$ is not a formula in the first-order theory of the reals, as it involves complex numbers. However, we can rewrite it as a sentence in the first-order theory of the reals by representing the real and imaginary parts of each complex quantity and combining them using real arithmetic (see [77] for details). In addition, the obtained formula $\tau'(y)$ is of size polynomial in $\|\mathbf{u}\|$. By Theorem 12, we can then compute in polynomial time an equivalent quantifier-free formula

$$\chi(x) = \bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} h_{i,j} \sim_{i,j} 0.$$

Recall that each $\sim_{i,j}$ is either $>$ or $=$. Now $\chi(x)$ must have a satisfiable disjunct, and since the satisfying assignment to y is unique (namely $y = \mu$), this disjunct must comprise at least one equality predicate. Since Theorem 12 guarantees that the degree and height of each $h_{i,j}$ are bounded by $\|\mathbf{u}\|^{O(1)}$ and $2^{\|\mathbf{u}\|^{O(1)}}$ respectively, we immediately conclude that μ is an algebraic number and with $\|\mu\| = \|\mathbf{u}\|^{O(1)}$.

We now split the analysis into several cases.

• If $A(n)$ is linear with negative leading coefficient, or if A is a constant and $A + \mu < 0$, then u_n is unbounded from below, and in particular $u_n \not\to \infty$.

• If $A(n)$ is linear with positive leading coefficient, or if A is a constant and $A + \mu > 0$, we can compute in polynomial time $N_0 \in \mathbb{N}$ and a rational $\varepsilon_0 > 0$ such that $A(n) + \mu > 2\varepsilon_0$ for all $n > N_0$. By Proposition 14, we can also compute in polynomial time $N_1 \in \mathbb{N}$ and $\varepsilon_1 \in (0, 1)$ such that $|r(n)| < (1 - \varepsilon_1)^n$ for all $n > N_1$. Taking $N_2 \geq \log_{1-\varepsilon_1} \varepsilon_0$, we have that for all $n > \max\{N_0, N_1, N_2\}$, $|r(n)| < \varepsilon_0$, and thus

$$\frac{u_n}{\rho^n} = A(n) + h(\lambda_1, \ldots, \lambda_m) + r(n) \geq A(n) + \mu - \varepsilon_0 > 2\varepsilon_0 - \varepsilon_0 = \varepsilon_0 \,.$$

Thus we have $u_n \geq \varepsilon_0 \rho^n$ for all $n > \max\{N_0, N_1, N_2\}$ and hence we have effective growth bounds in this case.

• If A is a constant and $A + \mu = 0$, things are more involved. Let $\lambda_j = e^{i\theta_j}$ and $C_j = |C_j|e^{i\phi_j}$ for $1 \leq j \leq 2$. From Equation (3.2) we have

$$\frac{u_n}{\rho^n} = A + \sum_{j=1}^{2} 2|C_j| \cos(n\theta_j + \phi_j) + r(n)$$

We further assume that all the C_j are non-zero. Indeed, if this does not hold, we can recast our analysis in lower dimension.

We now claim that h achieves its minimum μ only finitely many times over $\mathbb{T}$. To establish this claim, we proceed according to the cardinality p of the basis $\{\boldsymbol{\ell}_1, \ldots, \boldsymbol{\ell}_p\}$ of L:

(i) We first consider the case in which $p = 1$, and handle the case $p = 0$ immediately afterwards. Let $\boldsymbol{\ell}_1 = (\ell_{1,1}, \ell_{1,2}) \in \mathbb{Z}^2$ be the sole vector spanning L. For $x \in \mathbb{R}$, recall that we denote by $[x]_{2\pi}$ the distance from x to the closest integer multiple of 2π.

Write

$$R = \{(x_1, x_2) \in [0, 2\pi)^2 : [\ell_{1,1}x_1 + \ell_{1,2}x_2]_{2\pi} = 0\}.$$

Clearly, for any $(x_1, x_2) \in [0, 2\pi)^2$, we have $(x_1, x_2) \in R$ if and only if $(e^{ix_1}, e^{ix_2}) \in \mathbb{T}$. Define $f : \mathbb{R}^2 \to \mathbb{R}$ by setting

$$f(x_1, x_2) = \sum_{j=1}^{2} 2|C_j| \cos(x_j + \phi_j).$$

Clearly, for all $(x_1, x_2) \in [0, 2\pi)^2$ we have $f(x_1, x_2) = h(e^{ix_1}, e^{ix_2})$, and therefore the minimal values of f over $\mathbb{R}$ are in one-to-one correspondence with those of h over $\mathbb{T}$.

Define $g : \mathbb{R}^2 \to \mathbb{R}$ by setting

$$g(x_1, x_2) = \ell_{1,1}x_1 + \ell_{1,2}x_2.$$

Note that $g(x_1, x_2)$ cannot be of the form $\ell(x_i - x_j)$, for nonzero $\ell \in \mathbb{Z}$ and $i \neq j$, otherwise $\lambda_i^{\ell}\lambda_j^{-\ell} = 1$, i.e., λ_i/λ_j would be a root of unity, contradicting the non-degeneracy of $\mathbf{u}$. Likewise, g cannot be of the form $\ell(x_i + x_j)$, otherwise $\lambda_i/\overline{\lambda}_j$ would be a root of unity.

Finally, observe that for $(x_1, x_2) \in [0, 2\pi)^2$, we have $(x_1, x_2) \in R$ if and only if $\ell_{1,1}x_1 + \ell_{1,2}x_2 = 2\pi q$ for some $q \in \mathbb{Z}$ with $|q| \leq |\ell_{1,1}| + |\ell_{1,2}|$. For each of these finitely many q, we can invoke Lemma 16 with f, g, and $\psi = 2\pi q$, to conclude that f achieves its minimum μ finitely many times over R, and therefore that h achieves the same minimum finitely many times over $\mathbb{T}$.

The case $p = 0$, i.e., in which there are no non-trivial integer multiplicative relationships among λ_1, λ_2, is now a special case of the above, where we have $\ell_{1,1} = \ell_{1,2}$.

(ii) We observe that the case $p = 2$ cannot occur: indeed, a basis for L of dimension 2 would immediately entail that every λ_j is a root of unity.

This concludes the proof of the claim that h achieves its minimum at a finite number of points $Z = \{(\zeta_1, \zeta_2) \in \mathbb{T} : h(\zeta_1, \zeta_2) = \mu\}$.

We concentrate on the set Z_1 of first coordinates of Z. Write

$$\tau_1(x) = \exists z_1(\mathrm{Re}(z_1) = x \wedge z_1 \in Z_1)$$
$$\tau_2(y) = \exists z_1(\mathrm{Im}(z_1) = y \wedge z_1 \in Z_1)$$

Similarly to our earlier construction, $\tau_1(x)$ is equivalent to a formula $t_1'(x)$ in the in the first-order theory of the reals, over a bounded number of real variables, with $\|\tau_1'(x)\| = \|\mathbf{u}\|^{O(1)}$. Thanks to Theorem 12, we then obtain an equivalent quantifier-free formula

$$\chi_1(x) = \bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} h_{i,j} \sim_{i,j} 0.$$

Note that since there can only be finitely many $\hat{x} \in \mathbb{R}$ such that $\chi_1(\hat{x})$ holds, each disjunct of $\chi_1(\hat{x})$ must comprise at least one equality predicate, or can otherwise be entirely discarded as having no solution. A similar exercise can be carried out with $\tau_2(y)$ to obtain $\chi_2(y)$. The bounds on the degree and height of each $h_{i,j}$ in $\chi_1(x)$ and $\chi_2(y)$ then enable us to conclude that any $\zeta_1 = \hat{x} + i\hat{y} \in Z_1$ is algebraic, and moreover satisfies $\|\zeta_1\| = \|\mathbf{u}\|^{O(1)}$. In addition, bounds on I and J_i guarantee that the cardinality of Z_1 is at most polynomial in $\|\mathbf{u}\|$.

Since λ_1 is not a root of unity, for each $\zeta_1 \in Z_1$ there is at most one value of n such that $\lambda_1^n = \zeta_1$. Theorem 5 then entails that this value (if it exists) is at most $M = \|\mathbf{u}\|^{O(1)}$, which we can take to be uniform across all $\zeta_1 \in Z_1$. We can now invoke Lemma 3 to conclude that, for $n > M$, and for all $\zeta_1 \in Z_1$, we have

$$|\lambda_1^n - \zeta_1| > \frac{1}{n^{\|\mathbf{u}\|^D}}, \tag{3.3}$$

where $D \in \mathbb{N}$ is some absolute constant.

Let $b > 0$ be minimal such that the set

$$\{z_1 \in \mathbb{C} : |z_1| = 1 \text{ and, for all } \zeta_1 \in Z_1, |z_1 - \zeta_1| \geq \frac{1}{b}\}$$

is non empty. Thanks to our bounds on the cardinality of Z_1, we can use the first-order theory of the reals, together with Theorem 12, to conclude that b is algebraic and $\|b\| = \|\mathbf{u}\|^{O(1)}$.

Define the function $g : [b, \infty) \to \mathbb{R}$ as follows:

$$g(x) = \min\{h(z_1, z_2) - \mu : (z_1, z_2) \in \mathbb{T} \text{ and for all } \zeta_1 \in Z_1, |z_1 - \zeta_1| \geq \frac{1}{x}\}.$$

It is clear that g is continuous and $g(x) > 0$ for all $x \in [b, \infty)$. Moreover, g can be translated in polynomial time into a function in the first-order theory of the reals over a bounded number of variables. It follows from Proposition 2.6.2 of [23] (invoked with the function $1/g$) that there is a polynomial $P \in \mathbb{Z}[x]$ such that, for all $x \in [b, \infty)$,

$$g(x) \geq \frac{1}{P(x)} \tag{3.4}$$

Moreover, an examination of the proof of [23, Prop. 2.6.2] reveals that P is obtained through a process which hinges on quantifier elimination. By Theorem 12, we are therefore able to conclude that $\|P\| = \|\mathbf{u}\|^{O(1)}$, a fact which relies among others on our upper bounds for $\|b\|$.

By Proposition 14 we can find $\varepsilon \in (0, 1)$ and $N = 2^{\|\mathbf{u}\|^{O(1)}}$ such that for all $n > N$, we have $|r(n)| < (1 - \varepsilon)^n$, and moreover $1/\varepsilon = 2^{\|\mathbf{u}\|^{O(1)}}$. In addition, by Proposition 4, there is $N' = 2^{\|\mathbf{u}\|^{O(1)}}$ such that for every $n \geq N'$

$$\frac{1}{2P(n^{\|\mathbf{u}\|^D})} > (1 - \varepsilon)^n. \tag{3.5}$$

Combining Equations (3.2)–(3.5), we get

$$\begin{aligned}
\frac{u_n}{\rho^n} &= A + h(\lambda_1^n, \lambda_2^n) + r(n) \\
&\geq -\mu + h(\lambda_1^n, \lambda_2^n) - (1 - \varepsilon)^n \\
&\geq g(n^{\|\mathbf{u}\|^D}) - (1 - \varepsilon)^n \\
&\geq \frac{1}{P(n^{\|\mathbf{u}\|^D})} - (1 - \varepsilon)^n \\
&= \frac{1}{2P(n^{\|\mathbf{u}\|^D})} + \frac{1}{2P(n^{\|\mathbf{u}\|^D})} - (1 - \varepsilon)^n \\
&\geq \frac{1}{2P(n^{\|\mathbf{u}\|^D})}
\end{aligned}$$

provided $n > \max\{M, N, N'\}$. We thus have that $\frac{u_n}{\rho^n}$ is eventually lower bounded by an inverse polynomial and hence we have effective growth bounds in this case.

This concludes the decidability of divergence and computability of effective bounds on divergence for homogeneous LRS of order at most 5.

It remains to show how to handle inhomogeneous LRS of order at most[4] 5. Consider an inhomogeneous LRS $\mathbf{v} = \langle v_n \rangle_{n=0}^{\infty}$ of order 5, and let $\mathbf{u} = \textsc{hom}(\mathbf{v})$. Consider the

[4]In fact, by Proposition 37, LRS of order at most 4 can be handled by homogenisation. Thus, it is enough to handle exactly order 5.

dominant modulus ρ of u_n. If $\rho > 1$, then by Proposition 37 the exponential polynomial of $\frac{u_n}{\rho^n}$ is the same as that in Equation (3.2). Thus, we can proceed with the case analysis of Case 2 and Case 3 without change. If $\rho = 1$, things become more involved. Consider the exponential polynomial

$$u_n = A(n) + \sum_{i=1}^{m} \left(C_i(n)(\lambda_i^n) + \overline{C_i(n)}(\overline{\lambda}_i^n) \right) + r(n) \tag{3.6}$$

where $|r(n)|$ is exponentially decaying and the λ_i are characteristic roots of modulus 1.

If $A(n)$ is constant, or if $A(n)$ is not a constant and all the C_i are constants (if there are any), then the same analysis of Case 1 applies here, *mutatis-mutandis*. Otherwise, the only possible case is where $A(n)$ is linear, $m = 1$, $C_1(n)$ is linear, and $r(n) \equiv 0$. Indeed, this corresponds to the case where the characteristic roots of u_n are $1, \lambda, \overline{\lambda}$, each with multiplicity 2. Let $A(n) = a_1 n + b_1$ and $C_1(n) = a_2 n + b_2$, then we can write

$$u_n = a_1 n + b_1 + (a_2 n + b_2)\lambda^n + (\overline{a_2} n + \overline{b_2})\overline{\lambda}^n = n(a_1 + a_2\lambda^n + \overline{a_2}\overline{\lambda^n}) + (b_1 + b_2\lambda^n + \overline{b_2\lambda^n})$$

Since $|(b_1 + b_2\lambda^n + \overline{b_2\lambda^n})|$ is bounded, then u_n diverges if and only if $n(a_1 + a_2\lambda^n + \overline{a_2}\overline{\lambda^n})$ diverges. Let $\theta = \arg\lambda$ and $\phi = \arg a_2$. We have $n(a_1 + a_2\lambda^n + \overline{a_2}\overline{\lambda^n}) = n(a_1 + 2|a_2|\cos(n\theta + \phi))$.

Again, we split into cases.

• If $a_1 > 2|a_2|$, we have that u_n diverges. Then we can compute in polynomial time a rational $\varepsilon > 0$ and $N \in \mathbb{N}$ such that $a_1 - 2|a_2| > \varepsilon$ and $n(a_1 + 2|a_2|) - (b_1 - 2|b_2|) > \varepsilon n$ for all $n > N$. We then have that $u_n > \varepsilon n$ for all $n > N$, thus concluding effective decidability of divergence in this case.

• If $a_1 < 2|a_2|$, then u_n does not diverge, as it becomes negative infinitely often.

• The remaining case is when $a_1 = 2|a_2|$, where the expression above becomes $na_1(1 + \cos(n\theta + \phi))$. We show that in this case, u_n does not diverge. By Taylor approximation, for every $x \in (-\pi, \pi]$ it holds that $1 - \cos(x) \leq \frac{x^2}{2}$. For $n \in \mathbb{N}$, write $\Lambda(n) = n\theta + \phi - (2j+1)\pi$, where $j \in \mathbb{Z}$ is the unique integer such that $-\pi < \Lambda(n) \leq \pi$. We now have that

$$na_1(1 + \cos(n\theta + \phi)) = na_1(1 - \cos(n\theta + \phi + \pi)) = na_1(1 - \cos(\Lambda(n))) < na_1\frac{\Lambda(n)^2}{2}.$$

By Dirichlet's Approximation Theorem, we have that $|\Lambda(n)| < \frac{t}{n}$ for infinitely many values of n, where t is a constant depending on ϕ. Thus, we have $na_1\frac{\Lambda(n)^2}{2} < \frac{a_1 t^2}{2n}$. It follows that u_n is infinitely often bounded by a constant, and does not diverge. □

3.2.1.2 Effective Divergence Analysis of Simple LRS

We now turn to simple LRS. In fact, for simple LRS we have the following theorem.

Theorem 34. *There is a polynomial-time procedure that, given a simple rational LRS* $\mathbf{u} = \langle u_n \rangle_{n=0}^{\infty}$ *of order at most 8, decides whether it diverges and, in case of divergence, outputs divergence bounds. In particular, in case of divergence, we find* $d, N \in \mathbb{N}$ *and* $a, \rho > 0$ *such that*

$$u_n \geq a n^d \rho^n$$

for all $n \geq N$.

Proof. As in the proof of Theorem 33, we start by considering the homogeneous case, and we let $\langle u_n \rangle$ be a non-degenerate simple LRS of order $d \leq 8$ with a real positive dominant characteristic root $\rho \geq 1$.

As before, we write

$$\frac{u_n}{\rho^n} = a + \sum_{i=1}^{m} (c_i \lambda_i^n + \overline{c_i}\,\overline{\lambda_i^n}) + r(n) \tag{3.7}$$

with $a \in \mathbb{R}$, $c_i \in \mathbb{C} \setminus \mathbb{R}$ for every $1 \leq i \leq m$, and $|r(n)|$ exponentially decaying. Note that since $d \leq 8$ and $a \in \mathbb{R}$, it follows that $0 \leq m \leq 3$. In the following, we consider the case where $m = 3$. The cases where $m < 3$ are very similar and slightly simpler, and are therefore omitted.

Observe that if $\rho = 1$, the sequence u_n is bounded, and therefore does not diverge. We hence assume $\rho > 1$.

Let $L = \{(v_1, \ldots, v_m) \in \mathbb{Z}^m : \lambda_1^{v_1} \cdots \lambda_m^{v_m} = 1\}$, and let $\{\boldsymbol{\ell}_1, \ldots, \boldsymbol{\ell}_p\}$ be a basis for L of cardinality p. Write $\boldsymbol{\ell}_q = (\ell_{q,1}, \ldots, \ell_{q,m})$ for $1 \leq q \leq p$. From Theorem 5, such a basis can be computed in polynomial time, and moreover, each $\ell_{q,j}$ may be assumed to have magnitude polynomial in $\|u\|$.

Consider the set

$$\mathbb{T} = \{(z_1, z_2, z_3) \in \mathbb{C}^3 : |z_1| = |z_2| = |z_3| = 1 \text{ and for all } 1 \leq q \leq p, z_1^{\ell_{q,1}} z_2^{\ell_{q,2}} z_3^{\ell_{q,3}} = 1\}.$$

Define $h : \mathbb{T} \to \mathbb{R}$ by setting $h(z_1, z_2, z_3) = \sum_{i=1}^{3} (c_i z_i + \overline{c_i z_i})$, so that for every $n \in \mathbb{N}$, $\frac{u_n}{\rho^n} = a + h(\lambda_1^n, \lambda_2^n, \lambda_3^n) + r(n)$. Recall that the set $\{\lambda_1^n, \lambda_2^n, \lambda_3^n : n \in \mathbb{N}\}$ is a dense subset of $\mathbb{T}$. Since h is continuous, it follows that $\inf\{h(\lambda_1^n, \lambda_2^n, \lambda_3^n) : n \in \mathbb{N}\} = \min h|_{\mathbb{T}} = \mu$ for some $\mu \in \mathbb{R}$.

We now claim that μ is an algebraic number, computable in polynomial time, with $\|\mu\| = \|\mathbf{u}\|^{O(1)}$. We can represent μ via the following formula $\tau(y)$:

$$\exists (\zeta_1, \zeta_2, \zeta_3) \in \mathbb{T} : \ [h(\zeta_1, \zeta_2, \zeta_3) = y \wedge \forall (z_1, z_2, z_3) \in \mathbb{T}, y \leq h(z_1, z_2, z_3)].$$

Note that $\tau(y)$ is not a formula in the first-order theory of the reals, as it involves complex numbers. However, we can rewrite it as a sentence in the first-order theory of the reals by representing the real and imaginary parts of each complex quantity and combining them using real arithmetic (see [77] for details). In addition, the obtained formula $\tau'(y)$ is of size polynomial in $\|\mathbf{u}\|$. By Theorem 12, we can then compute in polynomial time an equivalent quantifier-free formula

$$\chi(x) = \bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} h_{i,j} \sim_{i,j} 0.$$

Recall that each $\sim_{i,j}$ is either $>$ or $=$. Now $\chi(x)$ must have a satisfiable disjunct, and since the satisfying assignment to y is unique (namely $y = \mu$), this disjunct must comprise at least one equality predicate. Since Theorem 12 guarantees that the degree and height of each $h_{i,j}$ are bounded by $\|\mathbf{u}\|^{O(1)}$ and $2^{\|\mathbf{u}\|^{O(1)}}$ respectively, we immediately conclude that μ is an algebraic number and with $\|\mu\| = \|\mathbf{u}\|^{O(1)}$.

We now split to cases according to the sign of $a + \mu$.

• If $a + \mu < 0$, then $\mathbf{u}$ is infinitely often negative, and does not diverge.

• If $a + \mu > 0$, then $\mathbf{u}$ diverges, and it remains to show an effective bound. We can compute in polynomial time a rational $\varepsilon_0 > 0$ such that $a + \mu > 2\varepsilon_0$. By Proposition 14, we can also compute in polynomial time $N_1 \in \mathbb{N}$ and $\varepsilon_1 \in (0, 1)$ such that $|r(n)| < (1 - \varepsilon_1)^n$ for all $n > N_1$. Taking $N_2 \geq \log_{1-\varepsilon_1} \varepsilon_0$, we have that for all $n > \max\{N_1, N_2\}$, $|r(n)| < \varepsilon_0$, and thus

$$\frac{u_n}{\rho^n} = A(n) + h(\lambda_1, \ldots, \lambda_m) + r(n) \geq A(n) + \mu - \varepsilon_0 > 2\varepsilon_0 - \varepsilon_0 = \varepsilon_0$$

Thus $u_n > \varepsilon_0 \rho^n$ for all $n > \max\{N_1, N_2\}$ and hence we have effective divergence bounds in this case.

• It remains to analyse the case where $a + \mu = 0$. To this end, let $\lambda_j = e^{i\theta_j}$ and $c_j = |c_j| e^{i\phi_j}$ for $1 \leq j \leq 3$. From Equation (3.7) we have

$$\frac{u_n}{\rho^n} = a + \sum_{j=1}^{3} 2|c_j| \cos(n\theta_j + \phi_j) + r(n)$$

We further assume that all the c_j are non-zero. Indeed, if this does not hold, we can recast our analysis in lower dimension.

We now claim that h achieves its minimum μ only finitely many times over $\mathbb{T}$. To establish this claim, we proceed according to the cardinality p of the basis $\{\boldsymbol{\ell}_1, \ldots, \boldsymbol{\ell}_p\}$ of L:

(i) We first consider the case in which $p = 1$, and handle the case $p = 0$ immediately afterwards. Let $\boldsymbol{\ell_1} = (\ell_{1,1}, \ell_{1,2}, \ell_{1,3}) \in \mathbb{Z}^3$ be the sole vector spanning L. For $x \in \mathbb{R}$, recall that we denote by $[x]_{2\pi}$ the distance from x to the closest integer multiple of 2π. Write

$$R = \{(x_1, x_2, x_3) \in [0, 2\pi)^3 : [\ell_{1,1}x_1 + \ell_{1,2}x_2 + \ell_{1,3}x_3]_{2\pi} = 0\}.$$

Clearly, for any $(x_1, x_2, x_3) \in [0, 2\pi)^3$, we have $(x_1, x_2, x_3) \in R$ if and only if $(e^{ix_1}, e^{ix_2}, e^{ix_3}) \in \mathbb{T}$. Define $f : \mathbb{R}^3 \to \mathbb{R}$ by setting

$$f(x_1, x_2, x_3) = \sum_{j=1}^{3} 2|c_j| \cos(x_j + \phi_j).$$

Clearly, for all $(x_1, x_2, x_3) \in [0, 2\pi)^3$ we have $f(x_1, x_2, x_3) = h(e^{ix_1}, e^{ix_2}, e^{ix_3})$, and therefore the minimal values of f over $\mathbb{R}$ are in one-to-one correspondence with those of h over $\mathbb{T}$.

Define $g : \mathbb{R}^3 \to \mathbb{R}$ by setting

$$g(x_1, x_2, x_3) = \ell_{1,1}x_1 + \ell_{1,2}x_2 + \ell_{1,3}x_3.$$

Note that $g(x_1, x_2, x_3)$ cannot be of the form $\ell(x_i - x_j)$, for nonzero $\ell \in \mathbb{Z}$ and $i \neq j$, otherwise $\lambda_i^\ell \lambda_j^{-\ell} = 1$, i.e., λ_i/λ_j would be a root of unity, contradicting the non-degeneracy of $\mathbf{u}$. Likewise, g cannot be of the form $\ell(x_i + x_j)$, otherwise $\lambda_i/\overline{\lambda}_j$ would be a root of unity.

Finally, observe that for $(x_1, x_2, x_3) \in [0, 2\pi)^3$, we have $(x_1, x_2, x_3) \in R$ if and only if $\ell_{1,1}x_1 + \ell_{1,2}x_2 + \ell_{1,3}x_3 = 2\pi q$ for some $q \in \mathbb{Z}$ with $|q| \leq |\ell_{1,1}| + |\ell_{1,2}| + |\ell_{1,3}|$. For each of these finitely many q, we can invoke Lemma 16 with f, g, and $\psi = 2\pi q$, to conclude that f achieves its minimum μ finitely many times over R, and therefore that h achieves the same minimum finitely many times over $\mathbb{T}$.

The case $p = 0$, i.e., in which there are no non-trivial integer multiplicative relationships among $\lambda_1, \lambda_2, \lambda_3$, is now a special case of the above, where we have $\ell_{1,1} = \ell_{1,2} = \ell_{1,3} = 0$.

(ii) We now turn to the case $p = 2$. We have $\boldsymbol{\ell}_1 = (\ell_{1,1}, \ell_{1,2}, \ell_{1,3}) \in \mathbb{Z}^3$ and $\boldsymbol{\ell}_2 = (\ell_{2,1}, \ell_{2,2}, \ell_{2,3}) \in \mathbb{Z}^3$ spanning L. Let $\boldsymbol{x}$ denote the column vector (x_1, x_2, x_3), and write

$$R = \{(x_1, x_2, x_3) \in [0, 2\pi)^3 : [\boldsymbol{\ell}_1 \cdot \boldsymbol{x}]_{2\pi} = 0 \text{ and } [\boldsymbol{\ell}_2 \cdot \boldsymbol{x}]_{2\pi} = 0\}.$$

Define $f : \mathbb{R}^3 \to \mathbb{R}$ by setting $f(x_1, x_2, x_3) = \sum_{j=1}^{3} 2|c_j| \cos(x_j + \phi_j)$. As before, the minima of f over R are in one-to-one correspondence with those of h over $\mathbb{T}$.

For $(x_1, x_2, x_3) \in [0, 2\pi)^3$, we have $[\boldsymbol{\ell}_1 \cdot \boldsymbol{x}]_{2\pi} = 0$ and $[\boldsymbol{\ell}_2 \cdot \boldsymbol{x}]_{2\pi} = 0$ if and only if there exist $q_1, q_2 \in \mathbb{Z}$, with $|q_1| \leq |\ell_{1,1}|+|\ell_{1,2}|+|\ell_{1,3}|$ and $|q_2| \leq |\ell_{2,1}|+|\ell_{2,2}|+|\ell_{2,3}|$ such that $\boldsymbol{\ell}_1 \cdot \boldsymbol{x} = 2\pi q_1$ and $\boldsymbol{\ell}_2 \cdot \boldsymbol{x} = 2\pi q_2$. For each of these finitely many $\boldsymbol{q} = (q_1, q_2)$, we can invoke Lemma 17 with f, $M = \begin{pmatrix} \ell_{1,1} & \ell_{1,2} & \ell_{1,3} \\ \ell_{2,1} & \ell_{2,2} & \ell_{2,3} \end{pmatrix}$, and $\boldsymbol{q}$, to conclude that f achieves its minimum μ finitely many times over R, and therefore that h achieves the same minimum finitely many times over $\mathbb{T}$.

(iii) Finally, we observe that the case $p = 3$ cannot occur: indeed, a basis for L of dimension 3 would immediately entail that every λ_j is a root of unity.

This concludes the proof of the claim that h achieves its minimum at a finite number of points $Z = \{(\zeta_1, \zeta_2, \zeta_3) \in \mathbb{T} : h(\zeta_1, \zeta_2, \zeta_3) = \mu\}$.

We concentrate on the set Z_1 of first coordinates of Z. Write

$$\tau_1(x) = \exists z_1(\mathrm{Re}(z_1) = x \wedge z_1 \in Z_1)$$
$$\tau_2(y) = \exists z_1(\mathrm{Im}(z_1) = y \wedge z_1 \in Z_1)$$

Similarly to our earlier constructions $\tau_1(x)$ is equivalent to a formula $t_1'(x)$ in the in the first-order theory of the reals, over a bounded number of real variables, with $\|\tau_1'(x)\| = \|\mathbf{u}\|^{O(1)}$. Thanks to Theorem 12, we then obtain an equivalent quantifier-free formula

$$\chi_1(x) = \bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} h_{i,j} \sim_{i,j} 0.$$

Note that since there can only be finitely many $\hat{x} \in \mathbb{R}$ such that $\chi_1(\hat{x})$ holds, each disjunct of $\chi_1(\hat{x})$ must comprise at least one equality predicate, or can otherwise be entirely discarded as having no solution. A similar exercise can be carried out with $\tau_2(x)$. The bounds on the degree and height of each $h_{i,j}$ in $\chi_1(x)$ and $\chi_2(y)$ then enables us to conclude that any $\zeta_1 = \hat{x} + i\hat{y} \in Z_1$ is algebraic, and moreover satisfies $\|\zeta_1\| = \|\mathbf{u}\|^{O(1)}$. In addition, bounds on I and J_i guarantee that the cardinality of Z_1 is at most polynomial in $\|\mathbf{u}\|$.

Since λ_1 is not a root of unity, for each $\zeta_1 \in Z_1$ there is at most one value of n such that $\lambda_1^n = \zeta_1$. Theorem 5 then entails that this value (if it exists) is at most $M = \|\mathbf{u}\|^{O(1)}$, which we can take to be uniform across all $\zeta_1 \in Z_1$. We can now invoke Lemma 3 to conclude that, for $n > M$, and for all $\zeta_1 \in Z_1$, we have

$$|\lambda_1^n - \zeta_1| > \frac{1}{n^{\|\mathbf{u}\|^D}}, \tag{3.8}$$

where $D \in \mathbb{N}$ is some absolute constant.

Let $b > 0$ be minimal such that the set

$$\{z_1 \in \mathbb{C} : |z_1| = 1 \text{ and, for all } \zeta_1 \in Z_1, |z_1 - \zeta_1| \geq \frac{1}{b}\}$$

is non empty. Thanks to our bounds on the cardinality of Z_1, we can use the first-order theory of the reals, together with Theorem 12, to conclude that b is algebraic and $\|b\| = \|\mathbf{u}\|^{O(1)}$.

Define the function $g : [b, \infty) \to \mathbb{R}$ as follows:

$$g(x) = \min\{h(z_1, z_2, z_3) - \mu : (z_1, z_2, z_3) \in \mathbb{T} \text{ and for all } \zeta_1 \in Z_1, |z_1 - \zeta_1| \geq \frac{1}{x}\}.$$

It is clear that g is continuous and $g(x) > 0$ for all $x \in [b, \infty)$. Moreover, g can be translated in polynomial time into a function in the first-order theory of the reals over a bounded number of variables. It follows from Proposition 2.6.2 of [23] (invoked with the function $1/g$ that there is a polynomial $P \in \mathbb{Z}[x]$ such that, for all $x \in [b, \infty)$,

$$g(x) \geq \frac{1}{P(x)} \tag{3.9}$$

Moreover, an examination of the proof of [23, Prop. 2.6.2] reveals that P is obtained through a process which hinges on quantifier elimination. By Theorem 12, we are therefore able to conclude that $\|P\| = \|\mathbf{u}\|^{O(1)}$, a fact which relies among others on our upper bounds for $\|b\|$.

By Proposition 14 we can find $\varepsilon \in (0, 1)$ and $N = 2^{\|\mathbf{u}\|^{O(1)}}$ such that for all $n > N$, we have $|r(n)| < (1 - \varepsilon)^n$, and moreover $1/\varepsilon = 2^{\|\mathbf{u}\|^{O(1)}}$. In addition, by Proposition 4, there is $N' = 2^{\|\mathbf{u}\|^{O(1)}}$ such that for every $n \geq N'$

$$\frac{1}{2P(n^{\|\mathbf{u}\|^D})} > (1 - \varepsilon)^n. \tag{3.10}$$

Combining Equations (3.7)–(3.10), we get

$$\begin{aligned}
\frac{u_n}{\rho^n} &= a + h(\lambda_1^n, \lambda_2^n, \lambda_3^n) + r(n) \\
&\geq -\mu + h(\lambda_1^n, \lambda_2^n, \lambda_3^n) - (1 - \varepsilon)^n \\
&\geq g(n^{\|\mathbf{u}\|^D}) - (1 - \varepsilon)^n \\
&\geq \frac{1}{P(n^{\|\mathbf{u}\|^D})} - (1 - \varepsilon)^n \\
&= \frac{1}{2P(n^{\|\mathbf{u}\|^D})} + \frac{1}{2P(n^{\|\mathbf{u}\|^D})} - (1 - \varepsilon)^n \\
&\geq \frac{1}{2P(n^{\|\mathbf{u}\|^D})}
\end{aligned}$$

provided $n > \max\{M, N, N'\}$. We thus have that $\frac{u_n}{\rho^n}$ is eventually lower bounded by an inverse polynomial and hence we have effective divergence bounds in this case.

It remains to show how to handle inhomogeneous LRS of order at most 8. Consider an inhomogeneous LRS $\langle v_n \rangle$ of order at most 8, and let $u_n = \text{HOM}(v_n)$. Observe that by Proposition 37, u_n might not be a simple LRS. However, all its characteristic roots have multiplicity 1, apart from, possibly, the characteristic root 1.

Consider the dominant modulus ρ of u_n. If $\rho > 1$, then by Proposition 37 the exponential polynomial of $\frac{u_n}{\rho^n}$ is of the same form as that in Equation (3.2), in the sense that $r(n)$ is still exponentially decaying. Thus, we can proceed with the analysis above without change. If $\rho = 1$, things become slightly more involved. Consider the exponential polynomial

$$u_n = A(n) + \sum_{i=1}^{m} (c_i \lambda_i^n + \overline{c_i}\,\overline{\lambda_i^n}) + r(n) \tag{3.11}$$

where $A(n)$ is either a constant or a polynomial, $c_i \in \mathbb{C} \setminus \mathbb{R}$ for every $1 \leq i \leq m$, $|r(n)|$ is exponentially decaying, and $0 \leq m \leq 4$. Observe that if $A(n)$ is a constant, then $|u_n|$ is bounded, and so does not diverge. In particular, if $m = 4$ then it has to be the case that $A(n)$ is constant. Thus, it suffices to consider the case where $m \leq 3$ and $A(n)$ is a polynomial.

In this case, similarly to Case 1 in the proof of Theorem 33, we have that $\mathbf{u}$ diverges if and only if the leading coefficient of $A(n)$ is positive, and in this case the bounds are effectively computable.

This completes the proof of Theorem 34. □

3.2.2 Effective Divergence Lower Bound

We observed that the Divergence Problem is decidable for homogeneous and inhomogeneous LRS of order at most 5. However, when the order the of the LRS is at least 6, the Divergence Problem remains open. As we will see later in this subsection, the difficulty arises when the LRS has 3 characteristic roots of multiplicity 2. In this scenario, the mathematical tools required for comparing the dominant term

$$(a_1 + c_1 \lambda^n + \bar{c}_1 \bar{\lambda}^n) n$$

and

$$a_0 + c_0 \lambda_1^n + \bar{c}_0 \bar{\lambda}^n,$$

which are required to decide whether

$$u_n = (a_1 + c_1 \lambda^n + \bar{c}_1 \bar{\lambda}^n) n + (a_0 + c_0 \lambda_1^n + \bar{c}_0 \bar{\lambda}^n) \to \infty,$$

have not yet been developed to the best of our knowledge. In fact, as we demonstrate in the rest of this subsection (cf. Example 36), the development of such tools will have a significant effect on number theory, and more specifically, on Diophantine approximation of a certain family of transcendental numbers. Surprisingly, these lower bounds hold already for homogeneous LRS even without requiring effectively computable bounds.

Theorem 35. *Ultimate Positivity is reducible to Divergence.*

Proof. We show a reduction from the Ultimate Positivity problem for non-degenerate LRS of order 6, shown to be hard in [76]. The key ingredient in the reduction is Theorem 31.

Consider a non-degenerate homogeneous LRS $\langle u_n \rangle$ of order 6 with dominant modulus ρ, and let $\mu = \max\{2, \frac{2}{\rho}\}$, then the sequence $v_n = \mu^n u_n$ is a non-degenerate homogeneous LRS of order 6 with dominant modulus $\mu\rho \geq 2$. By Theorem 31, taking $\varepsilon = \frac{1}{2}$, it follows that there exists $N \in \mathbb{N}$ such $|v_n| \geq 2^{n/2}$ for every $n > N$. It immediately follows that v_n is ultimately positive if and only if $v_n \to \infty$. Clearly, however, v_n and u_n have the same sign, and therefore u_n is ultimately positive if and only if v_n diverges, and we are done. □

In the next example we will study a family of LRS for which the Divergence Problem is hard. This family of LRS is used in [76, section 5] to show the hardness of deciding the Positivity and Ultimate Positivity Problems for homogeneous LRS of order 6.

Example 36. Consider the following family of recurrence equations

$$\begin{aligned} u_{n+6} = 4(p+1)u_{n+5} - 4(4p^2+8p+3)u_{n+4} + 32(2p^2+2p+1)u_{n+3} \\ - 16(4p^2+8p+3)u_{n+2} + 64(2p+1)u_{n+1} + 64u_n, \end{aligned} \tag{3.12}$$

where p is a rational number $0 < p < 1$. Let $0 < q < 1$ be any rational number with $p^2 + q^2 = 1$. The set of all such points,

$$\mathcal{A} = \left\{ p + qi \in \mathbb{C} : p, q \in \mathbb{Q}, p^2 + q^2 = 1, \text{and } p, q \neq 0 \right\},$$

contains all the points on the complex unit circle S^1 with rational real and imaginary parts, excluding $\{\pm 1, \pm i\}$. As shown in [76, secion 5], the set $\mathcal{A}$ is a dense set in S^1, consisting only of algebraic numbers of degree 2, none of which is a root of unity.

Remember from Subsubsection 2.1 that we use $\mathrm{Log}(\cdot)$ to denote the principal branch of the complex natural logarithm function. Write

$$\mathcal{T} = \left\{ \frac{\mathrm{Log}\,\lambda}{2\pi} : \lambda \in \mathcal{A} \right\}.$$

For any $\lambda \in \mathcal{A}$, since λ is not a root of unity, $t = \frac{\mathrm{Log}\,\lambda}{2\pi}$ cannot be a rational number. By the Gelfond-Schneider Theorem (Subsection 2.3.5), it follows that t must be a transcendental number.

For $\lambda = p + qi \in \mathcal{A}$ and $r \in \mathbb{Q}^+$, write

$$\begin{aligned} u_n &= -n1^n + \frac{1}{2}(n - ri)\lambda^n + \frac{1}{2}(n + ri)\bar{\lambda}^n, \\ v_n &= -n1^n + \frac{1}{2}(n + ri)\lambda^n + \frac{1}{2}(n - ri)\bar{\lambda}^n. \end{aligned} \tag{3.13}$$

Both $\mathbf{u} = \langle u_n \rangle_{n=0}^{\infty}$ and $\mathbf{v} = \langle v_n \rangle_{n=0}^{\infty}$ are LRS satisfying the homogeneous order 6 recurrence relation (3.12), with characteristic roots $1, \lambda$ and $\bar{\lambda}$, each of which have multiplicity two. Also, note that since λ and $\bar{\lambda}$ have rational real and imaginary parts, by induction u_n and v_n are rational for all $n \in \mathbb{N}$. Let $\theta = \mathrm{Log}\,\lambda$. For all $n \in \mathbb{N}$, u_n and v_n can be written as

$$\begin{aligned} u_n &= r \sin n\theta - n(1 - \cos n\theta), \\ v_n &= -r \sin n\theta - n(1 - \cos n\theta). \end{aligned}$$

For $n \in \mathbb{N}$, let

$$\begin{aligned} u'_n &= 2^n u_n, \\ v'_n &= 2^b v_n, \\ w_n &= \max\{u_n, v_n\} = r|\sin n\theta| - n(1 - \cos n\theta). \end{aligned}$$

We now show how we can compute the Lagrange constant of an arbitrary $t \in \mathcal{T}$ given an oracle for solving the Divergence Problem for $-\mathbf{u}' = \langle -u'_n \rangle_{n=0}^{\infty}$ and $-\mathbf{v}' = \langle -v'_n \rangle_{n=0}^{\infty}$.

Given $\varepsilon \in (0, 1)$, using the Taylor expansion of sin and cos, there exists $\delta > 0$ such that, for all $x \in [-\delta, \delta]$, we have

$$(1 - \varepsilon)|x| \leq |\sin x| \leq |x|, \text{ and} \tag{3.14}$$

$$(1 - \varepsilon)\frac{x^2}{2} \leq 1 - \cos x \leq \frac{x^2}{2}. \tag{3.15}$$

Moreover, we can choose a large enough $N \in \mathbb{N}$ with $2r/N \leq \delta$ such that, for all $x \in (-\pi, \pi]$,

$$\text{if } 1 - \cos x < \frac{2r}{N}, \text{ then } |x| \leq \delta, \tag{3.16}$$

since the *cos* function is $1-1$ and continuous in $(-\pi, \pi]$ interval.

Using the definition of L_∞ (Subsection 2.3.6), it is straightforward to show that

$$2\pi L_\infty(t) = \liminf_{n\in\mathbb{N}} n[n(2\pi t)]_{2\pi} = \liminf_{n\in\mathbb{N}} n[n\theta]_{2\pi}. \tag{3.17}$$

We now assert the following:

Claim 1: For any $n \geq N$, if $w_n > 0$, then $n[n\theta]_{2\pi} < \frac{2r}{1-\varepsilon}$.

Claim 2: For any $n \geq N$, if $n[n\theta]_{2\pi} < 2r(1-\varepsilon)$, then $w_n > 0$.

To prove Claim 1, assume that $n \geq N$ and $w_n > 0$. Then

$$\begin{aligned}
& n(1-\cos n\theta) < r && \text{[by definition of } w_n\text{]} \\
\Rightarrow\ & 1-\cos n\theta < \frac{r}{n} < \frac{2r}{n} \leq \frac{2r}{N} && \\
\Rightarrow\ & [n\theta]_{2\pi} \leq \delta && \text{[by (3.16)]} \\
\Rightarrow\ & 0 < w_n \leq r[n\theta]_{2\pi} - n(1-\varepsilon)\frac{([n\theta]_{2\pi})^2}{2} && \text{[(3.15), (3.14)]} \\
\Rightarrow\ & n[n\theta]_{2\pi} < \frac{2r}{1-\varepsilon}, &&
\end{aligned}$$

as required.

For Claim 2, assume that $n \geq N$ and $n[n\theta]_{2\pi} < 2r(1-\varepsilon)$. Then

$$\begin{aligned}
& [n\theta]_{2\pi} \leq 2r/N \leq \delta && \\
\Rightarrow\ & w_n \geq r(1-\varepsilon)[n\theta]_{2\pi} - n\frac{([n\theta]_{2\pi})^2}{2} && \text{[(3.14), (3.15)]} \\
\Rightarrow\ & w_n > 0, &&
\end{aligned}$$

since $r(1-\varepsilon)[n\theta]_{2\pi} > n\frac{([n\theta]_{2\pi})^2}{2}$, and since $[m\theta]_{2\pi} \neq 0$ because λ is not a root of unity. This proves Claim 2.

Remember from Subsubsection 2.1 that $L_\infty(t)$ is computable whenever there is an algorithm that can provide arbitrary accurate rational approximations of $L_\infty(t)$. To this end it suffices to validate arbitrary rational purported lower bounds ℓ of $\pi L_\infty(t)$.

Given the oracle for solving the Divergence Problem for $-\mathbf{u}'$ and $-\mathbf{v}'$, we can decide whether $L_\infty(t) \geq \ell/\pi$ as follows

- Let $r = \ell$. Observe that by Theorem 31, $-\mathbf{u}'$ (resp. $-\mathbf{v}'$) is divergent if an only if $-\mathbf{u}$ (resp. $-\mathbf{v}$) is ultimately positive. Therefore, if both $-\mathbf{u}'$ and $-\mathbf{v}'$ are divergent, then $w_n \leq 0$ for all sufficiently large $n \in \mathbb{N}$. Hence, by Claim 2, $n[n\theta]_{2\pi} \geq 2\ell(1-\varepsilon)$. Since this holds for all $\varepsilon \in (0,1)$, it follows from (3.17) that $\pi L_\infty(t) \geq \ell$.

- On the other hand, if one or both of $-\mathbf{u}'$ and $-\mathbf{v}'$ fail to diverge, then there must be infinitely many values of n such that $w_n > 0$. Claim 1 and Equation (3.17) then entail that $\pi L_\infty(t) \leq \ell$.

This shows solving the Divergence Problem for LRS of order 6 would entail a procedure for calculating the Lagrange constant of a given $t \in \mathcal{T}$, a long-standing open problem in Diophantine approximation of transcendental numbers, which is unlikely to be solved without a major breakthroughs in mathematics. □

Similarly to Positivity and Ultimate Positivity Problems, Figure 3.4 shows the location of eigenvalues of a hard instance of Divergence Problem.

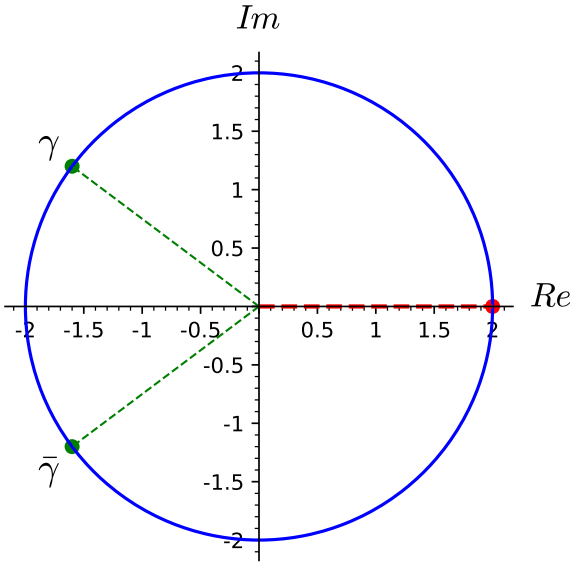

Figure 3.4: Eigenvalues $1, \gamma, \bar{\gamma}$ (each of multiplicity 2) of a hard instance of Divergence Problem.

3.3 Positivity and Ultimate Positivity of Inhomgeneous LRS

In this section we study the Positivity and Ultimate Positivity problems for inhomogeneous LRS. These problems were studied in [77, 76, 75] for homogeneous LRS. Using Proposition 15 and some careful analysis, we extend the decidability results to inhomogeneous LRS.

3.3.1 Correspondence between Homogeneous and Inhomogeneous LRS

Let us start by reformulating the notion of linear recurrence more abstractly as follows. Define the *shift operator* $E : \mathbb{R}^{\mathbb{N}} \to \mathbb{R}^{\mathbb{N}}$ by $E(f)(n) = f(n+1)$ for a sequence $f \in \mathbb{R}^{\mathbb{N}}$. The polynomial ring $\mathbb{R}[E]$ acts on the set of sequences $\mathbb{R}^{\mathbb{N}}$ on the left in a natural way, turning $\mathbb{R}^{\mathbb{N}}$ into a left $\mathbb{R}[E]$ module. Then a sequence $\mathbf{u} = \langle u_n \rangle_{n=0}^{\infty}$ satisfies the recurrence equation (3.1) if and only if $p(E) \cdot \mathbf{u} = a_{k+1} \cdot \mathbf{1}$, where p is the characteristic polynomial of the recurrence and $\mathbf{1}$ is the all-ones sequence.

We are now ready to prove Proposition 15:

Proof of Proposition 15. By assumption we have that $p(E) \cdot \mathbf{u} = \mathbf{c}$ for some monic polynomial $p(x)$ of degree k and constant sequence $\mathbf{c}$. Writing $q(x) = (x-1)p(x)$, we have $q(E) \cdot \mathbf{u} = (E-1) \cdot \boldsymbol{c} = 0$. □

Note that for a given LRS $\mathbf{u}$, the proof of Proposition 15 allows us to compute the homogeneous representation of $\mathbf{u}$, and remember from Subsubsection 2.5, that for a LRS $\mathbf{u}$, $\textsc{hom}(\mathbf{u})$ denotes the homogeneous representation of $\mathbf{u}$. Let $\|\mathbf{u}\|$ denote the binary representation length[5] of $\mathbf{u}$. We remark that the transformations back and forth between homogeneous and inhomogeneous LRS can be carried out in polynomial time in $\|u\|$ if the given LRS have real algebraic coefficients. The proof of Proposition 15 gives us the following useful property.

Proposition 37. *The characteristic roots of* $\textsc{hom}(\mathbf{v})$ *are the same as those of* $\mathbf{v}$*, with the same multiplicities, except for the characteristic root* 1*, which always occurs in* $\textsc{hom}(\mathbf{v})$*, and whose multiplicity is* $m+1$*, where* m *is the multiplicity of* 1 *in* $\mathbf{v}$*.*

Consider an LRS $\mathbf{u}$ with integer coefficients. Since the characteristic polynomial p of an LRS $\mathbf{u}$ has integer coefficients, the characteristic roots of $\mathbf{u}$ comprise real-algebraic roots $\{\rho_1, \ldots, \rho_d\}$, and conjugate pairs of complex-algebraic roots $\{\gamma_1, \overline{\gamma_1}, \ldots, \gamma_m, \overline{\gamma_m}\}$. There are now univariate polynomials $A_1, \ldots, A_d$ with real-algebraic coefficients and $C_1, \ldots, C_m$ with complex-algebraic coefficients such that, for every $n \geq 0$,

$$u_n = \sum_{i=1}^{d} A_i(n)\rho_i^n + \sum_{j=1}^{m} (C_j(n)\gamma_j^n + \overline{C_j(n)}\overline{\gamma}_j^n).$$

The degree of each of the polynomials in this exponential polynomial is strictly smaller than the multiplicity of the corresponding root. For a fixed order k, the coefficients appearing in the polynomials can be computed in time polynomial in $\|\mathbf{u}\|$.

[5] in general, we denote by $\|\cdot\|$ the binary-representation length of objects.

In order to extend the results in [77, 76, 75], we establish a correspondence between homogeneous and inhomogeneous LRS. It is known how to convert an inhomogeneous LRS to a homogeneous LRS using Proposition 15; for the reverse reduction we prove the following partial converse to Proposition 15.

Proposition 38. *Let* $\mathbf{u} = \langle u_n \rangle_{n=0}^{\infty}$ *satisfy a homogeneous linear recurrence of order* $k+1$ *with a positive real characteristic root* ρ*. Then the sequence* $\mathbf{v} = \langle v_n \rangle_{n=0}^{\infty}$ *defined by* $v_n = \frac{u_n}{\rho^n}$ *satisfies an inhomogeneous linear recurrence of order* k*.*

Proof. By assumption, $\mathbf{u}$ satisfies the recurrence $f(E) \cdot \mathbf{u} = 0$ for some monic polynomial $f(x) \in \mathbb{R}[x]$ of degree $k+1$ that has a positive real root ρ. Define a sequence $\mathbf{v} = \langle v_n \rangle_{n=0}^{\infty}$ by $v_n := \frac{u_n}{\rho^n}$ for all $n \in \mathbb{N}$. Then $\mathbf{v}$ satisfies the recurrence $g(E) \cdot \mathbf{v} = 0$ where g is the monic polynomial $g(x) = \rho^{-(k+1)} f(\rho x)$.

But $g(1) = 0$ and hence we have the factorization $g(x) = (x-1)h(x)$ for some monic polynomial $h(x) \in \mathbb{R}[x]$. It follows that $(E-1)h(E) \cdot \mathbf{v} = 0$ and hence $h(E) \cdot \mathbf{v}$ is constant, i.e., $\mathbf{v}$ satisfies an inhomogeneous recurrence of order k. □

3.3.2 Positivity and Ultimate Positivity Upper Bounds

We proceed to prove analogous results to Theorem 27 for inhomogeneous LRS.

Theorem 27 along with Proposition 15 readily give us the following:

Theorem 39. *Positivity and Ultimate Positivity are decidable for inhomogeneous LRS of order* 4 *or less, with complexity in* $\mathbf{coNP}^{\mathbf{PosSLP}}$ *and* **PTIME***, respectively.*

For simple LRS, things become more involved, as Proposition 15 does not preserve simplicity. However, Proposition 37 shows that simplicity is almost preserved, up to the multiplicity of the characteristic root 1. As we now show, this is sufficient to obtain upper bounds for inhomogeneous simple LRS.

We start by addressing effective Ultimate Positivity, which we then use for addressing Positivity.

Theorem 40. *Effective Ultimate Positivity is solvable in polynomial time for simple inhomogeneous LRS of order* 8 *or less.*

Proof. Let $\mathbf{v}$ be a simple, non-degenerate, inhomogeneous LRS of order 8 or less, and consider the homogeneous LRS $\mathbf{u} = \textsc{hom}(\mathbf{v})$. By Proposition 15, $\mathbf{u}$ is of order at most 9. If $\mathbf{u}$ is a simple LRS, then by [76] we can effectively decide its Ultimate Positivity. We hence assume that $\mathbf{u}$ is not simple.

By Proposition 37, it follows that the characteristic roots of $\mathbf{u}$ all have multiplicity 1, apart from the characteristic root 1 which has multiplicity 2. Consider the dominant modulus ρ of $\mathbf{u}$. If $\rho > 1$, then by writing the exponential polynomial of $\mathbf{u}$, we have

$$\frac{u_n}{\rho^n} = a + \sum_{i=1}^{m}(c_i\lambda_i^n + \overline{c_i}\overline{\lambda_i^n}) + r(n) \tag{3.18}$$

with $a \in \mathbb{R}$, $c_i \in \mathbb{C}$, and $|\lambda_i| = 1$ for every $1 \leq i \leq m$, and $|r(n)|$ exponentially decaying. Crucially, since 1 is not a dominant characteristic root, its effect is enveloped in $r(n)$. Specifically, we observe that the analysis of effective Ultimate Positivity in [76] only relies on Proposition 14. Since this holds in the case at hand, we can effectively decide Ultimate Positivity when 1 is not a dominant characteristic root.

Finally, if 1 is a dominant characteristic root, the exponential polynomial of $\mathbf{u}$ can be written as

$$u_n = A(n) + \sum_{i=1}^{m}(c_i\lambda_i^n + \overline{c_i}\overline{\lambda_i^n}) + r(n). \tag{3.19}$$

We observe that in this case, u_n is ultimately positive if and only if it diverges (indeed, clearly $|u_n| \to \infty$). Thus, we can reduce the problem to divergence, and proceed with the analysis as in Case 1 of Subsubsection 3.2.

This concludes the proof that Ultimate Positivity is effectively decidable for simple inhomogeneous LRS of order at most 8. □

Similarly to Theorem 40, we are able to conclude the following results.

Theorem 41. *Ultimate Positivity is decidable in polynomial time for simple inhomogeneous LRS of any order.*

Proof. Let $\mathbf{v}$ be a simple, non-degenerate, inhomogeneous LRS, and consider the homogeneous LRS $\mathbf{u} = \textsc{hom}(\mathbf{v})$. If $\mathbf{u}$ is a simple LRS, then by [76] we can effectively decide its Ultimate Positivity. We assume henceforth that $\mathbf{u}$ is not simple.

By Proposition 37, it follows that the characteristic roots of $\mathbf{u}$ all have multiplicity 1, apart from the characteristic root 1 which has multiplicity 2. Consider the dominant modulus ρ of $\mathbf{u}$. If $\rho > 1$, then by writing the exponential polynomial of $\mathbf{u}$, we have

$$\frac{u_n}{\rho^n} = a + \sum_{i=1}^{m}(c_i\lambda_i^n + \overline{c_i}\overline{\lambda_i^n}) + r(n) \tag{3.20}$$

with $a \in \mathbb{R}$, $c_i \in \mathbb{C} \setminus \mathbb{R}$ and $|\lambda_i| = 1$ for every $1 \leq i \leq m$, and $|r(n)|$ exponentially decaying. Crucially, since 1 is not a dominant characteristic root, its effect is enveloped in $r(n)$. Specifically, we observe that the analysis of effective Ultimate Positivity in [75]

only relies on Proposition 14. Since this holds in the case at hand, we can effectively decide Ultimate Positivity when 1 is not a dominant characteristic root.

Finally, if 1 is a dominant characteristic root, the exponential polynomial of $\mathbf{u}$ can be written as

$$u_n = A(n) + \sum_{i=1}^{m}(c_i\lambda_i^n + \overline{c_i}\overline{\lambda_i^n}) + r(n) \tag{3.21}$$

We observe that in this case, u_n is ultimately positive if and only if it diverges (indeed, clearly $|u_n| \to \infty$). Thus, we can reduce the problem to divergence, and proceed with the analysis as in Case 1 of Subsubsection 3.2. □

Finally, using Theorem 40, we can solve the Positivity problem.

Theorem 42. *Positivity is decidable for simple inhomogeneous LRS of order* 8 *or less, with complexity in* $\mathbf{coNP^{PosSLP}}$.

Proof. Given the proof of Theorem 40, Positivity is now easily decidable: given an inhomogeneous simple LRS $\mathbf{u}$ of order at most 8, decide if its ultimately positive, and if so - compute the bound from which it is ultimately positive. Then deciding Positivity amounts to checking a finite number of elements.

Note that the bound computed in Theorem 40 is $N = 2^{\|\mathbf{u}\|^{O(1)}}$. This implies that checking whether an ultimately-positive LRS is *not* positive can be done using a *guess-and-check* procedure, and employing **PosSLP** in order to compute double exponential numbers. This yields an $\mathbf{NP^{PosSLP}}$ algorithm. In fact, thanks to [3], we obtain an upper bound of $\mathbf{coNP^{PP^{PP^{PP}}}}$ for Positivity (see [76] for details). □

3.3.3 Positivity and Ultimate Positivity Lower Bounds

We now turn to study lower bounds of the Positivity and Ultimate Positivity Problems, proving analogous results to Theorems 25 and 30 for inhomogeneous LRS.

Ultimate Positivity Lower Bound

Theorem 43. *If Ultimate Positivity is decidable for inhomogeneous rational LRS of order at least 5 then there is an algorithm that computes the Lagrange constant of any number* $\theta/2\pi$ *such that* $e^{i\theta}$ *has rational real and imaginary parts.*

Proof. In [76], it is shown that deciding Ultimate Positivity of the homogeneous LRS of order 6 given by

$$u_n = r\sin n\theta - n(1-\cos n\theta) \text{ and } v_n = -r\sin n\theta - n(1-\cos n\theta)$$

for every $r \in \mathbb{Q}$ such that $r > 0$ and $\theta \in (0, 2\pi)$ such that $e^{i\theta}$ has rational real and imaginary parts would allow one to compute $L_\infty(\theta/2\pi)$ (cf. Example 44).

We observe that both sequences u_n and v_n fall under the premise of Proposition 38. Thus, by applying Proposition 38, we obtain an equivalent inhomogeneous LRS of order 5, concluding the proof. □

Example 44. In Example 36, we showed that if we can solve the Divergence Problem for $-\mathbf{u}'$ and $-\mathbf{v}'$, we can compute the Lagrange constant $L_\infty(t)$ of a given transcendental number $t \in \mathcal{T}$. As part of our analysis, we also showed that $-\mathbf{u}'$ and $-\mathbf{v}'$ are divergent to ∞ if and only if $-\mathbf{u}$ and $-\mathbf{v}$ are ultimately positive. Remember that

$$-u_n = n1^n - \frac{1}{2}(n - ri)\lambda^n - \frac{1}{2}(n + ri)\bar{\lambda}^n,$$
$$-v_n = n1^n - \frac{1}{2}(n + ri)\lambda^n - \frac{1}{2}(n - ri)\bar{\lambda}^n.$$

Both $-\mathbf{u}$ and $-\mathbf{v}$ satisfy the order 6 homogeneous recurrence equation (3.12). Using the homogenisation technique of Proposition 15, we see that $-\mathbf{u}$ and $-\mathbf{v}$ satisfy the following inhomogeneous order 5 recurrence

$$u_n = (4p+1)u_{n+4} - (4p^2+4p+2)u_{n+3} + (4p^2+4p+2)u_{n+2} - (4p+1)u_{n+1} + u_n + 1. \quad (3.22)$$

This completes the reduction from the problem of computing the Lagrange constant for $t \in \mathcal{T}$ to deciding the Ultimate Positivity Problem for order 5 inhomogeneous LRS. □

Positivity Lower Bound A similar proof, using the results of [76], gives us also the following theorem.

Theorem 45. *If Positivity is decidable for inhomogeneous rational LRS of order at least 5 then there is an algorithm that computes the approximation type of any number $\theta/2\pi$ such that $e^{i\theta}$ has rational real and imaginary parts.*

Example 46. Let us now demonstrate a family of LRS of inhomogeneous order 5, namely the same as Example 44, to show why deciding positivity of inhomogeneous order 5 LRS is hard. We will achieve this by using $-\mathbf{u}$ and $-\mathbf{v}$ from Example 44, which satisfy the inhomogeneous order 5 recurrence (3.22), and the reduction in [76, section 5] for showing the hardness of the Positivity Problem for order 6 homogeneous LRS.

Our approach in this example will be similar to Example 36. We first need the following counterpart to (3.17)

$$2\pi L(t) = \inf_{m\in\mathbb{N}} m[m(2\pi t)]_{2\pi} = \inf_{m\in\mathbb{N}} m[m\theta]_{2\pi}. \tag{3.23}$$

We can now show how given an oracle for deciding the Positivity Problem for $-\mathbf{u}$ and $-\mathbf{v}$, one can compute $L(t)$ for a given $t \in \mathcal{T}$. To show this, it suffices to validate arbitrary rational purported lower bounds ℓ of $\pi L(t)$ as following

- Simliarly to Example 36, let $r = \ell$. If both $-\mathbf{u}$ and $-\mathbf{v}$ are positive, then $w_n \leq 0$ for all $n \in \mathbb{N}$. Hence, by Claim 2, $n[n\theta]_{2\pi} \geq 2\ell(1-\varepsilon)$. Since this holds for all $\varepsilon \in (0,1)$, it follows from (3.23) that $\pi L(t) \geq \ell$.

- On the other hand, if one or both of $-\mathbf{u}$ and $-\mathbf{v}$ fail to be positive, then there must exist some $n \in \mathbb{N}$ such that $w_n > 0$. Claim 1 and Equation (3.23) then entail that $\pi L(t) < \ell$.

This shows solving the Positivity Problem for inhomogeneous LRS of order 5 would entail a procedure for calculating the approximation type of a given $t \in \mathcal{T}$, another long-standing open problem in Diophantine approximation of transcendental numbers, which is unlikely to be solved without a major breakthroughs in mathematics.

□

Chapter 4

Integer Linear Loops

4.1 Introduction

In this chapter, we will consider the *Universal Termination Problem* for the *single-path affine loop programs*, or *affine loops* for short. Remember from Chapter 1 that affine loop programs are program defined by a loop

$$\textit{while } (B\boldsymbol{x} > \boldsymbol{b}) \textit{ do } \boldsymbol{x} := A\boldsymbol{x} + \boldsymbol{c}\,, \tag{4.1}$$

where $A, B, \boldsymbol{b}, \boldsymbol{c}$ are matrices of appropriated dimensions. In (4.1), $\boldsymbol{x}$ is the variable vector, and the constraint $B\boldsymbol{x} > \boldsymbol{b}$ is called the loop guard; the matrix A is the update matrix, and the function $\boldsymbol{x} \to A\boldsymbol{x} + \boldsymbol{c}$ is referred to as the update function of the loop. We say that a loop P of the form (4.2) is homogeneous when $\boldsymbol{b}$ and $\boldsymbol{c}$ are both zero vectors. 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., [24, 45, 52]).

For a set $S \subseteq \mathbb{R}^d$, we say that the above loop *terminates on* S or *is terminating over initial values in* S if it terminates on all initial values in S. This problem is sometimes referred to as the *universal termination problem* as it asks for termination over all initial values in S. Despite the simplicity of single-path affine loops, the question of deciding termination has proven challenging (and termination becomes undecidable if the update function in the loop body is allowed to be piecewise linear or if the loop body consists of a nondeterministic choice between two different linear updates [17]).

Example 47. Consider the loop

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

where $A = \left(\begin{smallmatrix} 3 & -4 \\ 4 & 3 \end{smallmatrix}\right)$. The matrix $A/5$ is the rotation matrix with rotation angle $\theta = \cos^{-1} 3/5$. Starting from any point $\boldsymbol{x}_0 \in \mathbb{Z}^2$, we will eventually end up in the lower half-plane. Thus, Q is terminating over $\mathbb{Z}^2$. This is demonstrated in Figure 4.1. □

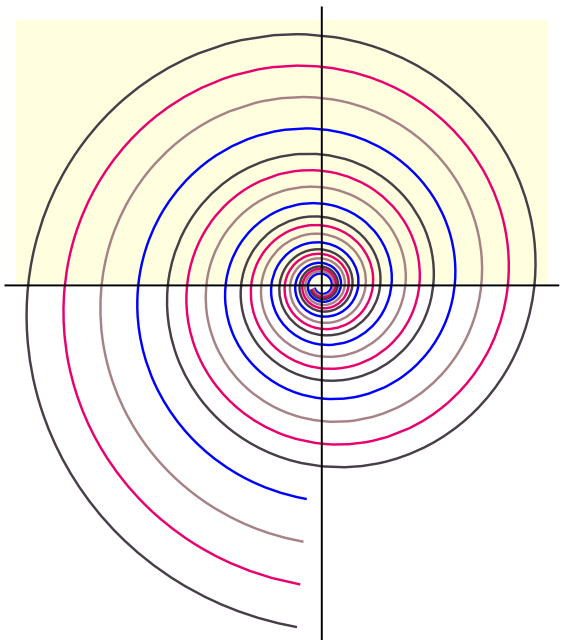

Figure 4.1: A Terminating Linear Loop Program

Tiwari [102] showed that termination of single-path affine loops is decidable over $\mathbb{R}^d$. Subsequently, Braverman [26], 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 $\boldsymbol{b}, \boldsymbol{c}$ are both all-zero vectors. More recently, Ouaknine, Sousa-Pinto, and Worrell [72] have proven that termination over $\mathbb{Z}^d$ is decidable in the non-homogeneous case under the assumption that the update matrix A is a diagonalisable integer matrix. Decidability of termination for non-homogeneous affine loops over $\mathbb{Z}^d$ was conjectured by Tiwari [102, Conjecture 1], but has remained open until now.

In this chapter we give a procedure for deciding termination of the general class of single-path affine loops over the integers, i.e., we generalise the result of [72] by lifting the assumption of diagonalisability. Note that for this class of programs, the question of termination on a single 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 long-standing open problem (going back at least as far as the 1970s [88, 98]), and as we saw in Subsection 3.3.3, solution to the problem will require significant breakthroughs in number theory. However, in considering termination over $\mathbb{Z}^d$ we show that one can benefit from the freedom to choose the initial values of the loop variables. In the present chapter we exploit this freedom in order to circumvent the need to solve "hard instances" of the Positivity Problem when deciding termination of affine loops. In particular, we avoid the use of sophisticated Diophantine-approximation techniques, such as the S-units theorem, that were employed in [76]. By eschewing such tools we lose all hope of obtaining an effective characterisation of the set of non-terminating points. (Compare with the approach in [72], which yielded an effective characterisation of the set of all eventually non-terminating points in the diagonalisable case.) Nevertheless our methods manage to solve the decision problem in the general case.

Among the tools we use are a circle of closely related classical results on 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 chapter 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 affine loops. In particular, techniques to prove termination via synthesis of linear ranking functions [12, 13, 25, 30, 32, 82, 84] and their extension, multiphase linear ranking functions [15, 11], have been developed. Many of these techniques have been implemented in software verification tools, such as Microsoft's TERMINATOR [33]. Although these methods are capable of handling non-deterministic affine loops, they can only guarantee termination whenever ranking functions of a certain form exist.

4.1.1 Linear Loops and LRS

Linear loop programs and LRS are tightly related, and many problem about one can be translated to problems about the other one. In this subsection we will explore this link.

Given a linear loop program P of the form (4.2), by applying the homogenisation process we can assume that $\boldsymbol{b} = \mathbf{0}$ and $\boldsymbol{c} = \mathbf{0}$ so that the loop$\mathsf{P}$ in (4.2) can be written as

$$\textit{while } (B\boldsymbol{x} > \mathbf{0}) \textit{ do } \boldsymbol{x} := A\boldsymbol{x}\,.$$

$$A \in \mathbb{Q}^{d\times d}, B \in \mathbb{Q}^{m\times d}, \boldsymbol{b} = \mathbf{0}, \boldsymbol{c} = \mathbf{0},$$

we can write P as

$$\textit{while } (B_1\boldsymbol{x} > b_1 \wedge \cdots \wedge B_m\boldsymbol{x} > b_m) \textit{ do } \boldsymbol{x} := A\boldsymbol{x} + \boldsymbol{c}\,,$$

where B_i and b_i are rows of B and $\boldsymbol{b}$ respectively. Let us assume that the characteristic polynomial χ_A of A is

$$\chi_A(x) = x^e + a_{e-1}x^{e-1} + \cdots + a_1x + a_0.$$

The Cayley-Hamilton Theorem (Subsection 2.2.1) implies that the matrix A annihilates its characteristic polynomial χ_A. This implies that for all $i \in \{1,\ldots,m\}$ and all $n \in \mathbb{N}$ we have

$$\begin{aligned} & A^d = -a_{d-1}A^{d-1} - \cdots - a_1A - a_0 \\ \Rightarrow\ & A^{n+d} = -a_{d-1}A^{n+d-1} - \cdots - a_1A^{n+1} - a_0A^n \\ \Rightarrow\ & (B_iA^{n+d}\boldsymbol{x}) = -a_{d-1}(B_iA^{n+d-1}\boldsymbol{x}) - \cdots - a_1(B_iA^{n+1}\boldsymbol{x}) - a_0(B_iA^n\boldsymbol{x}). \end{aligned}$$

Hence, if we let $\mathbf{u}^{(i)} = \langle B_iA\boldsymbol{x}\rangle_{n=0}^{\infty}$ for all $i \in \{1,\ldots,m\}$, then $\mathbf{u}^{(i)}$'s are all linear recurrences of order e satisfying the recurrence relation

$$u_{n+d} = -a_{d-1}u_{n+d-1} - \cdots - a_1u_{n-1} - a_0u_n.$$

This relationship allows us to translate termination of P over an initial value $\boldsymbol{x}_0$ to the Positivity Problem for the linear recurrence sequences $\mathbf{u}^{(1)},\ldots,\mathbf{u}^{(m)}$ with initial values $x_1,\ldots,x_d$ where $(x_1,\ldots,x_d)^\top = \boldsymbol{x}_0$. More accurately, the program P is non-terminating on $\boldsymbol{x}_0$ if and only if all linear recurrence sequences $\mathbf{u}^{(1)},\ldots,\mathbf{u}^{(m)}$ are positive.

Conversely, let $\mathbf{u} = \langle u_n\rangle_{n=0}^{\infty}$ be an LRS satisfying the recurrence relation

$$u_{n+k} = a_1u_{n+k-1} + \cdots + a_{k-1}u_{n+1} + a_ku_n.$$

It can be readily checked that

$$u_n = BA^n\boldsymbol{u}_{k-1},$$

where

$$B = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \end{pmatrix},\ A = \begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix},\ \boldsymbol{u}_{k-1} = \begin{pmatrix} u_{k-1} \\ u_{k-2} \\ u_{k-3} \\ \vdots \\ u_0 \end{pmatrix}.$$

Positivity Problem for the LRS $\mathbf{u}$ can be reformulated as problem of termination of the loop

$$\textit{while } (B\boldsymbol{x} > \mathbf{0}) \textit{ do } \boldsymbol{x} := A\boldsymbol{x}\,,$$

on the initial value $\boldsymbol{u}_{k-1}$.

4.1.2 A Survey of Existing Literature

Linear loop programs have been extensively studied due to their wide-range of applications. From computer science perspective, loops with integer values are the most interesting. However, when one permits real initial values, there are strong tools available from continuous mathematics that make the study of loops over such domains considerably easier. Before diving deep into studying integer linear loops, we will first give a brief history of existing results on real, rational, and integer linear loops.

4.1.2.1 Termination of Linear Loop Programs over Real Numbers

Consider the following question:

"Given a loop P of the form (4.2) with rational matrices of appropriate dimensions $A, B, \boldsymbol{b}, \boldsymbol{c}$, does P terminate for all initial values $\boldsymbol{x} \in \mathbb{R}^d$?"

Despite its simplicity it is not obvious how to answer this problem. Tiwari, in 2004, showed that eigenvalues and eigenvectors of the loop P provide enough information to decide whether it terminates or not [102]. In short, he proved the following theorem.

Theorem 48. *It is decidable in* **PTIME** *whether a linear loop program of the form* (4.2) *terminates over all real initial values.*

Example 49 (Example from [102])**.** Consider the loop

$$\mathsf{Q}_1 : \textit{while } (\boldsymbol{x} > \mathbf{0}) \textit{ do } \boldsymbol{x} := A\boldsymbol{x}\,,$$

where $A = \left(\begin{smallmatrix} -2 & 10 \\ 0 & 1 \end{smallmatrix}\right)$. The matrix A has eigenvalues $\lambda_1 = -2$ and $\lambda_2 = 1$, and is diagonalisable. In fact, we have that $P^{-1}AP = \left(\begin{smallmatrix} -2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ where $P = \left(\begin{smallmatrix} 1 & 10 \\ 0 & 3 \end{smallmatrix}\right)$. Transforming

the program Q_1 by P, i.e., by multiplying all the vectors and matrices in Q_1 by P^{-1} from the left and P from the right, we get

$$\mathsf{Q}_2 : \textit{while } (\begin{pmatrix} 1 & 10 \\ 0 & 3 \end{pmatrix} \boldsymbol{y} > \mathbf{0}) \textit{ do } \boldsymbol{y} := \begin{pmatrix} -2 & 0 \\ 0 & 1 \end{pmatrix} \boldsymbol{y}\,,$$

whose termination over the real numbers is equivalent to that of Q_1. The point $\boldsymbol{y}_0 = (0,1)^\top$, corresponding to the positive eigenvalue 1 is a non-terminating initial value for the loop Q_2, which corresponds to the non-terminating initial value $\boldsymbol{x}_0 = (10,3)^\top$ for the loop Q_1. Hence the loop Q_1 is non-terminating over $\mathbb{R}^2$.

We can, moreover, compute the set of eventually non-terminating points. Every initial value $\boldsymbol{v} \in \mathbb{R}^2$ can be written as $\boldsymbol{v} = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2$, where $\boldsymbol{v}_1 = (1,0)^\top$ and $\boldsymbol{v}_2 = (10,3)^\top$ are the eigenvectors corresponding to λ_1 and λ_2, respectively. After n application of the update matrix A, starting from the vector $\boldsymbol{v}$ we obtain

$$A^n\boldsymbol{v} = a_1\lambda_1^n\boldsymbol{v}_1 + a_2\lambda_2^n\boldsymbol{v}_2.$$

Since $\lambda_1 < 0$ and $|\lambda_1| > |\lambda_2|$, whenever $a_1 \neq 0$, the loop Q_1 is terminating over the initial value $\boldsymbol{v}$. Therefore, it can be readily seen that the set of non-terminating initial values is the set $\{a_2\boldsymbol{v}_2 : a_2 > 0\}$.

Intuitively, since the most expensive part of the computation required for deciding the termination of linear loop programs is the computation of eigenvalues and eigenvectors of the update matrix, termination of linear loop programs can be decided in **PTIME**. For the exact details on the complexity, we refer the interested reader to [102]. □

Tiwari, consequently, conjectured that the universal halting problem is also decidable over rational numbers and integers [102, Conjecture 1].

4.1.2.2 Termination of Linear Loop Programs over Rational Numbers

In 2006, Braverman proved Tiwari's conjecture for rational numbers [26]. In other words, he showed the answer to following question is positive.

"Given a loop P of the form (4.2) with rational matrices of appropriate dimensions $A, B, \boldsymbol{b}, \boldsymbol{c}$, does P terminate for all initial values $\boldsymbol{x} \in \mathbb{Q}^d$?"

The tools he used are more advanced than those of Tiwari, and the proof involves a more fine-tuned analysis of eigenvectors and eigenvalues of the update matrix. The following theorem is from [26].

Theorem 50. *It is decidable in* **PTIME** *whether a linear loop program of the form* (4.2) *terminates over all rational initial values.*

Example 51 demonstrates a linear loop program that is terminating over rational initial values, but is non-terminating over real initial values, while Example 52 demonstrates a linear loop program that is terminating over rational initial values.

Example 51 (Example from [26])**.** Consider the loop

$$\mathsf{Q} : \textit{while } (B\boldsymbol{x} > \mathbf{0}) \textit{ do } \boldsymbol{x} := A\boldsymbol{x}\,,$$

where $A = \left(\begin{smallmatrix} -2 & 4 \\ 4 & 0 \end{smallmatrix}\right)$, and $B = (4\ 1)$. The matrix A has two eigenvectors $\boldsymbol{v}_1 = (-1-\sqrt{17}, 4)$ and $\boldsymbol{v}_2 = (-1+\sqrt{17}, 4)$ corresponding to the eigenvalues $\lambda_1 = -1-\sqrt{17}$ and $\lambda_2 = -1+\sqrt{17}$, respectively.

Every vector $\boldsymbol{v} \in \mathbb{R}^2$ can be written as $\boldsymbol{v} = t_1\boldsymbol{v}_1 + t_2\boldsymbol{v}_2$. Starting from the initial value $\boldsymbol{v}$, after n consecutive application of the update function, we have that

$$A^n\boldsymbol{v} = t_1A^n\boldsymbol{v}_1 + t_2A^n\boldsymbol{v}_2 = t_1\lambda_1^n\boldsymbol{v}_1 + t_2\lambda_2^n\boldsymbol{v}_2.$$

When $t_1 = 0$, i.e., when $\boldsymbol{v} = t_2\boldsymbol{v}_2$, we see that for all $n > 0$ the loop guard is satisfied, i.e., $BA^n\boldsymbol{v} = t_2BA^n\boldsymbol{v}_2 > 0$, and hence the loop is non-terminating. However, we observe that for all non-zero t_2, we have that $\boldsymbol{v} = t_2\boldsymbol{v}_2 \notin \mathbb{Q}^2$.

When $t_1 \neq 0$, the vector $A^n\boldsymbol{v}$ is dominated by the $t_1\lambda_1^n\boldsymbol{v}_1$ term. Since $\lambda_1 < 0$, $BA^n\boldsymbol{v} < 0$ for infinitely many $n > 0$, and therefore, Q terminates over $\boldsymbol{v}$. Thus, there is no non-terminating rational initial value.

Hence, the loop is terminating over $\mathbb{Q}^2$ even though it is non-terminating over $\mathbb{R}^2$. □

Example 52 (Example from [26])**.** Consider the loop

$$\mathsf{Q} : \textit{while } (B\boldsymbol{x} > \mathbf{0}) \textit{ do } \boldsymbol{x} := A\boldsymbol{x}\,,$$

where $A = \left(\begin{smallmatrix} 2 & 4 \\ 4 & 0 \end{smallmatrix}\right)$, and $B = (4\ -5)$. The matrix A has two eigenvectors $\boldsymbol{v}_1 = (1+\sqrt{17}, 4)$ and $\boldsymbol{v}_2 = (1-\sqrt{17}, 4)$ corresponding to the eigenvalues $\lambda_1 = 1+\sqrt{17}$ and $\lambda_2 = 1-\sqrt{17}$, respectively.

We notice that $\lambda_1 > 0 > \lambda_2$. The eigenvector $\boldsymbol{v}_1$ satisfies the loop guard, and corresponds to the positive eigenvalue λ_1. Hence, the loop does not terminate over $\mathbb{R}^2$. Even though the line $\{t\boldsymbol{v}_1 : t \in \mathbb{R}^2\}$ does not contain any non-zero rational points, the orbit of a rational perturbation $\boldsymbol{v}_1'$ of $\boldsymbol{v}_1$ converges to the direction of $\boldsymbol{v}_1$ as λ_1 is bigger in modulus than λ_2. The point $q_1 = (9, 7)$ is an example of a such point. Note that $|\frac{9}{7} - \frac{1+\sqrt{17}}{4}| < 0.005$, which means that $\boldsymbol{v}_1'$ is a good rational approximation of $\boldsymbol{v}_1$. Hence, the loop is non-terminating over $\mathbb{Q}^2$.

An important observation here is that even though the update matrices in this Example and Example 51 are similar, in contrast to Example 51 the dominant eigenvalue in this Example is positive. similarly to Example 51, all non-zero multiples of the eigenvector corresponding to the positive eigenvalue are not in $\mathbb{Q}^2$. However, since in this example, the positive eigenvalue is dominant, we can find rational initial values that are close enough to the line $\{t\boldsymbol{v}_1 : t \in \mathbb{R}^2\}$ and are non-terminating. □

The following corollary is a by-product of Theorem 50.

Corollary 53. *It is decidable in* **PTIME** *whether a linear loop program of the form* (4.2) *terminates over all integer initial values whenever* P *is homogeneous.*

Termination of integer linear loops had yet to wait 10 years for any progress.

4.1.2.3 Termination of Linear Loop Programs over Integers

Assuming the update matrix A in (4.2) is diagonalisable, Ouaknine, Pinto, and Worrell [72] provided a procedure to decide the following question

"Given a loop P of the form (4.2) with integer matrices of appropriate dimensions $A, B, \boldsymbol{b}, \boldsymbol{c}$, does P terminate for all initial values $\boldsymbol{x} \in \mathbb{Z}^d$?"

Their result can be summarised in the following theorem.

Theorem 54. *It is decidable in* **EXPSPACE** *whether a linear loop program of the form* (4.2) *terminates over all integer initial values whenever the update matrix A of* P *is diagonalisable.*

Their procedure, in fact, computes a representation of the set of all eventually non-terminating integer points. The problem of termination of linear loops over integers, however, remained open in its most general case.

4.2 Termination of Affine Loops over Integers

In this section, we fully settle the problem of termination of affine loops over integer. At a high level, the main results of this chapter can be summarised as follows:

> Given an affine loop program
>
> $$\textit{while } (B\boldsymbol{x} > \boldsymbol{b}) \textit{ do } \boldsymbol{x} := A\boldsymbol{x} + \boldsymbol{c}\,,$$
>
> with integer matrices of appropriate dimensions $A, B, \boldsymbol{b}, \boldsymbol{c}$, it is decidable whether the loop terminates over all integer initial values.

The precise decision procedure for solving the Termination Problem of affine loops over integers can be found in Subsection 4.2.3.

4.2.1 Termination Analysis via Spectral Theory

The general form of a single-path affine loop in dimension d can be, alternatively, written as:

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

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

$$\begin{pmatrix} f(\boldsymbol{x}) \\ 1 \end{pmatrix} = \begin{pmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \boldsymbol{x} \\ 1 \end{pmatrix} \text{ and } g_i(\boldsymbol{x}) = (\boldsymbol{b}_i^\top \; c_i) \begin{pmatrix} \boldsymbol{x} \\ 1 \end{pmatrix}. \tag{4.2}$$

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 $\left(\begin{smallmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{smallmatrix}\right)$ is a root of unity.

Example 55. In Example 51, we saw an integer linear loop program that despite being terminating over $\mathbb{Q}^2$, is non-terminating over $\mathbb{R}^2$. This example provides an integer linear loop program that terminates over $\mathbb{Z}^2$, but is non-terminating over $\mathbb{Q}^2$, and consequently is non-terminating over $\mathbb{R}^2$ as well.

Let

$$\mathsf{Q} : \textit{while } (B\boldsymbol{x} > \boldsymbol{b}) \textit{ do } \boldsymbol{x} := A\boldsymbol{x} + \boldsymbol{c}\,,$$

where $A = \left(\begin{smallmatrix} -9 & 0 \\ 0 & 6 \end{smallmatrix}\right)$, $B = (-1 \;\; 1)$, $\boldsymbol{b} = -4$, and $\boldsymbol{c} = (-45 \;\; -9)^\top$. Applying the homogenisation process in Subsection 4.1.1 to Q_1, we have that the program Q_1 terminates over all integer (resp. rational) initial values if and only if the program

$$\mathsf{Q}' : \textit{while } (B'\left(\begin{smallmatrix} \boldsymbol{x} \\ 1 \end{smallmatrix}\right) > \boldsymbol{0}) \textit{ do } \left(\begin{smallmatrix} \boldsymbol{x} \\ 1 \end{smallmatrix}\right) := A'\left(\begin{smallmatrix} \boldsymbol{x} \\ 1 \end{smallmatrix}\right),$$

where $A' = \left(\begin{smallmatrix} A & \boldsymbol{c} \\ \boldsymbol{0} & 1 \end{smallmatrix}\right)$ and $B' = (B \;\; -\boldsymbol{b})$, terminates over all integer (resp. rational) initial values.

The matrix A' has three eigenvectors $\boldsymbol{v}_1 = (1, 0, 0)$, $\boldsymbol{v}_2 = (0, 1, 0)$, and $\boldsymbol{v}_3 = (-\frac{9}{2}, \frac{9}{5}, 1)$, corresponding to the eigenvalues $\lambda_1 = -9, \lambda_2 = 6$, and $\lambda_3 = 1$, respectively.

Any vector $\boldsymbol{u} \in \mathbb{R}^3$ can be written as a linear sum of $\boldsymbol{v}_1, \boldsymbol{v}_2$ and $\boldsymbol{v}_3$. Note that the eigenvalue $\lambda_3 = 1$ and eigenvector $\boldsymbol{v}_3$ appear due to the homogenisation. For a valid

initial value $\boldsymbol{u} = (u_1, u_2, u_3)^\top = t_1\boldsymbol{v}_1 + t_2\boldsymbol{v}_2 + t_3\boldsymbol{v}_3$ of the loop Q' we must have $u_3 = 1$. Hence, $t_3 = 1$.

Moreover, whenever $t_1 \neq 0$, the vector $\boldsymbol{u}$ is dominated by the negative eigenvalue $\lambda_1 = -9$ since λ_1 is larger in modulus than λ_2 and λ_3. Therefore, we have that $B'(\binom{\boldsymbol{x}}{1}) \leq 0$ infinitely often and consequently, Q' terminates over $\boldsymbol{u}$. Thus, the only candidates of non-termination lie on the line

$$\{t_2\boldsymbol{v}_2 + \boldsymbol{v}_3 : t_2 \in \mathbb{R}\} = \left\{(-\frac{9}{2}, \frac{9}{5} + t_2, 1)^\top : t_2 \in \mathbb{R}\right\},$$

which does not have any integer point. However, the rational initial value $(-\frac{9}{2}, 5, 1)^\top$ satisfies the loop guard and is non-terminating. Therefore, the integer linear loop Q is non-terminating over $\mathbb{Q}^2$, but it is terminating over $\mathbb{Z}^2$. □

Proposition 56. *The termination problem for single-path affine loops on integers is reducible to the special case of the problem for non-degenerate update functions.*

Proof. Consider a single-path affine 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 $\frac{\lambda_i}{\lambda_j}$ for $i \neq j$. It is known that $L = 2^{O(d\sqrt{\log d})}$ [38, 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

$$\mathsf{P}: \textit{ while } (g(\boldsymbol{x}) > 0) \textit{ do } \boldsymbol{x} \leftarrow f(\boldsymbol{x}) \tag{4.3}$$

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 Subsection 4.2.2.

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 $\left(\begin{smallmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{smallmatrix}\right)$ and let $k_{\max}$ be the maximum multiplicity over all these eigenvalues.

Intuitively, we know that eigenvalues of the largest modulus dominate the behaviour of the program; and among eigenvalues of the same modulus, the ones with higher multiplicity have a higher influence on the program. To formalise and utilise this notion, we define a linear preorder on $I := \{0, \ldots, k_{\max} - 1\} \times \{1, \ldots, s\}$ 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 $i_1 \leq i_2$. Write $(i_1, j_1) \prec (i_2, j_2)$ if $(i_1, j_1) \preccurlyeq (i_2, j_2)$ and $(i_2, j_2) \not\preccurlyeq (i_1, j_1)$. Now we observe that

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

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 $(i_1, j_1) \approx (i_2, j_2)$ if and only if $(i_1, j_1) \preccurlyeq (i_2, j_2)$ and $(i_2, j_2) \preccurlyeq (i_1, j_1)$.

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

Proposition 57. *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 $n \geq d$ 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. Using the Jordan-Chevalley decomposition (Subsection 2.2.4), we can write $\left(\begin{smallmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{smallmatrix}\right) = P^{-1}DP + N$, 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 $D_1, \ldots, D_s$.

Then for all $n \in \mathbb{N}$ with $n \geq d$ we have

$$\begin{aligned}
g(f^n(\boldsymbol{x})) &= (\boldsymbol{b}^\top\ c) \begin{pmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{pmatrix}^n \begin{pmatrix} \boldsymbol{x} \\ 1 \end{pmatrix} \\
&= (\boldsymbol{b}^\top\ c)(P^{-1}DP + N)^n \begin{pmatrix} \boldsymbol{x} \\ 1 \end{pmatrix} \\
&= (\boldsymbol{b}^\top\ c) \sum_{i=0}^{n} \binom{n}{i} P^{-1} D^{n-i} P N^i \begin{pmatrix} \boldsymbol{x} \\ 1 \end{pmatrix} \\
&= (\boldsymbol{b}^\top\ c) \sum_{i=0}^{d} \binom{n}{i} P^{-1} (\lambda_1^{n-i} D_1 + \cdots + \lambda_s^{n-i} D_s) P N^i \begin{pmatrix} \boldsymbol{x} \\ 1 \end{pmatrix} \quad (\text{since } N^{d+1} = 0) \\
&= \sum_{j=1}^{s} \lambda_j^n \sum_{i=0}^{d} \binom{n}{i} \underbrace{\lambda_j^{-i} (\boldsymbol{b}^\top\ c) P^{-1} D_j P N^i \begin{pmatrix} \boldsymbol{x} \\ 1 \end{pmatrix}}_{h_{i,j}(\boldsymbol{x})} \qquad (4.4) \\
&= \sum_{j=1}^{s} \sum_{i=0}^{d} \binom{n}{i} \lambda_j^n h_{i,j}(\boldsymbol{x}) \,,
\end{aligned}$$

where for $(i,j) \in I$ the affine function $h_{i,j}$ is defined in Line (4.4). Clearly each function $h_{i,j}$ is a complex-valued affine function on $\mathbb{R}^d$ with algebraic coefficients. $\square$

Define $\gamma_i = \frac{\lambda_i}{|\lambda_i|}$ for $i = 1, \ldots, s$, that is, we obtain the γ_i by normalising the eigenvalues to have length 1. Recall from Subsection 2.3.4 the definition of the group $L(\boldsymbol{\gamma})$ of multiplicative relations that hold among $\gamma_1, \ldots, \gamma_s$, *viz.*,

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

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

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

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

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

$$\Phi_L(\boldsymbol{x}, \boldsymbol{\mu}) = \sum_{(i,j) \in L} h_{i,j}(\boldsymbol{x}) \mu_j \,. \qquad (4.5)$$

[1]That the function Φ_L 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 57).

From the above definition of Φ_L we have

$$\sum_{(i,j)\in L} \binom{n}{i} \lambda_j^n h_{i,j}(\boldsymbol{x}) = \binom{n}{i_L} \rho_L^n \Phi_L(\boldsymbol{x}, \boldsymbol{\gamma}^n)\,. \tag{4.6}$$

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 58. *Consider the loop* P *in* (4.3). *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 57 and Equation (4.6) we have that for all $n \geq d$,

$$\begin{aligned} g(f^n(\boldsymbol{x})) &= \sum_{(i,j)\in I} \binom{n}{i} \lambda_j^n h_{i,j}(\boldsymbol{x}) \\ &= \binom{n}{i_E} \rho_E^n \Phi_E(\boldsymbol{x}, \boldsymbol{\gamma}^n) + \sum_{(i,j)\in I\setminus E} \binom{n}{i} \lambda_j^n h_{i,j}(\boldsymbol{x})\,. \end{aligned} \tag{4.7}$$

Moreover by the dominance of E we have that

$$\lim_{n\to\infty} \frac{\binom{n}{i}|\lambda_j|^n}{\binom{n}{i_E}\rho_E^n} = 0 \tag{4.8}$$

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 (4.8), this shows that the asymptotically dominant term in Equation (4.7) 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.

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 item 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. □

Example 59. Let Q and Q' be the same integer linear loop programs as Example 55, and $\boldsymbol{x} = (-\frac{9}{2}, 5, 1)^\top$. We observe that for the initial value $\boldsymbol{x}$ we have that $\boldsymbol{\gamma} = T(\boldsymbol{\gamma}) = \{1\}$, and

$$\inf_{\boldsymbol{\mu} \in T(\boldsymbol{\gamma})} \Phi_E(\boldsymbol{x}, \boldsymbol{\mu}) = \inf_{\mu_1 \in \{1\}} \frac{16}{5}\mu_1 = \frac{16}{5} > 0.$$

By Proposition 58, $\boldsymbol{x}$ is an eventually non-terminating initial value for Q'. Therefore, $(-\frac{9}{2}, 5)^\top$ is an eventually non-terminating initial value for Q. Nonetheless, for all $\boldsymbol{y} \in \mathbb{Z}^2$ we have that $\boldsymbol{\gamma} = \{-1\}$, $T(\boldsymbol{\gamma}) = \{\pm 1\}$, and

$$\inf_{\boldsymbol{\mu} \in T(\boldsymbol{\gamma})} \Phi_E(\binom{\boldsymbol{y}}{1}, \boldsymbol{\mu}) = \inf_{\mu_1 \in \{\pm 1\}} \left(y_1 + \frac{9}{2}\right)\mu_1 = -\left|y_1 + \frac{9}{2}\right| < 0$$

since $y_1 + \frac{9}{2} \neq 0$ for all $y_1 \in \mathbb{Z}$. Therefore, we observe, in a different approach than Example 55, that Q is terminating for all integer initial values. □

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 58 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 (4.3) 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 notoriously difficult open problem, only known to be decidable up to dimension 4, which we revisited in Subsection 3.3.3. 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 58.

4.2.2 Analysis of Critical Points

In this section we continue to analyse termination of the loop P, as given in (4.3) in the previous section, and refer to the notation established therein.

4.2.2.1 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 60. *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

$$(\boldsymbol{b}^\top \; c) \begin{pmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{pmatrix}^n \begin{pmatrix} \boldsymbol{x} \\ 1 \end{pmatrix} = \sum_{(i,j)\in I} h_{i,j}(\boldsymbol{x}) \binom{n}{i} \lambda_j^n \tag{4.9}$$

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

$$(\boldsymbol{b}^\top \; c) \begin{pmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{pmatrix}^{n+1} \begin{pmatrix} \boldsymbol{x} \\ 1 \end{pmatrix} = \sum_{(i,j)\in I} \widetilde{h}_{i,j}(\boldsymbol{x}) \binom{n}{i} \lambda_j^n \, . \tag{4.10}$$

Combining Equations (4.9) and (4.10) 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 (see Subsection 2.2.3). 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 61. *If $\boldsymbol{z} \in \mathbb{R}^d$ is critical then for all $n \geq 2d+1$, all points in the relative interior of* $\operatorname{conv}(\{f^d(\boldsymbol{z}), f^{d+1}(\boldsymbol{z}), \ldots, f^n(\boldsymbol{z})\})$ *are eventually non-terminating.*

Proof. Let E be the $\approx$-equivalence class that is dominant for $\boldsymbol{z}$. Fix $\boldsymbol{\mu} \in T(\boldsymbol{\gamma})$. We claim that there exists $n \geq d$ such that $\Phi_E(f^n(\boldsymbol{z}), \boldsymbol{\mu}) > 0$. If this were not the case then by Proposition 60 for all $n \geq d$ we would have $\Phi_E(f^n(\boldsymbol{z}), \boldsymbol{\mu}) = \rho_E^n \, \Phi_E(\boldsymbol{z}, \boldsymbol{\gamma}^n\boldsymbol{\mu}) = 0$. But by Theorem 7, the set $\{\boldsymbol{\gamma}^n\boldsymbol{\mu} : n \geq d\}$ 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. This establishes the claim.

In fact we can sharpen the above claim to state that for some $n \in \{d, d+1, \ldots, 2d+1\}$ we have $\Phi_E(f^n(\boldsymbol{z}), \boldsymbol{\mu}) > 0$. Indeed for all $n \geq d$ we have

$$\Phi_E(f^n(\boldsymbol{z}), \boldsymbol{\mu}) = \rho_E^n \Phi_E(\boldsymbol{z}, \boldsymbol{\gamma}^n\boldsymbol{\mu}) = \sum_{(i,j)\in E} h_{i,j}(\boldsymbol{z}) \rho_E^n \gamma_j^n \mu_j \, .$$

Thus the sequence $\langle \Phi_E(f^n(\boldsymbol{z}), \boldsymbol{\mu}) : n \geq d \rangle$ can be written as a sum of exponentials with at most $d+1$ terms. Since this sequence is not identically zero, it has a non-zero entry for some $n \in \{d, d+1, \ldots, 2d+1\}$ (cf. Subsection 2.2.3). Since $\boldsymbol{\mu}$ was arbitrary, we have that for all $\boldsymbol{\mu} \in T(\boldsymbol{\gamma})$ there exists $n \in \{d, d+1, \ldots, 2d+1\}$ with $\Phi_E(f^n(\boldsymbol{z}), \boldsymbol{\mu}) > 0$.

By Proposition 9, for all $n \geq 2d+1$ and all points $\boldsymbol{x}$ lying in the relative interior of $\operatorname{conv}(\{f^d(\boldsymbol{z}), f^{d+1}(\boldsymbol{z}), \ldots, f^n(\boldsymbol{z})\})$, there exist $\alpha_d, \ldots, \alpha_n > 0$ 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 58. □

4.2.2.2 Integer Non-Terminating Points from Critical Points

Lemma 61 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

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

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 62. *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 $x_n := \boldsymbol{v}^\top f^n(\boldsymbol{z}_*) = v^\top \left(\begin{smallmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{smallmatrix}\right)^n \left(\begin{smallmatrix} \boldsymbol{z}_* \\ 1 \end{smallmatrix}\right)$. If this sequence were constant then $\boldsymbol{v}$ would be orthogonal to V_0, contradicting the fact that $\boldsymbol{v}$ is a non-zero vector in V_0. Since the sequence is non-constant, integer-valued, and satisfies a non-degenerate linear recurrence of order at most $d+1$ (see, e.g., [38, 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 [38, section 2.2]).[2] □

[2]The above argument actually establishes that $\langle x_n \rangle_{n=0}^\infty$ diverges to infinity in absolute value. We briefly sketch a more elementary proof of mere unboundedness. If the sequence $\langle x_n \rangle_{n=0}^\infty$ 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 $d+1$, $\langle x_n \rangle_{n=0}^\infty$ would have an infinite constant subsequence $\langle x_{\ell+pn} \rangle_{n=0}^\infty$. If $p = 1$, then $\langle x_n \rangle_{n=0}^\infty$ is constant, and if $p > 1$, then by [90, Lemma 9.11], $\langle x_n \rangle_{n=0}^\infty$ is degenerate.

Proposition 63. *There exists M such that for all $n \geq M$ the set*

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

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 $C := \operatorname{conv}(\{f^n(\boldsymbol{z}_*) : n \geq d\}) \subseteq V$ 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

$$\boldsymbol{v}^\top(\theta(f^n(\boldsymbol{z}_*)) - \theta(f^d(\boldsymbol{z}_*))) = (\theta^*\boldsymbol{v})^\top(f^n(\boldsymbol{z}_*) - f^d(\boldsymbol{z}_*))\,, \tag{4.11}$$

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 62 entails that the absolute value of (4.11) is unbounded as n runs over $\mathbb{N}$. This proves the claim.

Since $\theta(C_0)$ is a full-dimensional convex subset of $\mathbb{R}^{d_0}$, by Theorem 10 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 4.2.1 and 4.2.2 with a theorem characterising when a loop with a single guard is terminating.

Theorem 64. *The loop* P*, given in* (4.3)*, 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 58.(2). Conversely, if such a $\boldsymbol{z}$ exists then by Lemma 61 and Proposition 63 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 58.(1). □

We postpone the question of the effectiveness of the above characterisation until we handle loops with multiple guards, in Subsection 4.2.3.

4.2.3 Multiple Guards

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

$$\mathsf{Q} \,:\, \textit{while}\ (g_1(\boldsymbol{x}) > 0 \wedge \ldots \wedge g_m(\boldsymbol{x}) > 0)\ \textit{do}\ \boldsymbol{x} := f(\boldsymbol{x})\,, \tag{4.12}$$

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 64.

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 $\gamma_j = \lambda_j/|\lambda_j|$ 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 (4.5). 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 65. *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 58.(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 $E_1, \ldots, E_m$. By Lemma 61 and Proposition 63, there is an integer point $\boldsymbol{z}' \in \mathrm{conv}(\{f^n(\boldsymbol{z}) : n \geq d\})$ 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 58.(1), each loop Q_i fails to terminate on $\boldsymbol{z}'$ and hence also Q is non-terminating on $\boldsymbol{z}'$. □

Proposition 65 leads to the following procedure for deciding termination of a given affine loop Q, as shown in (4.12).

1. Compute the eigenvalues of the matrix corresponding to the loop update function, as given in (4.2).

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 in polynomial time via standard symbolic computations with algebraic numbers. (We refer to [72] for a detailed treatment in a very similar setting.) By Theorem 5, 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 11.

We have thus established the main result of the chapter:

Theorem 66. *There is a procedure to decide termination of single-path affine loops (of the form specified in* (4.12)*) over the integers.*

Furthermore, we can obtain the following crude upper bound on the complexity of termination of affine loops.

Corollary 67. *Termination of single-path affine loop programs is decidable in* **2-EXPSPACE**.

Proof. Computing the eigenvalues of a matrix and the dominance preorder $\preccurlyeq$ among the eigenvalues can be easily accomplished in polynomial time in the size of the input update matrix.

Next, using Theorem 5, we can compute a basis for the group $L(\boldsymbol{\gamma})$ in space $O(\|\boldsymbol{\gamma}\|)$.

Finally in Step 4, we can use Theorem 11 to decide whether $W_{E_1,\ldots,E_m}$ contains any integer point in exponential space. See [50] for the exact complexity.

Therefore, when the update matrix is non-degenerate, we can decide the termination of affine loops over integers in **EXPSPACE**. However, when the update matrix is non-degenerate, using Proposition 56, termination of affine loops can be reduced to termination of non-degenerate affine loops in at most **EXPSPACE**. This results in overall **2-EXPSPACE** complexity. □

Example 68. Let

$$\mathsf{Q} : \textit{while } (B\boldsymbol{x} > \boldsymbol{b}) \textit{ do } \boldsymbol{x} := A\boldsymbol{x}\,,$$

where

$$A = \begin{pmatrix} 5 & 1 & 0 & 0 \\ 0 & 4 & -3 & 0 \\ 0 & 3 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix},\ B = \begin{pmatrix} 1 & 2 & 5 & -6 \\ 3 & -1 & 1 & 4 \end{pmatrix},\ \text{and } \boldsymbol{b} = \begin{pmatrix} 7 \\ -2 \end{pmatrix}.$$

After homogenising Q, we see that the update function has the dominant modulus $\rho = 5$. It also has three eigenvectors

$$\boldsymbol{v}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \boldsymbol{v}_2 = \begin{pmatrix} \frac{3-i}{10} \\ i \\ 1 \\ 0 \\ 0 \end{pmatrix},\ \text{and } \boldsymbol{v}_3 = \begin{pmatrix} \frac{3+i}{10} \\ -i \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

corresponding to the dominant eigenvalues $\lambda_1 = \rho = 5$, $\lambda_2 = \rho\,\gamma = 4 + 3i$, and $\lambda_3 = \rho\,\bar{\gamma} = 4 - 3i$, respectively.

Therefore, we observe that $\boldsymbol{\gamma}^{(1)} = \boldsymbol{\gamma}^{(2)} = (1, \gamma, \bar{\gamma})$, and $T(\boldsymbol{\gamma}^{(1)}) = T(\boldsymbol{\gamma}^{(2)}) = \{(1, \mu, \mu^{-1}) : \mu \in \mathbb{T}\}$; moreover, for a given $\boldsymbol{x} \in \mathbb{Z}^4 \times \{1\}$, we have that

$$\begin{aligned} \inf_{\boldsymbol{\mu} \in T(\boldsymbol{\gamma}^{(1)})} \Phi_{E_1}(\boldsymbol{x}, \boldsymbol{\mu}) &= \inf_{\mu \in \mathbb{T}} \left\{ x_1 + \frac{1 + 19\mu}{10} x_2 + \frac{-3 + 53\mu}{10} x_3 \right\} \\ &= x_1 + \frac{1}{10} x_2 - \frac{3}{10} x_3 - \sqrt{\frac{317(x_2^2 + x_3^2)}{10}}, \\ \inf_{\boldsymbol{\mu} \in T(\boldsymbol{\gamma}^{(2)})} \Phi_{E_2}(\boldsymbol{x}, \boldsymbol{\mu}) &= \inf_{\mu \in \mathbb{T}} \left\{ 3x_1 + \frac{3 - 13\mu}{10} x_2 + \frac{-9 + 19\mu}{10} x_3 \right\} \\ &= 3(x_1 + \frac{1}{10} x_2 - \frac{3}{10} x_3) - \sqrt{\frac{53(x_2^2 + x_3^2)}{10}}. \end{aligned}$$

A simple search over the set of all possible initial values shows that besides $\mathbf{0}$, which is an impostrous critical point, the smallest initial values (in Euclidean norm) for which $\inf_{\boldsymbol{\mu} \in T(\boldsymbol{\gamma}^{(1)})} \Phi_{E_1}(\boldsymbol{x}, \boldsymbol{\mu}) \geq 0$ and $\inf_{\boldsymbol{\mu} \in T(\boldsymbol{\gamma}^{(2)})} \Phi_{E_2}(\boldsymbol{x}, \boldsymbol{\mu}) \geq 0$ are

$$\boldsymbol{x}_1 = \begin{pmatrix} 8 \\ 1 \\ -1 \\ 0 \\ 1 \end{pmatrix} \text{ and } \boldsymbol{x}_2 = \begin{pmatrix} 8 \\ -1 \\ -1 \\ 0 \\ 1 \end{pmatrix}.$$

Hence $W_{E_1,E_2} \neq \emptyset$ and Q is non-terminating. □

Chapter 5

Conclusions & Future Research Directions

The goal of this chapter is to summarise topics that we have covered in this thesis on LRS and affine loop programs in order to reflect on the state-of-the-art and the prospects for further progress in this area. We will, further, introduce some of the related research directions that are natural extensions of the problems considered in this thesis.

5.1 Recurrence Sequences

5.1.1 Linear Recurrence Sequences

Let us start by briefly summarising the decidability results and lower-bounds from Chapter 3.

5.1.1.1 Upper Bounds

Table 5.1 indicates the state-of-the-art decidability results for some of the most important computational problems about LRS. For each decision problem $\mathcal{P}$ (e.g., Divergence) and type of LRS $\mathcal{T}$ (e.g., Simple Homogeneous LRS) the integer in the intersection of their corresponding row and column indicates the highest order for which the problem $\mathcal{P}$ for LRS of type $\mathcal{T}$ is decidable, and the complexity class, in a pair of parentheses in front of that integer, indicates the best complexity upper-bound known to this date. Every "?" in Table 5.1 indicates that there is no known nontrivial complexity upper-bound for the corresponding problem-LRS type pair.

	Skolem	Positivity	Ultimate Positivity	Absolute Divergence	Divergence
Hom. LRS	4 (?)	5 (**coNP$^{\mathbf{PosSLP}}$**)	5 (**PTIME**)	3 (?)	5 (**PTIME**)
LRS	3 (?)	4 (**coNP$^{\mathbf{PosSLP}}$**)	4 (**PTIME**)	2 (?)	5 (**PTIME**)
Simple Hom. LRS	4 (?)	9 (**coNP$^{\mathbf{PosSLP}}$**)	∞ (**PSPACE**)	3 (?)	8 (**PTIME**)
Simple LRS	3 (?)	8 (**coNP$^{\mathbf{PosSLP}}$**)	∞ (**PSPACE**)	2 (?)	8 (**PTIME**)

Table 5.1: The upper-bounds for some of the decision problems about LRS

Skolem Problem: The decidability of the Skolem Problem for order 4 homogeneous LRS was shown in [104] and [69]; deducing the decidability of the Skolem Problem for order 3 LRS simply follows from this and the reduction in Subsection 3.3.1

Positivity Problem: The decidability of the Positivity Problem for order 5 homogeneous LRS and order 9 homogeneous simple LRS in **coNP$^{\mathbf{PosSLP}}$** was shown in [76] and [75], respectively. We showed the decidability of the Positivity Problem for order 4 LRS and order 8 simple LRS in **coNP$^{\mathbf{PosSLP}}$** in [4], and a detailed discussion on this can be found in Subsection 3.3.2.

Ultimate Positivity Problem: The decidability of the Ultimate Positivity Problem for order 5 homogeneous LRS in **PTIME** and all homogeneous simple LRS in **PSPACE** was shown in [76] and [77], respectively. We showed the decidability of the Ultimate Positivity Problem for order 4 LRS in **PTIME** and order 8 simple LRS in **PSPACE** in [4], and a detailed discussion on this can be found in Subsection 3.3.2.

Absolute Divergence Problem: The decidability of the Absolute Divergence Problem for order 3 homogeneous LRS was shown in [69]; deducing the decidability of the Absolute Divergence Problem for order 2 LRS simply follows from this and the reduction in Subsection 3.3.1

Divergence Problem: We showed the decidability of the Divergence Problem for (homogeneous) LRS and (homogeneous) simple LRS in **PTIME** in [4], and a detailed discussion on this can be found in Subsection 3.2.1.

5.1.1.2 Lower Bounds

In Chapter 3, we also revisited some of the lower-bounds from [76, 77] for the Positivity and Ultimate Positivity Problems of homogeneous LRS, and extended them to inhomogeneous LRS. Moreover, in [4], and in more detail in Subsection 3.2.2, We

obtained lower-bounds for the Divergence Problem, which are similar to that of the Ultimate Positivity Problem. All of these lower-bounds are obtained by reducing from some of the long-standing open problems in Diophantine approximations of real numbers. Let us encapsulate this in Table 5.2. The integers in Table 5.2 indicate the lowest degrees for which the lower bound applies, while the specific type of lower-bound result is indicated within the parentheses.

	Skolem	Positivity	Ultimate Positivity	Absolute Divergence	Divergence
Hom. LRS	**NP-Hard**	6 (Appr. type)	6 (Lagr. cons.)	?	6 (Lagr. cons.)
LRS	**NP-Hard**	5 (Appr. type)	5 (Lagr. cons.)	?	6 (Lagr. cons.)
Simple Hom. LRS	**NP-Hard**	?	**coNP**	?	?
Simple LRS	**NP-Hard**	?	**coNP**	?	?

Table 5.2: The lower-bounds for some of the decision problems about LRS

5.1.2 Holonomic Sequences

A *holonomic sequence* (cf. Subsubsection 3.1) is an infinite sequence defined by a recursion of the form

$$a_0(n)u_{n+k} = a_1(n)u_{n+k-1} + \cdots + a_{k-1}(n)u_{n+1} + a_k(n)u_n + a_{k+1}(n),$$

where $a_0(n), \ldots, a_{k+1}(n) \in \mathbb{Q}[n]$ are rational polynomial over the variable n. Holonomic sequences are a natural generalisation of LRS and describe a wide range of natural phenomena. Decision questions about holonomic sequences arise in a wide range of scientific areas. These questions are natural extensions of corresponding problem for LRS, and they provide tools to better understand the behaviour holonomic sequences.

Since holonomic sequences encompass LRS, decision questions such as the Skolem Problem, etc. are expected to be significantly harder for holonomic sequences, in the sense that one expects decidability for lower-order holonomic sequences compared to LRS. Nevertheless, progress has been made by resorting to low orders sequences. Kauers and Pillwein [46] provided an incomplete procedure for the Positivity Problem for holonomic sequences, and Kenison et al. showed the Positivity Problem for holonomic sequences is decidable for a certain family of order 2 holonomic sequences [47].

Other questions such as the Skolem Problem, Ultimate Positivity Problem, and Divergence Problem, however, still remain untouched to this date to the best of our knowledge.

5.1.3 Polynomial Recursive Sequences

Another natural extension of LRS are *Polynomial Recursive Sequence (PRS)* (cf. Subsubsection 3.1). A PRS is an infinite sequence defined by a recursion of the form

$$p(u_{n+k}, u_{n+k-1}, \ldots, u_n) = 0,$$

where $p \in \mathbb{Q}[x_1, \ldots, x_{k+1}]$ is a multivariate polynomial.

Cadilhac et al. considered the expressiveness of PRS and showed that the sequence $\langle n^n \rangle_{n=0}^{\infty}$ is not a PRS [28]. However, to the best of our knowledge, All decision problems considered in this thesis are open for PRS to this date.

5.2 Loop Programs

5.2.1 Linear Loops

In Chapter 4, we recalled that Tiwari [102] and Braverman [26] showed that the Universal Termination Problem is decidable over real and rational numbers. In [44], and in more details in Subsubsection 4.2, we showed that the Universal Termination Problem is decidable over integers as well.

A crucial part of our proof is the requirement for a loop's update matrix to have integer entries. This is required so that the variables in the loop attain integral values after updates. However, when one allows non-integral update matrices, the set $\{|\boldsymbol{v}^\top f^n \boldsymbol{z}_*)| : n \geq d\}$ in Proposition 62 will not be necessarily unbounded. We predict that using techniques in this thesis one can find a decision procedure for affine loops in dimension at most 4, and find lower bounds similar to Subsection 3.3.3 for dimension 5 and higher.

The decision procedure that we have provided in this thesis solves the Universal Termination of affine loops over integers in **2-EXPSPACE**, compared to the **PTIME** complexity of the Universal Termination problem of affine loops over real and rational numbers. Although we provide a **2-EXPSPACE** upper-bound for the universal termination of affine programs, the exact complexity remains open.

5.2.2 Linear Constraint Loops

Linear Constraint Loop programs are a generalisation of single-path affine loop programs. Linear constraint loops are while loop programs of the form

$$\mathsf{P} : \textit{while } B \begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{x}' \end{pmatrix} > \boldsymbol{b} \textit{ do } A \begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{x}' \end{pmatrix} + \boldsymbol{c} > 0\,.$$

Note that here the primed variable represents the values at the completion of an iteration. To this date, the most effective methods for solving the Universal Termination Problem for linear constraint loops are *linear ranking functions (LRF)* [83] and *multiphase-linear ranking functions (MLRF)* [16, 14].

Although, the methods for finding LRF and MLRF are complete, i.e., they find an LRF or MLRF when one exists, they do not decide termination. The reason is that a linear constraint loop program can be terminating without admitting an LRF or MLRF.

A complete method for solving the Universal Termination Problem for linear constraint loop programs remains open over real numbers, rational numbers, and integers, even in low dimensions. We predict that by restricting the family of programs, such as resorting to lower dimensions, we can obtain partial results on the Universal Termination Problem for linear constraint loops. For instance, see [11, 57] for some of the recent progress, where the authors show that the Universal Termination Problem is decidable for the linear constraint loops when the loop guard, i.e., the region defined by $B(\begin{smallmatrix}\boldsymbol{x}\\ \boldsymbol{x'}\end{smallmatrix}) > \boldsymbol{b}$, is compact for all $\boldsymbol{x}$.

Bibliography

[1] Lars Ahlfors. *Complex Analysis (1979) 3rd edition*. McGraw-Hill New York, 3 edition, 1979.

[2] S. Akshay, Timos Antonopoulos, Joël Ouaknine, and James Worrell. Reachability problems for Markov chains. *Inf. Process. Lett.*, 115(2):155–158, 2015.

[3] Eric Allender, Peter Bürgisser, Johan Kjeldgaard-Pedersen, and Peter Bro Miltersen. On the complexity of numerical analysis. *SIAM J. Comput.*, 38(5):1987–2006, 2009.

[4] 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.

[5] Alan Baker. Transcendental number theory. *Cambridge University Press, London*, 1975.

[6] Alan Baker and Gisbert Wüstholz. Logarithmic forms and group varieties. *J. reine angew. Math*, 442(19-62):3, 1993.

[7] Wojciech Banaszczyk, Alexander E Litvak, Alain Pajor, and Stanislaw J Szarek. The flatness theorem for nonsymmetric convex bodies via the local theory of banach spaces. *Mathematics of operations research*, 24(3):728–750, 1999.

[8] W. J. Baumol. *Economic Dynamics. An Introduction*. Macmillan, 1970.

[9] William J Baumol. Economic dynamics: an introduction. Technical report, 1970.

[10] Paul C Bell and Igor Potapov. On the undecidability of the identity correspondence problem and its applications for word and matrix semigroups. *International Journal of Foundations of Computer Science*, 21(06):963–978, 2010.

[11] Amir M. Ben-Amram, Jesús J. Doménech, and Samir Genaim. Multiphase-linear ranking functions and their relation to recurrent sets. In Bor-Yuh Evan Chang, editor, *Static Analysis - 26th International Symposium, SAS 2019, Porto, Portugal, October 8-11, 2019, Proceedings*, volume 11822 of *Lecture Notes in Computer Science*, pages 459–480. Springer, 2019.

[12] 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.

[13] Amir M. Ben-Amram and Samir Genaim. Ranking functions for linear-constraint loops. *J. ACM*, 61(4):26:1–26:55, 2014.

[14] Amir M. Ben-Amram and Samir Genaim. Ranking functions for linear-constraint loops. *J. ACM*, 61(4):26:1–26:55, 2014.

[15] 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.

[16] Amir M. Ben-Amram and Samir Genaim. On multiphase-linear ranking functions. In Rupak Majumdar and Viktor Kuncak, editors, *Computer Aided Verification - 29th International Conference, CAV 2017, Heidelberg, Germany, July 24-28, 2017, Proceedings, Part II*, volume 10427 of *Lecture Notes in Computer Science*, pages 601–620. Springer, 2017.

[17] Amir M. Ben-Amram, Samir Genaim, and Abu Naser Masud. On the termination of integer loops. *ACM Trans. Program. Lang. Syst.*, 34(4):16:1–16:24, 2012.

[18] Jean Berstel and Maurice Mignotte. Deux propriétés décidables des suites récurrentes linéaires. *Bulletin de la Société Mathématique de France*, 104:175–184, 1976.

[19] Vincent D. Blondel, Olivier Bournez, Pascal Koiran, Christos H. Papadimitriou, and John N. Tsitsiklis. Deciding stability and mortality of piecewise affine dynamical systems. *Theor. Comput. Sci.*, 255(1-2):687–696, 2001.

[20] Vincent D. Blondel, Emmanuel Jeandel, Pascal Koiran, and Natacha Portier. Decidable and undecidable problems about quantum automata. *SIAM J. Comput.*, 34(6):1464–1473, 2005.

[21] Vincent D Blondel and Natacha Portier. The presence of a zero in an integer linear recurrent sequence is np-hard to decide. *Linear algebra and its Applications*, 351:91–98, 2002.

[22] Vincent D. Blondel and John N. Tsitsiklis. A survey of computational complexity results in systems and control. *Autom.*, 36(9):1249–1274, 2000.

[23] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. *Real algebraic geometry*, volume 36. Springer Science & Business Media, 2013.

[24] Bernard Boigelot. On iterating linear transformations over recognizable sets of integers. *Theor. Comput. Sci.*, 309(1-3):413–468, 2003.

[25] 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.

[26] 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.

[27] John R. Burke and William A. Webb. Asymptotic behavior of linear recurrences. 1981.

[28] Michaël Cadilhac, Filip Mazowiecki, Charles Paperman, Michal Pilipczuk, and Géraud Sénizergues. On polynomial recursive sequences. In Artur Czumaj, Anuj Dawar, and Emanuela Merelli, editors, *47th International Colloquium on Automata, Languages, and Programming, ICALP 2020, July 8-11, 2020, Saarbrücken, Germany (Virtual Conference)*, volume 168 of *LIPIcs*, pages 117:1–117:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

[29] Gregory J Chaitin. A theory of program size formally identical to information theory. *Journal of the ACM (JACM)*, 22(3):329–340, 1975.

[30] Hong Yi Chen, Shaked Flur, and Supratik Mukhopadhyay. Termination proofs for linear simple loops. *STTT*, 17(1):47–57, 2015.

[31] Henri Cohen. *A course in computational algebraic number theory*, volume 138. Springer Science & Business Media, 2013.

[32] 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.

[33] 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.

[34] Julian L Coolidge. The story of the binomial theorem. *The American Mathematical Monthly*, 56(3):147–157, 1949.

[35] Thomas W Cusick and Mary E Flahive. *The Markoff and Lagrange spectra*. Number 30. American Mathematical Soc., 1989.

[36] Jean-Paul Delahaye et al. *Information, complexité et hasard*. 1994.

[37] Harm Derksen, Emmanuel Jeandel, and Pascal Koiran. Quantum automata and algebraic groups. *J. Symb. Comput.*, 39(3-4):357–371, 2005.

[38] 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.

[39] Jan-Hendrik Evertse. On sums of s-units and linear recurrences. *Compositio Math*, 53(2):225–244, 1984.

[40] Susantha Goonatilake. *Toward a global science: Mining civilizational knowledge*. Indiana University Press, 1998.

[41] Fernando Q. Gouvêa. *p-adic Numbers: An Introduction*. Universitext. Springer International Publishing; Springer, 3rd edition, 2020.

[42] V. Halava, T. Harju, M. Hirvensalo, and J. Karhumäki. Skolem's problem – on the border between decidability and undecidability. Technical Report 683, Turku Centre for Computer Science, 2005.

[43] Vesa Halava, Tero Harju, and Mika Hirvensalo. Positivity of second order linear recurrent sequences. *Discret. Appl. Math.*, 154(3):447–451, 2006.

[44] Mehran Hosseini, Joël Ouaknine, and James Worrell. Termination of linear loops over the integers. In Christel Baier, Ioannis Chatzigiannakis, Paola Flocchini, and Stefano Leonardi, editors, *46th International Colloquium on Automata, Languages, and Programming, ICALP 2019, July 9-12, 2019, Patras, Greece*, volume 132 of *LIPIcs*, pages 118:1–118:13. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[45] 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.

[46] Manuel Kauers and Veronika Pillwein. When can we detect that a p-finite sequence is positive? In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, pages 195–201, 2010.

[47] G. Kenison, O. Klurman, E. Lefaucheux, F. Luca, P. Moree, J. Ouaknine, A. Whiteland, and J. Worrell. On inequality decision prolems for low-order holonomic sequences. Submitted.

[48] G. Kenison, R. Lipton, J. Ouaknine, and J. Worrell. On the skolem problem and prime powers. In *International Symposium on Symbolic and Algebraic Computation, ISSAC '20*. ACM, 2020.

[49] Evelyn Kennedy. Omar khayyam. *The Mathematics Teacher*, 59(2):140–142, 1966.

[50] 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.

[51] Aleksandr Yakovlevich Khinchin. Dirichlet's principle in the theory of diophantine approximations. *Uspekhi Matematicheskikh Nauk*, 3(3):3–28, 1948.

[52] Zachary Kincaid, Jason Breck, John Cyphert, and Thomas W. Reps. Closed forms for numerical loops. *PACMPL*, 3(POPL):55:1–55:29, 2019.

[53] Donald E Knuth. The art of computer programming, generating all trees-history of combinatorial generation, volume 4 (fascicle 4), 2006.

[54] Vichian Laohakosol and Pinthira Tangsupphathawat. Positivity of third order linear recurrence sequences. *Discret. Appl. Math.*, 157(15):3239–3248, 2009.

[55] Vichian Laohakosol and Pinthira Tangsupphathawat. Positivity of third order linear recurrence sequences. *Discrete Applied Mathematics*, 157(15):3239–3248, 2009.

[56] Christer Lech. A note on recurring series. *Arkiv för Matematik*, 2(5):417–421, 1953.

[57] Jan Leike and Matthias Heizmann. Geometric nontermination arguments. In Dirk Beyer and Marieke Huisman, editors, *Tools and Algorithms for the Construction and Analysis of Systems - 24th International Conference, TACAS 2018, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2018, Thessaloniki, Greece, April 14-20, 2018, Proceedings, Part II*, volume 10806 of *Lecture Notes in Computer Science*, pages 266–283. Springer, 2018.

[58] Aristid Lindenmayer, Grzegorz Rozenberg, et al. *Automata, languages, development*. North-Holland Pub. Co., 1976.

[59] Richard J Lipton. Mathematical embarrassments. In *The P= NP Question and Gödel's Lost Letter*, pages 209–213. 2010.

[60] Mario Livio. *The golden ratio: The story of phi, the world's most astonishing number*. Crown, 2008.

[61] Kurt Mahler. *Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen*. Noord-Hollandsche Uitgevers Mij, 1935.

[62] Kurt Mahler and JWS Cassels. On the taylor coefficients of rational functions. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 52, pages 39–48. Cambridge University Press, 1956.

[63] Davender S Malik, John M Mordeson, and MK Sen. *Fundamentals of abstract algebra*. McGraw-Hill, 1996.

[64] A Markov. On certain insoluble problems concerning matrices. In *Doklady Akad. Nauk SSSR*, volume 57, pages 539–542, 1947.

[65] David W Masser. Linear relations on algebraic groups. *New Advances in Transcendence Theory*, pages 248–262, 1988.

[66] Yuri Matiyasevich. *Hilbert's tenth problem*. MIT press, 1993.

[67] Carl D. Meyer. *Matrix Analysis and Applied Linear Algebra*. Society for Industrial and Applied Mathematics, USA, 2000.

[68] M. Mignotte. A note on linear recursive sequences. *J. Austral. Math. Soc.*, 20(2):242–244, 1975.

[69] M. Mignotte, T. Shorey, and R. Tijdeman. The distance between terms of an algebraic recurrence sequence. *J. für die reine und angewandte Math.*, 349, 1984.

[70] Kenji Nagasaka and Jau-Shyong Shiue. Asymptotic positiveness of linear recurrence sequences. *Fibonacci Quart*, 28(4):340–346, 1990.

[71] Ivan Morton Niven. *Diophantine approximations*. Courier Corporation, 2008.

[72] 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.

[73] Joël Ouaknine and James Worrell. Decision problems for linear recurrence sequences. In *International Workshop on Reachability Problems*, pages 21–28. Springer, 2012.

[74] Joël Ouaknine and James Worrell. Effective positivity problems for simple linear recurrence sequences. *CoRR*, abs/1309.1550, 2013.

[75] Joël Ouaknine and James Worrell. On the positivity problem for simple linear recurrence sequences,. In *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part II*, pages 318–329, 2014.

[76] 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.

[77] Joël Ouaknine and James Worrell. Ultimate positivity is decidable for simple linear recurrence sequences. In *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part II*, pages 330–341, 2014.

[78] Joël Ouaknine and James Worrell. On linear recurrence sequences and loop termination. *SIGLOG News*, 2(2):4–13, 2015.

[79] Michael S Paterson. Unsolvability in 3×3 matrices. *Studies in Applied Mathematics*, 49(1):105–107, 1970.

[80] Peter Petersen. *Linear algebra*. Undergraduate texts in mathematics. Springer, 2017.

[81] Leonardo Pisano and LE Sigler. Fibonacci's liber abaci: a translation into modern english of the book of calculation. *Sources and Studies in the History of Mathematics and Physical Sciences, Sigler, Laurence E., trans, Springer*, 2002.

[82] 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.

[83] Andreas Podelski and Andrey Rybalchenko. A complete method for the synthesis of linear ranking functions. In Bernhard Steffen and Giorgio Levi, editors, *Verification, Model Checking, and Abstract Interpretation, 5th International Conference, VMCAI 2004, Venice, Italy, January 11-13, 2004, Proceedings*, volume 2937 of *Lecture Notes in Computer Science*, pages 239–251. Springer, 2004.

[84] 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.

[85] Roshdi Rashed. *The development of Arabic mathematics: between arithmetic and algebra*, volume 156. Springer Science & Business Media, 2013.

[86] James Renegar. On the computational complexity and geometry of the first-order theory of the reals. part i: Introduction. preliminaries. the geometry of semi-algebraic sets. the decision problem for the existential theory of the reals. *Journal of symbolic computation*, 13(3):255–299, 1992.

[87] Andrew M Rockett and Peter Szusz. *Continued fractions*. World Scientific Publishing Company, 1992.

[88] G. Rozenberg and A. Salomaa. *Cornerstones of Undecidability*. Prentice Hall, 1994.

[89] Arto Salomaa. Growth functions of lindenmayer systems: Some new approaches. *Automata, Languages, Development. North-Holland*, 1976.

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

[91] Wolfgang M Schmidt. *Diophantine approximation*. Springer Science & Business Media, 1996.

[92] Tony C Scott and Pan Marketos. On the origin of the fibonacci sequence. *MacTutor History of Mathematics*, pages 1–46, 2014.

[93] Helaine Selin. *Encyclopaedia of the history of science, technology, and medicine in non-westen cultures*. Springer Science & Business Media, 2013.

[94] T. N. Shorey and C. L. Stewart. On the Diophantine equation $ax^{2t}+bx^{t}y+cy^{2} = d$ and pure powers in recurrence sequences. *Math. Scand.*, 52(1):24–36, 1983.

[95] Nathan Sidoli and Glen Van Brummelen. *From Alexandria, Through Baghdad: Surveys and Studies in the Ancient Greek and Medieval Islamic Mathematical Sciences in Honor of JL Berggren*. Springer Science & Business Media, 2013.

[96] Parmanand Singh. The so-called fibonacci numbers in ancient and medieval india. *Historia Mathematica*, 12(3):229–244, 1985.

[97] Thoralf Skolem. Ein verfahren zur behandlung gewisser exponentialer gleichungen und diophantischer gleichungen. *Comptes Rendus*, 8:163–188, 1934.

[98] Matti Soittola. On D0L synthesis problem. In A. Lindenmayer and G. Rozenberg, editors, *Automata, Languages, Development*. North-Holland, 1976.

[99] Eduardo Sontag. From linear to nonlinear: some complexity comparisons. In *Proceedings of 1995 34th IEEE Conference on Decision and Control*, volume 3, pages 2916–2920. IEEE, 1995.

[100] Terrence Tao. Open question: Effective skolem-mahler-lech theorem. *Terence Tao personal blog*, 2007.

[101] Alfred Tarski. A decision method for elementary algebra and geometry. *Bulletin of the American Mathematical Society*, 59, 1951.

[102] 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.

[103] Alfred J Van Der Poorten and Hans Peter Schlickewei. Additive relations in fields. *Journal of the Australian Mathematical Society*, 51(1):154–170, 1991.

[104] Nikolai K. Vereshchagin. The problem of appearance of a zero in a linear recurrence sequence. *Mat. Zametki*, 38(2):609–615, 1985.

[105] Michel Waldschmidt. *Diophantine approximation on linear algebraic groups: transcendence properties of the exponential function in several variables*, volume 326. Springer Science & Business Media, 2013.

[106] Kazuhiro Yokoyama, Ziming Li, and István Nemes. Finding roots of unity among quotients of the roots of an integral polynomial. In *Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation*, ISSAC '95, page 85–89, New York, NY, USA, 1995. Association for Computing Machinery.